Microsoft

Azure 云安全白皮书

目录 Contents

Chapter 1
背景介绍

1.1 外部环境变化

在谈论安全之前，我们不得不先环顾四周，看下我们是处在怎样的一种环境中来做好保护。一直以外，企业安全与黑客攻击，就像 DNA 的双螺旋结构一样，交替的演变，进化。而时至今日，在如今移动为先，云为先的企业环境下，此二者也转移到了这一片战场中，延续着厮杀。

首先我们不能，也无法不注意到现在企业日常工作中所碰到的变化，就是你所使用的很多应用，已经不仅仅掌握在公司总部 IT 的数据中心中，越来越多的供应商及厂商自身也转而选择云端的 IaaS, PaaS，SaaS 的服务，根据 Gartner 的预测，如 Table 1[1] 所示，SaaS 领域的投资将会达到 850 亿美元的量级，并且将在一年后达到近千亿美元级别的市场。与此同时，云端的 IaaS，PaaS 或者其他更细分的新兴领域像 Data as a Service，或者 Cloud Management and Security Services 也都会不断的扩展其在企业应用中的份额。

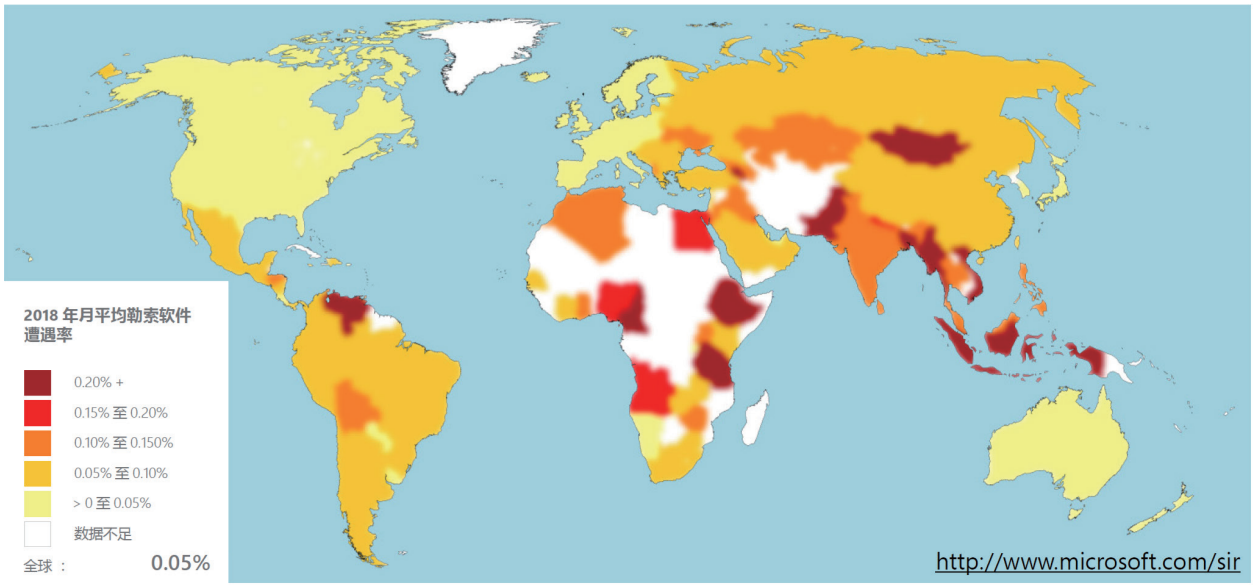
Table 1. Worldwide Public Cloud Service Revenue Forecast (Billions of U.S. Dollars)

	2017	2018	2019	2020	2021
Cloud Business Process Services (BPaaS)	42.2	46.6	50.3	54.1	58.1
Cloud Application Infrastructure Services (PaaS)	11.9	15.2	18.8	23.0	27.7
Cloud Application Services (SaaS)	58.8	72.2	85.1	98.9	113.1
Cloud Management and Security Services	8.7	10.7	12.5	14.4	16.3
Cloud System Infrastructure Services (IaaS)	23.6	31.0	39.5	49.9	63.0
Total Market	**145.3**	**175.8**	**206.2**	**240.3**	**278.3**

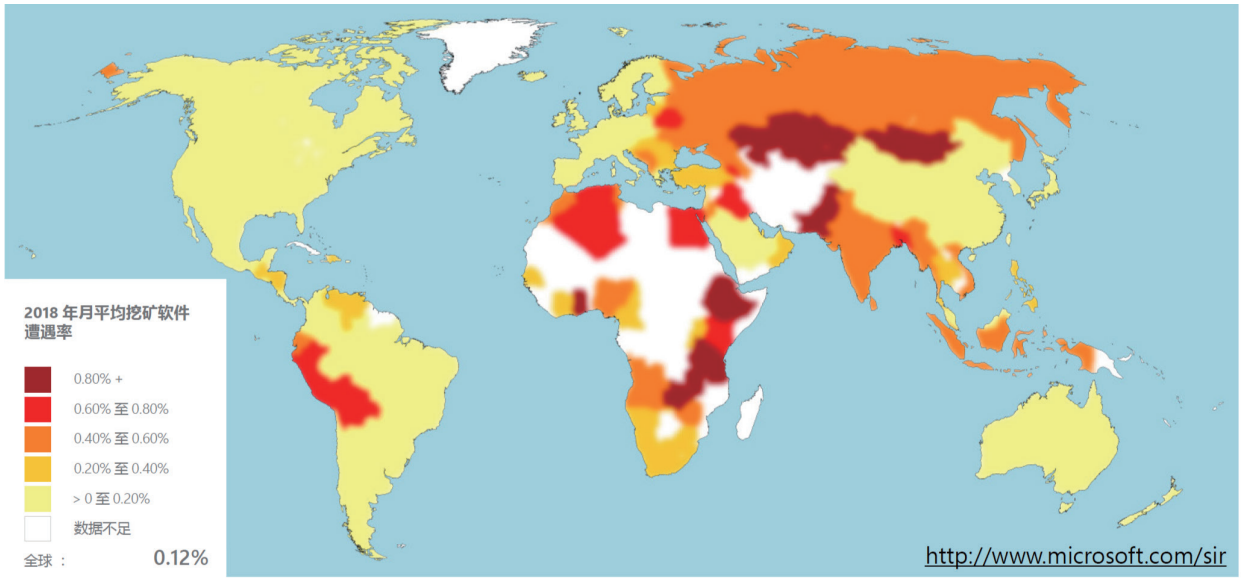
其次，所谓的知己知彼，方能百战百胜，我们再来看看敌方现在的目标是什么？很久以前，我们看到的所谓的黑客，是为了名声，花数月钻研如何攻破像微软，IBM 这样的行业巨头，来让自己扬名立万，就像当年的熊猫烧香病毒一样，名噪一时，但不直接求利；如果继续回想，可能进入脑海中的就是 WannaCry 或者是 Petya 这两者，纯粹的攻击企业或个人的重要服务器或者数据，通过加密的方式，索取比特币作为回报，直截了当。虽然现如今还是会听闻企业时不时地仍旧会遭遇到类似勒索病毒的危害，但到如今两年过去了，在过去的 2018 年、2019 年，我们的对手又在做什么研究呢？

1 https://www.zdnet.com/article/gartner-predicts-saas-revenues-to-reach-85-billion-in-2019/

根据来自“Microsoft 安全情报报告”，再进入 2018 年以后，上述勒索病毒已不再是企业或个人遭受最多的来自恶意软件的攻击。



随着全球数字货币体系的建立，攻击者发现了还有另外一种更为方便的直接获利的方式，就是挖矿：



可以看到，在 2018 年挖矿软件的遭遇率已经是勒索软件的两倍之多。对于攻击者来说，挖矿软件的普遍性使得其攻击成本大大降低，挖矿软件可以通过不同的方式加载到受害者的计算机终端，来为攻击者提供算力进行挖矿。甚至现在市面上已经出现了不需要透过恶意软件渗透到终端进行安装后挖矿，而直接基于游览器的方式，让用户在访问网站的当下，在后台进行挖矿（例如像：Brocoiner）。

又或者是像长久以来的像 Koobface 这样的僵尸病毒所组件的僵尸网络，也从原先提供

DDoS 攻击的业务线，随着数字货币的成型及其在网络市场中的流通性，拓展到为黑色产业链直接提供其所控制的僵尸网络，直接以算力的方式提供给攻击者，攻击者在利用上文提供的各种不同的挖矿木马，用于挖矿。

从整个演变的过程中，其实可以看到，整个产业就像是一个人的成长，从最初刚刚崭露头角的叛逆期，为了制造头条，为了轰动的效应进行攻击，接着进入到刚工作的青年阶段，在为了利的同时，仍旧对于高曝光度有强烈的追求；紧接着产业进入到了成熟期，从产业的运作，流程，盈利模式的成熟，渐渐隐去其自身的光环，转而成为希望闷声发大财的成熟青年。对于攻击到的服务器，现如今他们更希望长期保有对其的控制，不管是为了保持庞大的僵尸网络，来卖个更高的价钱，还是直接进行挖矿，都不希望宿主机上的管理员发现任何异样，导致将其进行物理隔离或者重置。因此在如今的环境下，我们面对的是一个老辣的，喜欢躲在暗处的敌军，攻击方式也从原先的致命一击，转而变成像血蛭或寄生虫中，进行大面积的寄宿攻击。

1.2 企业安全边界的定义

因此，在这样一个企业的环境慢慢从本地往云端转变，攻击手段越来越多样化的大背景下，传统的以服务器为中心的安全框架的搭建，以内网外网区分的安全边界已经无法再像往昔那样，强有力地去掌握企业的安全。那如今，我们该以什么来作为企业全新的安全边界呢？

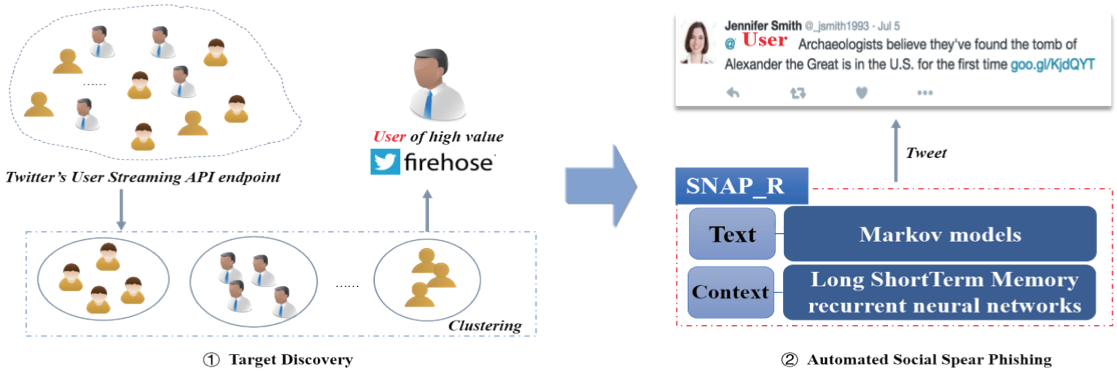
而这样的企业办公环境的变化，其实也带给了以往的攻击者的挑战，试想一下，如果企业不使用任何本地的云环境，而转而使用市场上几大 SaaS，PaaS，IaaS 云厂商的云资源，那从以往已攻破物理机为目的的行为也变得十分困难，攻击目标从原来众多企业自建的数据中心，转而成了各大财力雄厚，数据中心安全系数顶尖的云厂商。所以自然的，攻击者也顺应时代的变化，其攻击目标也发生了改变。

根据微软第 22 期"Microsoft Security Intelligence Report"的统计，微软的 live id 及其企业账号在 2016 年至 2017 年受到的攻击增长了整整 3 倍，来自可疑 IP 的登录事件在该年的第一季度，比同期增长了 44%。

并且随着技术的进步，现如今大数据的应用和体现也已经在所有人的生活中快速渗透着。零售行业中，几乎每一个面向消费者的企业都希望通过其搜集到的用户的信息，进行千人千面的计划，来学习消费者的行为从而刺激消费者进行消费；又或者是餐饮行业的动态发券，针对不同用户的就餐喜好及频率，不断地，在合适的时间，发放给用户合适的券，促成其消费。那同样的，我的疑问就是，这样的一些个人行为的分析模型，攻击者是否也可以进行利用，从而让受害者可以在他期望的时间，期望的地点，点击期望的链接来打开病毒呢？

早在 2016 年的 Black Hat USA 的议题 "Weaponizing data science for social engineering: Automated E2E spear phishing on Twitter"里，研究员 John Seymour 和 Philip Tully 就阐述了

他们在之前的一段时间中做的研究，谁能够更成功地，让 Twitter 的用户点击一个钓鱼的链接，人还是 AI（这里具体指的是 SNAP_R: 递归神经网络模型）。最终时间结果表明，在同样的时间内，AI 可以进行 800 次的尝试，并成功诱导 275 名用户点击钓鱼链接，而同时，人类只能已类似的命中率进行 129 次尝试，成功 49 次。



上述举得基于某个 ID 的行为分析而进行的攻击，其实有一个官方的学名，叫做 Social Engineering Attacks（社会工程攻击），而早在 2014 年，社会工程攻击就已经占到了所有来自于黑客攻击的三分之二之多[2]。时至今日，在很多调查中，很大部分的测试者都愿意在没有确认对方身份的情况下，给出自己的名字和邮箱，甚至在特定的场合下，给出员工号，甚至是代表个人信息的身份证号或者社保号码。

在中国，这样的情况尤甚，大家应该不难发现，在很多的 APP 或者网页端注册的过程中，很多应用在没有给清楚具体的信息使用原因的情况下要求得知注册者的个人可识别信息，或者对接到微信或者是支付宝的账号。正是在这样的大环境下，社会工程攻击者只要针对特定的场景，学习用户的行为，就能轻易得到他们所需要的信息，开启对于企业机密信息的攻击过程。

根据 Microsoft Defender ATP Researcher Team 在 2018 年的抵御报告[3]，在加拿大的 Calgary，发生过只针对本土的公司，总目标不到 100 台虚拟机的社会工程攻击，其攻击方式，是通过某相似的供应商或者服务商的邮箱给这些所在的企业的员工发送一份加密的 PDF 文件。

2 https://www.social-engineer.org/social-engineering/social-engineering-infographic/

3 https://www.microsoft.com/security/blog/2018/06/07/machine-learning-vs-social-engineering/

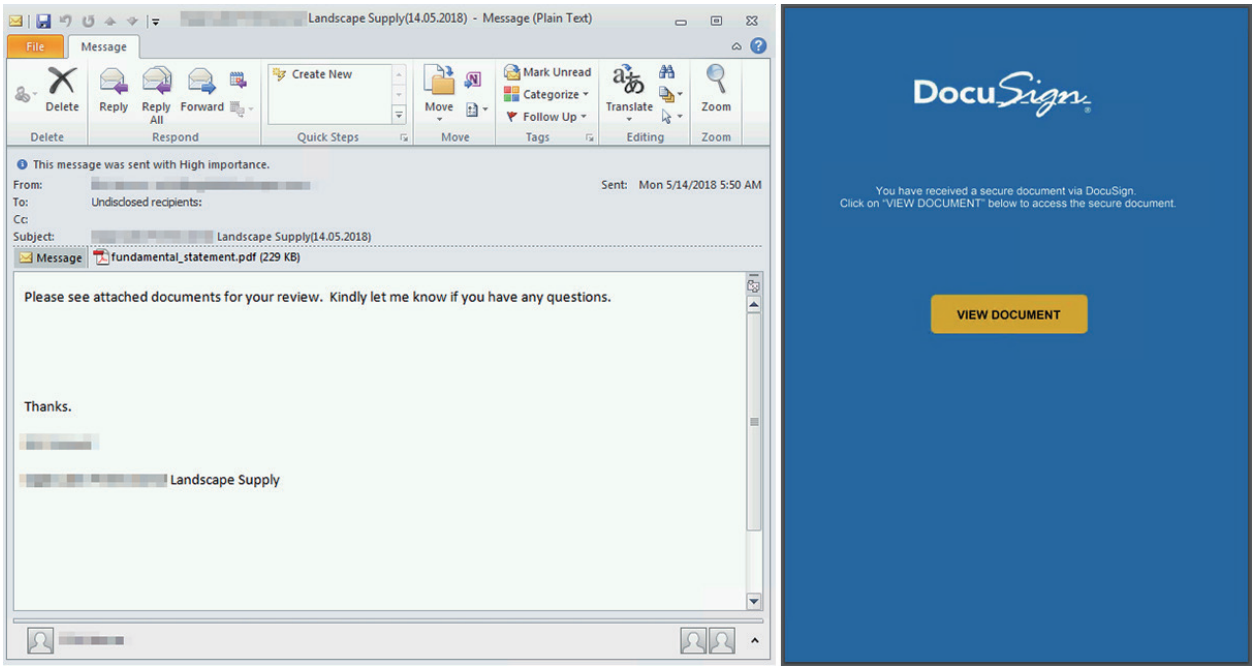


Figure 2: 钓鱼邮件里的加密 PDF 文件

当受害打开了对应的附件，就会登录到一个可疑的站点上，并要求输入企业中的用户名和密码，导致某些用户的凭据的泄露，帮助黑客潜伏在企业中，继续其更深入的渗透和横向移动。

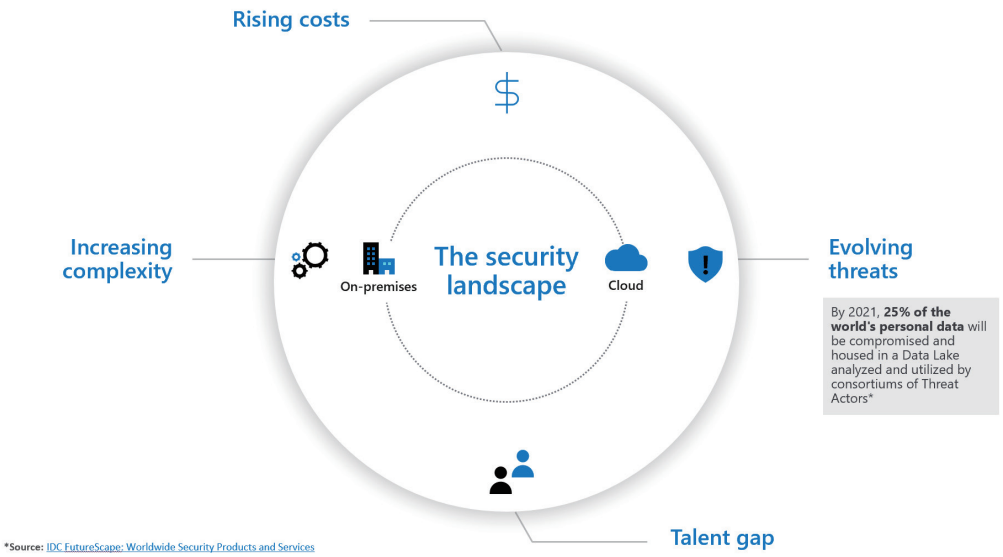
很多时候，这样的钓鱼邮件都会伪装成发票，收据，包裹信息或者是优惠券之类的形式发送到对应的账户中。

而如今，当机器学习的技术遇到了社会工程攻击，攻击者就有了更广阔，更专业的方式来借助用户行为分析进行更精准到用户 ID 的攻击，来对企业发起后续的攻击。因此，在如今的环境下，如何对企业所有员工的账户信息进行加固和防御，成为了企业安全的核心话题，其安全边界，也慢慢从设备或者服务器，转向企业员工的信息进行转移。

1.3 企业自建安全框架面临的挑战

然而，即使企业已经看到了变化， 想要去重组企业的安全框架，他们也将面临一系列严峻的挑战。当他想要针对全新的外部环境和企业内的应用的变化进行安全框架重构时，首先需要考虑的，自然是谁可以单但如此重任。可是这样的一个人选的选择却十分困难。根据网络安全职业调研报告的数据显示[4]，网络安全领域的风投预估，到 2021 年，这个行业的人才缺口将达到 350 万人。随着整个环境中，网络犯罪的暴增，这意味着，预计会在 2021 年造成全球 6 万亿美金的损失。全球各地，像美国商务部，或来自欧洲信息安全认证机构（ISC）2 的调研结果等，都继续安全人才的加入。

4 https://cybersecurityventures.com/jobs/



其次，从产品角度来看，企业如何保证安全方案的有效落地也需要面对重重困难：

从最基础的终端设备的防护说起，加固宿主机，补丁升级，保持软件时刻最新，另外还有防火墙的配置，杀毒软件的选择，访问控制机制的设定，这些就会占据 IT 很大一部分的精力。

然而，在现实中，面对一直在迭代，推陈出新的威胁，仅仅依靠单一的某种安全组件，例如杀毒软件，或者网关等，已经远远不够了。由于各种保护工具来自不同的供应商，并且没有互操作性标准，因此几乎很难去快速地做出协调的响应。例如，如果想要阻止 Nimda 蠕虫的传播，就需要企业从防病毒软件、入侵防护和防火墙三个维度，讲出现地异常情况汇总分析，才能真正找出是何种病毒造成的影响。

以及，为了应对今后其他威胁的防范，企业安全框架的可伸缩性又是另一个值得关注的问题。企业如果希望可以应对持续增加的威胁，那就需要扩大特定类别攻击（例如蠕虫和病毒签名）的知识库的规模，例如需要当前体系结构下的产品能够不断扩展其数据库。而不希望像目前可用的大多数多功能安全设备那样，只能处理一组有限的 IPS/IDS 签名或 URL。伸缩性除了指的是平台硬件或应用层面，容量的可伸缩性，还有另一个方案就是其安全功能的可伸缩性，这个平台或者应用程序是否可以扩展新型的威胁检查或者防御机制来应对全新的威胁。

因此，如果企业希望想去搭建一套完备的安全平台，那需要去衡量其在人力招收上的成本投入，产品选型上的风险，以及平台应对未来的不确定性等各个因素，这样的一个平台的成功，将不仅仅只是依赖于企业投入的资金的多少。

Chapter 2

搭建企业级应用环境安全框架

2.1 安全加固应用环境

2.1.1 网络安全

微软对安全的重视遍布到每一个细小环节，从代码开发到对事件的响应都会投入大量安全防护措施，充分保障 Azure 资源的安全性。我们都是知道，全球范围内网络攻击每时每刻都在发生，保障网络安全离不开产品及使用者的共同努力。Azure 始终为用户提供一套全面的且易操作的安全防护体系供。我们认为如果把一个问题变得复杂，人们往往会选择绕开它，所以 Azure 每年在安全问题上投资超过 10 亿美金，推出多种 AI 和自动化的安全防护产品和服务[5]。

在 Azure 上，用户需要将资源部署在 Azure 虚拟网络（VNet）中。Azure 虚拟网络是一个构建于 Azure 物理网络结构上的逻辑结构，每个虚拟网络之间默认相互隔离，从而保障不同用户之间资源与网络流量的隔离。用户可以像管理内部网络一样，控制虚拟网络的 IP 地址块、DNS 配置、安全策略和路由表；还可以通过网络安全组、VPN 网关或网络专线 ExpressRoute 来控制虚拟网络的访问权限。除了对网络访问的控制之外，我们还需要针对各种网络安全威胁，进行安全防护，例如配置 Azure 防火墙、应用程序防火墙、DDoS 防护等。

（1）网络安全组（NSG）

配置严格的网络访问权限，是最简单直接的防范网络攻击，屏蔽恶意流量的方式。所以第一步，为 Azure 中的资源进行网络访问控制。网络安全组（Network Security Group, NSG）是一种静态数据包筛选防火墙，提供基本的网络级别访问控制（基于 IP 地址和 TCP 或 UDP 协议）。用户通过使用网络安全组，可以简化管理，减少配置错误的可能性。

网络安全组可以用来筛选 Azure 虚拟网络中出入 Azure 资源的网络流量。用户可以通过配置网络安全组规则自定义网络流量的筛选条件，通过规则实现允许或拒绝多种 Azure 资源的入站和出站网络流量。可以使用五元组信息（源 IP、源端口、目标、目标端口和协议）来配置安全规则[6]，如果通信是从外部发起的，则只需指定入站安全规则，反之亦然。为了最大程序简化安全规则的配置流程，可以通过以下方式对一组应用相同安全规则的资源 IP 进行整合，然后创建一条网络安全组规则实现对一组资源的安全访问控制。

- 扩充安全规则：可以在一条规则中同时指定多个端口和多个显式 IP 地址。
- 服务标记：服务标记是 Microsoft 标签，表示一组 IP 地址。例如，如果用户希望

5 https://www.microsoft.com/en-us/security

6 配置 NSG 参考 https://docs.microsoft.com/zh-cn/azure/virtual-network/tutorial-filter-network-traffic

为 EastUS 中使用的 Azure 存储服务创建一条安全组规则，可以直接使用"Storage.EastUS"这条服务标记来表示，且该标记会根据用户使用的 Azure 存储服务动态更新。

- 应用程序安全组：也是用来表示一组 IP 地址，例如用户可以创建一个"Webservers"应用程序安全组名称，然后把 Web 服务器部署到"Webservers"中，通过创建一个安全规则进行统一的访问控制管理。不能向同一应用程序安全组添加来自不同虚拟网络的网络接口。

默认安全组入站规则：

- 默认允许来自虚拟网络中的资源入站流量

AllowVNetInBound

Priority	Source	源端口	目标	目标端口	Protocol	访问权限
65000	VirtualNetwork	0-65535	VirtualNetwork	0-65535	任意	Allow

- 默认允许所有来自负载均衡器（LB）的流量入站

AllowAzureLoadBalancerInBound

Priority	Source	源端口	目标	目标端口	Protocol	访问权限
65001	AzureLoadBalancer	0-65535	0.0.0.0/0	0-65535	任意	Allow

- 默认拒绝来自其他（Internet，其他未打通的虚拟网络）资源的入站

DenyAllInbound

Priority	Source	源端口	目标	目标端口	Protocol	访问权限
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	任意	拒绝

默认安全组出站规则：

- 默认允许向虚拟网络内部资源的出站流量

AllowVnetOutBound

Priority	Source	源端口	目标	目标端口	Protocol	访问权限
65000	VirtualNetwork	0-65535	VirtualNetwork	0-65535	任意	Allow

- 默认允许虚拟网络中的资源向 Internet 的出站流量

AllowInternetOutBound

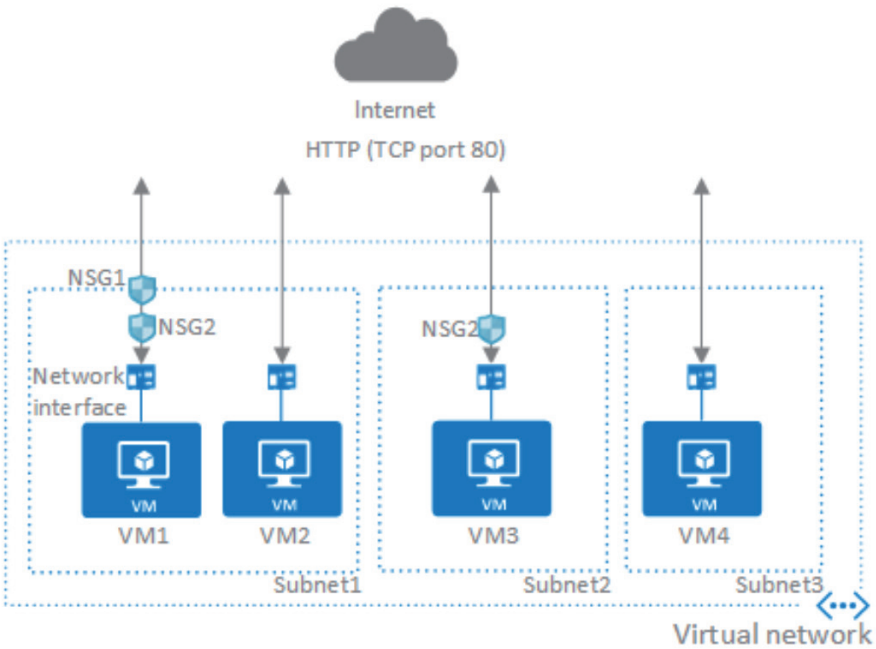
Priority	Source	源端口	目标	目标端口	Protocol	访问权限
65001	0.0.0.0/0	0-65535	Internet	0-65535	任意	Allow

- 默认拒绝其他情况的出站流量

DenyAllOutBound

Priority	Source	源端口	目标	目标端口	Protocol	访问权限
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	任意	拒绝

在 Azure 虚拟网络中，网络安全组（NSG）可以与虚拟网络子网（subnet）关联，同时也可以与子网中具体的网卡（NIC）相关联，二者可以同时存在。在同时配置时，要避免二者冲突。例如[7]：



对于入站流量，Azure 先处理与某个子网相关联的网络安全组中的规则，然后处理与网络接口相关联的网络安全组中的规则。

- VM1：VM1 位于 Subnet1 中，Subnet1 有与之相关联网络安全组 NSG1，系统会先处理 NSG1 中的安全规则。NSG1 中如果用户事先自定义创建了一条允许端口 80 入站流量的规则，则流量可以进入 Subnet1，否则流量会被 DenyAllInbound 默认安全规则拒绝，无法进入 Subnet1。NSG1 有一条允许端口 80 的安全规则，则流量会进一步由 与 VM1 网卡相关联的 NSG2 处理。 若要允许从端口 80 到虚拟机的流量，NSG1 和 NSG2 都要配置一条允许从 Internet 访问 VM 80 端口的安全规则。
- VM2：因为 VM2 也在 Subnet1 中，系统会处理 NSG1 中的规则。 VM2 没有关联到其网络接口的网络安全组，因此会接收 NSG1 所允许的所有流量，或者会拒绝 NSG1 所拒绝的所有流量。 当网络安全组关联到子网时，对于同一子网中的所有资源，流量

7 https://docs.microsoft.com/zh-cn/azure/virtual-network/security-overview

要么被允许，要么被拒绝。

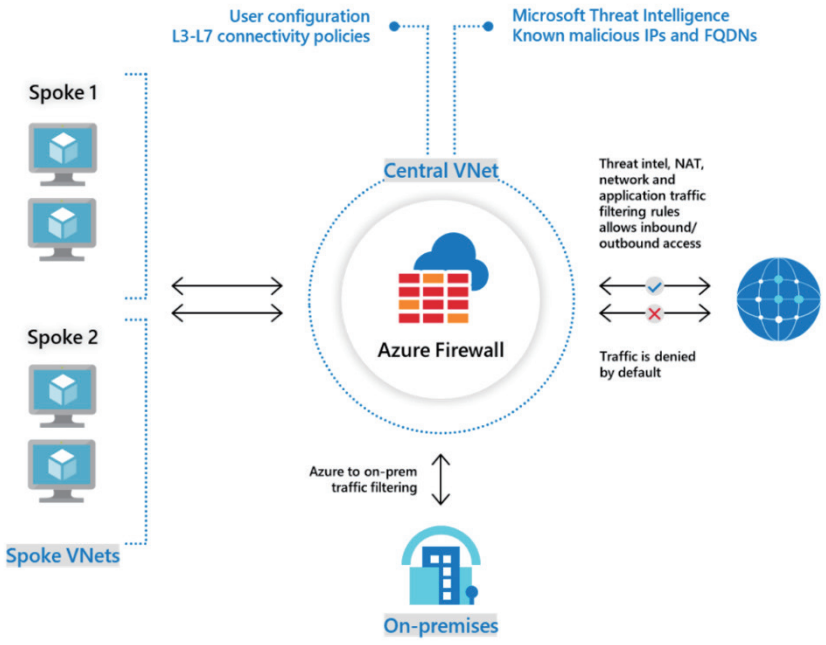
- VM3：由于没有网络安全组关联到 Subnet2，系统允许流量进入子网并直接由与 VM3 网卡相关联的 NSG2 处理。
- VM4：允许流量发往 VM4，因为网络安全组没有关联到 Subnet3 或虚拟机中的网络接口。 如果没有关联的网络安全组，则允许所有网络流量通过子网和网络接口。

对于出站流量，Azure 先处理与某个网络接口相关联的网络安全组中的规则，然后处理与子网相关联的网络安全组中的规则。

- VM1：系统会处理 NSG2 中的安全规则。 除非创建一条安全规则来拒绝从端口 80 到 Internet 的出站流量，否则 NSG1 和 NSG2 中的 AllowInternetOutbound 默认安全规则都会允许该流量。 如果 NSG2 有一条拒绝端口 80 的安全规则，则流量会被拒绝，不会由 NSG1 评估。 若要拒绝从虚拟机到端口 80 的流量，则两个网络安全组或其中的一个必须有一条规则来拒绝从端口 80 到 Internet 的流量。
- VM2：所有流量都会通过网络接口发送到子网，因为附加到 VM2 的网络接口没有关联的网络安全组。 系统会处理 NSG1 中的规则。
- VM3：如果 NSG2 有一条拒绝端口 80 的安全规则，则流量会被拒绝。 如果 NSG2 有一条允许端口 80 的安全规则，则允许从端口 80 到 Internet 的出站流量，因为没有关联到 Subnet2 的网络安全组。
- VM4：允许来自 VM4 的所有网络流量，因为网络安全组没有关联到已附加到虚拟机的网络接口，或者没有关联到 Subnet3。

（2）Azure 防火墙

Azure 防火墙为网络安全组（NSG）功能提供了补充，为构建网络安全环境提供了更好的 “深层防御”。网络安全组提供分布式网络层流量过滤，以限制每个订阅中虚拟网络内资源的访问流量。如果用户需要跨订阅，跨虚拟网络，启用某些应用程序级别的保护时，则需要使用 Azure 防火墙服务。Azure 防火墙是一个服务形式的完全有状态的集中式网络防火墙，具有内置的高可用性和不受限制的可伸缩性。



Azure 防火墙主要功能有[8]：

- 内置的高可用性，Azure 防火墙内置了高可用架构，用户不需要配置额外的负载均衡器，也不需要进行任何配置，减少用户的使用成本。
- 不受限制的云可伸缩性，Azure 防火墙服务可以很好的适应不断变化的网络流量，最大程度实现纵向扩展，因此不需要为峰值流量做出预算。
- 应用程序 FQDN 筛选规则：Azure 防火墙可将出站 HTTP/S 流量或 Azure SQL 流量（Preview）限制到指定的一组完全限定的域名（FQDN），此功能不需要 SSL 终止。
- 网络流量筛选规则：可以根据源和目的 IP 地址、端口和协议，集中创建"允许"或"拒绝"网络筛选规则。Azure 防火墙是完全有状态的，因此它能区分不同类型的连接的合法数据包，将跨多个订阅和虚拟网络实施与记录规则。还可以使用 FQDN 标记、服务标记配置筛选规则。
- 支持源和目的网络地址转换（SNAT 和 DNAT）
- 与 Azure Monitor 完全集成，使用户能够在存储账户中存档日志，并将事件流式传输到实践中心，或者将其发送到 Azure Monitor 日志。
- 支持混合部署，可以在 VPN 和 ExpressRoute 网关后部署 Azure 防火墙。

（3）Web 应用程序防火墙（WAF）

Azure 防火墙为非 HTTP/S 协议（例如 RDP\SSH\FTP 协议）提供入站保护，为所有端口和协议提供出站网络级别的保护，所以如果用户需要为 HTTP/S 协议提供入站保护，需要使用 Web 应用程序防火墙（WAF）。

Web 应用程序防火墙（WAF）是应用程序网关的一项功能，可在出现常见攻击和漏洞时

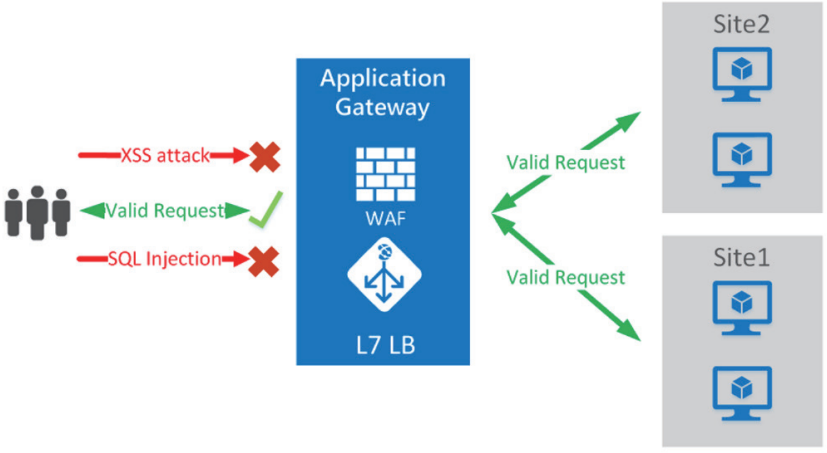
8 https://docs.microsoft.com/zh-cn/azure/firewall/overview

为 Web 应用程序提供集中的入站保护。

Azure 应用程序网关通过 Web 应用程序防火墙 (WAF) 在 Region 内部集中保护 Web 应用程序，使其免受常见攻击和漏洞的侵害。如果用户希望跨 Region 进行全球范围内 Web 应用程序防护，可以使用 Azure Front Door 中的 Web 应用程序防火墙功能[9]。

Web 应用程序正逐渐成为利用常见已知漏洞的恶意攻击的目标。 最常见的攻击包括 SQL 注入和跨站点脚本。防止应用程序代码遭受此类攻击颇具挑战性。 这可能需要对应用程序拓扑的多个层进行严格的维护、修补和监视。 集中式 Web 应用程序防火墙有助于大幅简化安全管理。 WAF 还能为抵卸威胁和入侵的应用程序管理员提供更好的保障。

相较保护每个单独的 Web 应用程序，WAF 解决方案可以通过集中修补已知漏洞，更快地对安全威胁做出反应。 可将现有应用程序网关轻松转换为支持防火墙的应用程序网关。

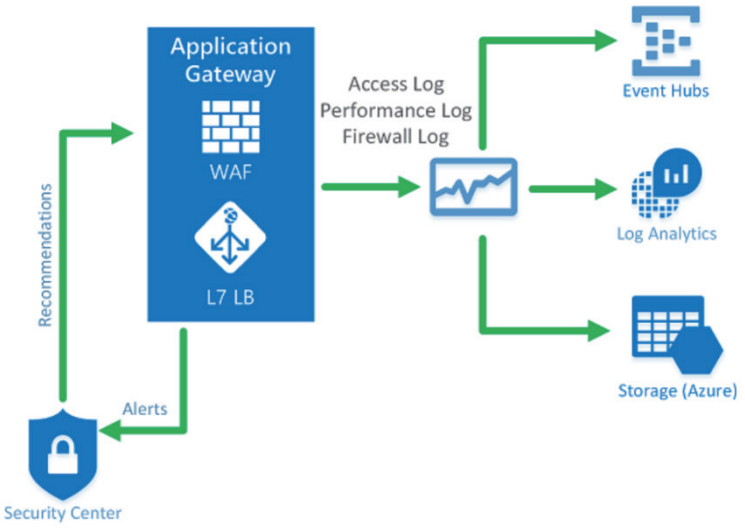


应用程序网关以应用程序传送控制器 (ADC) 的形式运行。 它提供安全套接字层 (SSL) 终止、基于 Cookie 的会话相关性、轮循负载分配、基于内容的路由，以及托管多个网站和安全增强功能的能力。

应用程序网关安全增强功能包括 SSL 策略管理和端到端 SSL 支持。 WAF 与应用程序网关集成，使应用程序的安全性得到增强。 这种组合可使 Web 应用程序免受常见漏洞的威胁。应用程序网关 WAF 已与 Azure 安全中心（Security Center）集成。 在安全中心可以集中查看所有 Azure 资源的安全状态。监视应用程序网关的运行状况非常重要。 将 WAF 与 Azure 安全中心、Azure Monitor 和 Azure Monitor 日志集成后，可以监视 WAF 及其保护的应用程序的运行状况[10]。

9 https://docs.microsoft.com/zh-cn/azure/frontdoor/front-door-faq

10 https://docs.azure.cn/zh-cn/application-gateway/waf-overview



（4）安全远程访问和跨界连接

除了 Azure 云上资源的安全防护之外，为了更好帮助混合部署的场景，Azure 提供了多种安全远程访问的连接方式——VPN 和 ExpressRoute。

VPN 网关用于在 Azure 虚拟网络与本地位置之间，以及 Azure 虚拟网络之间跨公共 Internet 发送加密流量。ExpressRoute 连接不通过公共 Internet，与通过 Internet 的连接相比，ExpressRoute 连接提供更高的可靠性、更快的速度、更低的延迟和更高的安全性。

➢ VPN 网关 SKU[11]：

VPN 网关 SKU：Basic、VpnGw1、VpnGw2、VpnGw3。可以根据工作负荷、吞吐量、功能和 SLA 的类型，选择满足需求的 SKU。

SKU	S2S/VNet 到 VNet 隧道	P2S SSTP 连接	P2S IKEv2 连接	聚合吞吐量基准	BGP
Basic	最大 10	最大 128	不支持	100 Mbps	不支持
VpnGw1	最大 30*	最大 128	最大 250	650 Mbps	支持
VpnGw2	最大 30*	最大 128	最大 500	1 Gbps	支持
VpnGw3	最大 30*	最大 128	最大 1000	1.25 Gbps	支持

这四种类型均支持 RouteBased VPN，但只有基本 SKU 支持 PolicyBased VPN。

基本 SKU 被视为旧版 SKU，它具有某些功能限制。使用基本 SKU 的网关无法直接调整为新网关 SKU 中的一种。在 ARM 部署模式下，如果希望从旧版 SKU 更改为新版 SKU，需删除

11 https://docs.microsoft.com/zh-cn/azure/vpn-gateway/vpn-gateway-about-vpngateways

现有 VPN 网关并创建新的 VPN 网关。此外，基本 SKU VPN 网关不支持点到站点连接（P2S），且站点到站点（S2S）的连接数只能有一个，也不支持边界网关协议（BGP）路由。
使用 VpnGw1、VpnGw2、VpnGw3 这三种新版 SKU，创建之后可以根据需要在这三种 SKU 之间对 VPN 网关的 SKU 进行更改。
在关键工作负荷中建议用户使用 VpnGw1、VpnGw2 和 VpnGw3 这三种 VPN 网关 SKU。

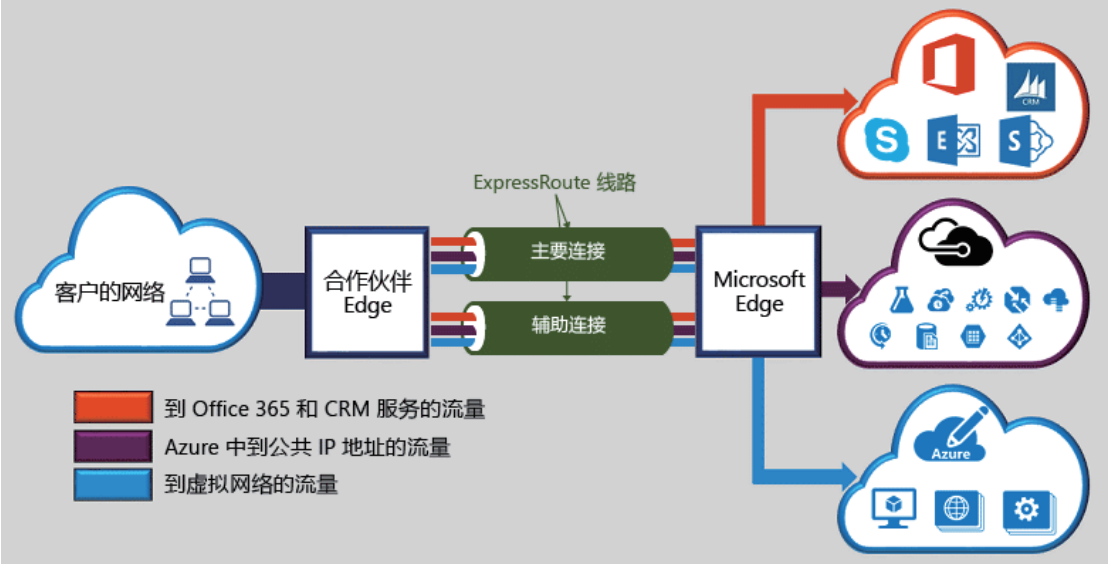
- ExpressRoute 网关 SKU：标准、高性能、超高性能[12]

如果希望使用专线在 Azure 虚拟网络和本地位置之间发送网络流量，在创建虚拟网络网关时，选择网关类型为“ExpressRoute”。

如果选择更高级别的网关 SKU，则为该网关分配更多的 CPU 和网络带宽，这样使网关能够支持到虚拟网络更高的吞吐量。

创建 ER 网关之后在标准和高性能 SKU 之间可以进行升级，若要升级到超高性能 SKU，需要重新创建网关，重新创建网关会导致停机。

ExpressRoute 线路支持多种带宽，可以在不中断连接的情况下增大 ExpressRoute 线路带宽。每个 ExpressRoute 线路有两道连接，用于从连接服务提供商 / 网络边缘连接到两个 Azure 企业边缘路由器（MSEE）。Azure 要求通过连接服务提供商 / 网络边缘建立双重 BGP 连接——各自连接到每个 MSEE。可以选择不要在一端部署冗余设备 / 以太网路线。但是，连接服务提供商会使用冗余设备，确保以冗余方式将连接移交给 Azure。冗余的第 3 层连接配置是 Azure SLA 生效的条件。



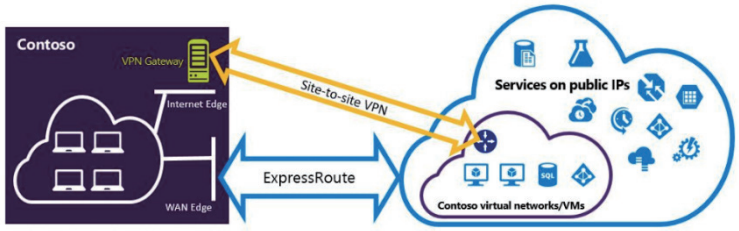
在介绍 VPN 网关时讲到，虚拟网络只能有一个 VPN 网关。同理，虚拟网络也只能有一个 ExpressRoute 网关，二者可以共存。也就是说，能够为同一虚拟网络配置 S2S 的 VPN 网关

12 https://docs.azure.cn/zh-cn/expressroute/expressroute-introduction

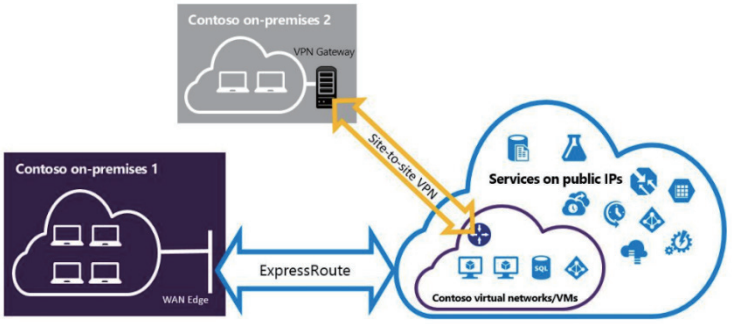
和 ExpressRoute 网关。

配置站点到站点 VPN 和 ExpressRoute 具有多项优势：

- 可以将站点到站点 VPN 配置为 ExpressRoute 的安全故障转移路径



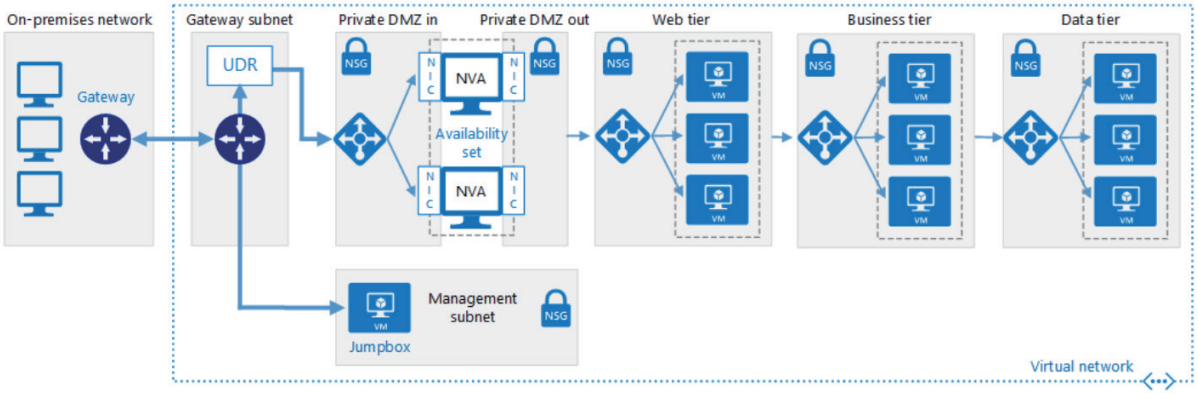
- 也可以从同一站点分别使用 VPN 和 ExpressRoute 连接到不同的站点



（5）外围网络架构

➢ Azure 与本地之间的外围网络

本地网络与 Azure 虚拟网络 (VNet) 之间实现一个 DMZ（也称为外围网络）。 DMZ 包括防火墙和数据包检查等实现安全功能的网络虚拟设备 (NVA)。 来自 VNet 的所有传出流量都通过本地网络强制隧道传输到 Internet，以便可以进行审核。



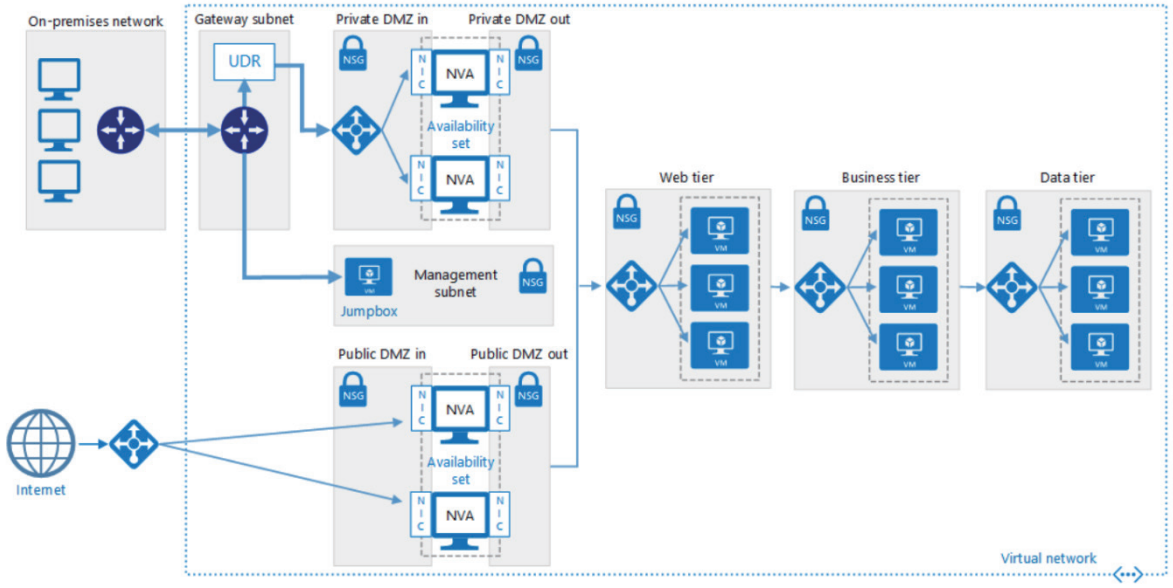
该体系结构包括以下组件。

- 本地网络： 本地实现的专用局域网。
- Azure 虚拟网络 (VNet)： VNet 承载 Azure 中运行的应用程序和其他资源。
- 网关： 网关为本地网络与 VNet 之间提供连接。

- 网络虚拟设备 (NVA)： NVA 是一种通用术语，用于描述执行诸如允许或拒绝访问（作为防火墙）、优化广域网 (WAN) 操作（包括网络压缩）、自定义路由或其他网络功能这类任务的 VM。
- Web 层、业务层和数据层子网：承载在云中运行的各种 VM 服务器。
- 用户定义的路由 (UDR)： 用户定义的路由定义 Azure vnet 中的 IP 流量流。

➢ Azure 与 Internet 之间的外围网络[13]

此参考体系结构扩展了在 Azure 和本地数据中心之间实现外围网络中所述的体系结构。 它添加了一个用于处理 Internet 流量的公共外围网络，以及一个用于处理来自本地网络的流量的专用外围网络。



该体系结构包括以下组件。

- 公共 IP 地址 (PIP)： 公共终结点的 IP 地址。 连接到 Internet 的外部用户可通过此地址访问系统。
- 网络虚拟设备 (NVA)： 此体系结构包含一个用于处理源自 Internet 的流量的独立 NVA 池。
- Azure 负载均衡器：来自 Internet 的所有传入请求通过负载均衡器，并分发到公共外围网络中的 NVA。
- 公共外围网络入站子网：此子网接受来自 Azure 负载均衡器的请求。 传入的请求传递到公共外围网络中某个 NVA。

13 https://docs.microsoft.com/zh-cn/azure/architecture/reference-architectures/dmz/secure-vnet-hybrid

- 公共外围网络出站子网： NVA 允许的请求通过此子网传递到 Web 层的内部负载均衡器。

（6）Azure DDoS 防护 [14]

分布式拒绝服务 DDoS 攻击是一种常见的也是危害较大的网络攻击方式，其攻击类型多样，对网络安全防护措施也要求比较高。Azure 平台本身启用了基本的 DDoS 防护功能，持续监测网络中的异常流量，实时进行风险防护，为 Azure 平台上的用户资源提供实时保护。如果用户希望特别针对自身虚拟网络中的资源进行 DDoS 网络安全防护，可以采用标准版 DDoS 防护功能。

Feature	DDoS Protection Basic	DDoS Protection Standard
Active traffic monitoring & always on detection	Yes	Yes
Automatic attack mitigations	Yes	Yes
Availability guarantee	Azure region	Application
Mitigation policies	Tuned for Azure region traffic volume	Tuned for application traffic volume
Metrics & alerts	No	Real time attack metrics & diagnostic logs via Azure monitor
Mitigation reports	No	Post attack mitigation reports
Mitigation flow logs	No	NRT log stream for SIEM integration
Mitigation policy customizations	No	Engage DDoS experts
Support	Best effort	Access to DDoS Experts during an active attack
SLA	Azure region	Application SLA guarantee & cost protection
Pricing	Free	Monthly & usage based

标准版 DDoS 防护易于启用，无需更改应用程序，通过专用流量监测和机器学习算法优化保护策略。策略应用到与部署虚拟网络中资源相关的公共 IP 地址，例如 Azure 负载均衡器、Azure 应用程序网络和 Azure Service Fabric 实例。对于应用服务网络安全防护更加复杂多变，因此可以将标准 DDoS 防护与 Azure 应用程序网关、Web 应用程序防火墙结合使用，实现从第 3 层到第 7 层完整的 DDoS 安全防护功能。标准版 DDoS 防护可以为用户虚拟网络中的资源提供更为全面的保障，主要防护的攻击类型可分为以下几类：

- 容量耗尽攻击：借助看似合法的流量涌入网络层，如 UDP 数据包洪水，造成服务器容量耗尽使合法用户无法进行正常访问，引起服务器宕机业务中断。借助 Azure 的全球网络规模，标准 DDoS 防护可以自动吸收和清理这些潜在的数千兆字节的攻击，从而为用户自身的网络资源提供保护。
- 协议攻击：通过利用第 3 层和第 4 层网络协议对目标发起攻击，如 SYN 泛洪、反射攻击，同样会造成目标主机无法访问。标准 DDoS 防护通过与客户端交互来区分恶意流量和合法流量并阻止恶意流量，从而缓解这些攻击。
- 应用程序层的攻击：这些攻击利用 Web 应用程序数据包来中断主机之间的数据传输，

14 https://docs.microsoft.com/zh-cn/azure/virtual-network/ddos-protection-overview

如 HTTP 协议冲突、SQL 注入，可以与 Azure 应用程序网关、Web 应用程序防火墙配合使用，实现更全面的安全防护保障。

标准 DDoS 防护功能已防护超过 60 种已知的攻击类型，与 Web 应用程序防火墙配合使用时，可以提供完整的堆栈 DDoS 保护。

标准 DDoS 防护通过监测实际流量利用率，并不断将其与 DDoS 策略中定义的阈值进行比较，当超过流量阈值时，Azure 自动启用 DDoS 防护策略。标准 DDoS 防护为用户提供自适应的优化策略，当流量随时间变化时，配置文件将自动进行调整。在风险缓解期间，

- 标准 DDoS 防护服务将受保护资源的入站流量进行重定向，执行进一步检查。
- 检查数据包是否符合 Internet 规范且格式正确；与客户端进行交互确定该流量是否可能是欺骗性的数据包；如果没有其他可以执行的强制方法，将对数据包进行速率限制。
- 标准 DDoS 防护服务还提供受到攻击期间详细的增量报告，将日志实时传输到离线安全信息和事件管理（SIEM）系统，以便在攻击期间进行实时监测。攻击结束后用户会收到完整的事件摘要。

可以在 Azure Monitor 查看每个攻击的汇总指标，并配置预警功能。Microsoft 已与 BreakingPoint Cloud 合作构建接口，用户可在其中针对已启用 DDoS 保护的公共 IP 地址生成模拟的流量。 借助 BreakPoint Cloud 模拟，您可以：

- 验证 Microsoft Azure DDoS 防护标准如何保护 Azure 资源免受 DDoS 攻击
- 受到 DDoS 攻击时如何优化事件响应过程
- 查看 DDoS 防护的合规性
- 帮助用户培训网络安全团队

（6）总结与补充

针对上述所介绍的 Azure 网络防护功能，进行如下总结与补充

安全防护位置	边界	连接方式	安全措施
虚拟网络内部	子网 / 网卡	VNet 内部路由	NSG/ASG
虚拟网络之间	虚拟网络	VNet Peering	Azure 防火墙
Container pods	Container pods	Azure 内部路由	Kubernetes Policies
PaaS 服务	PaaS 服务账户	服务终结点	服务终结点策略 /Azure 防火墙 FQDN 筛选
与 Internet 交互位置	应用程序边界	Internet 连接	应用程序防火墙（WAF）/ DDoS 防护

➢ 虚拟网络内部

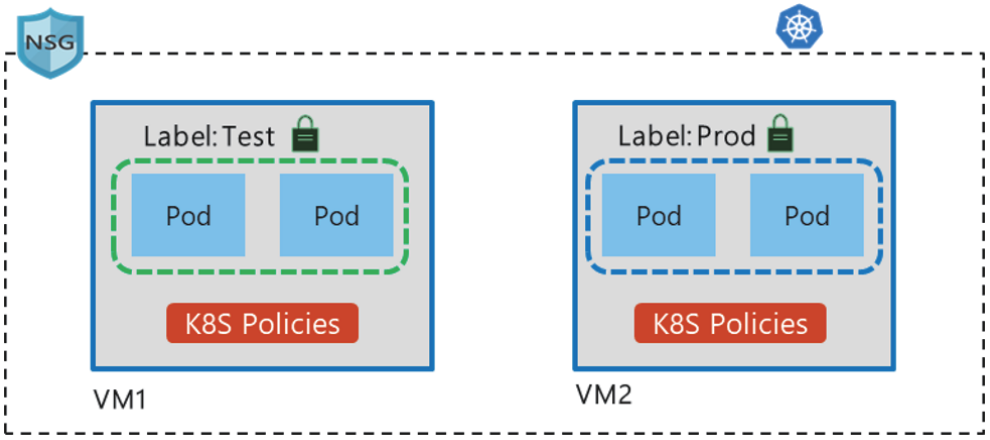
可以使用子网或应用程序标签在 vnet 中划分应用程序组件。通过使用网络安全组或应用程序安全组来控制资源之间的流量访问。这种方式可用于虚拟网络中任何类型的工作负载（例如 Windows、Linux VMs）；无需安装任何软件；可以与 Azure DevOps 工具链集成；可以使用 Azure Monitor 查看安全访问报告；还可以通过 Azure 安全中心管理 NSG 策略的合规性。

- 虚拟网络之间

可以将多个 VNet 与一个 Hub VNet 建立对等互联，通过将 Azure 防火墙部署在 Hub VNet 中来实施某些安全策略用于控制 VNet 之间的流量转发以及 VNet 与外部 Internet 或本地数据中心流量转发。Azure 防火墙的方式能够集成管理三层到七层网络的连接策略。

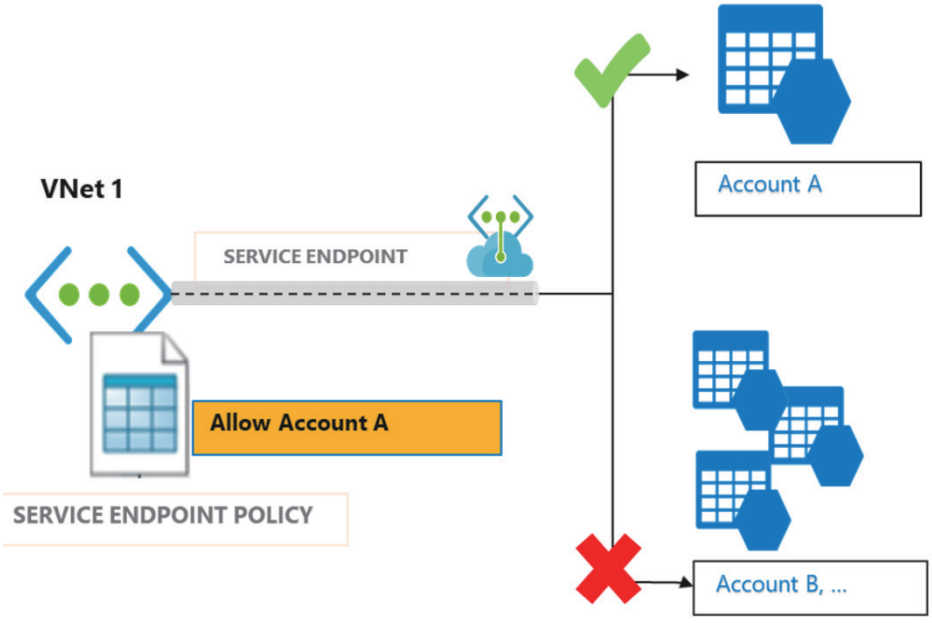
- container pods

与上述两个场景相补充的是 Azure 对容器化应用程序进行 pod 级安全防护的能力。这些 pod 片段之间的连接可以通过 Azure Kubernetes 服务策略进行管理。



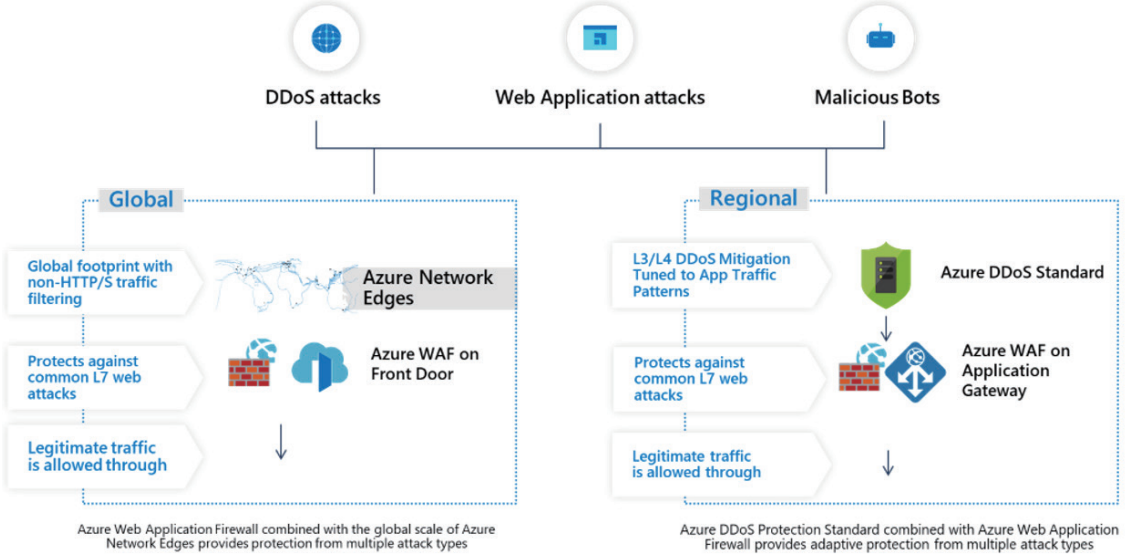
- PaaS 服务

PaaS 服务在虚拟网络内部默认可以进行访问。通过使用服务终结点可以限制虚拟网络对 PaaS 服务的访问权限，可以通过策略对某些特定的 PaaS 服务账户进行访问权限的控制。



➢ 与 Internet 交互位置

与 Internet 进行交互的边界位置容易受到各种网络攻击，例如应用程序攻击，恶意机器人攻击、DDoS 攻击等。用户可以使用应用程序防火墙（WAF）来抵御来自全球范围内或 Region 内部的针对应用程序层的攻击。在 Region 内部还可以通过 Azure 标准 DDoS 防护加强网络安全。



2.1.2 虚拟机安全（Windows & Linux）

在大多数基础结构即服务（IaaS）方案中，虚拟机 (VM) 仍是云计算用户最常用的资源。

毫无疑问，保证虚拟机的安全是 Microsoft Azure 的重中之重——保护好虚拟机的安全，也就确保了业务的稳定。就像大家所熟知的名为 Lilocked 的 Linux 勒索病毒，该勒索病毒针对 Linux 主机，使用了未公开的漏洞将自身提升为 root 权限后加密文件，并勒索比特币[15]。假设有恶意流量（如类似 Lilocked 的勒索病毒、挖矿软件等）对 Azure 某虚拟机进行攻击，表现为 Azure 门户的 Dashboard 上该虚拟机流量异常高或收到了监控警报。本节介绍并阐述多种可用于虚拟机和操作系统的核心 Azure 安全功能与最佳实践，通过合理使用 Azure 安全功能，将恶意软件、勒索病毒等拒之门外。

在恶意流量进入 Azure 虚拟网络前，Azure 平台即实施了物理层面的 DDos 保护和服务终结点。当流量进入虚拟网络并通过了设置的安全保护措施如流量隔离、NSG、UDR/IP 转发等之后，在虚拟机层面 Azure 提供的多种安全防护功能将发挥作用。使用 Azure 可以构建安全增强且符合法规的解决方案，包括但不限于：

- 保护虚拟机不受病毒和恶意软件的侵害
- 加密敏感数据
- 保护网络流量的安全
- 识别和检测威胁

(1) 虚拟机的安全加固

系统作为最终承载用户应用的环境，是最后一道攻破应用的安全防线，需要进行严谨的设计和管理，特别是公有云环境中的系统。云服务管理员对其 IaaS 的虚拟机及其他产品享有完全的控制权，因此也需要负责虚拟机及其上层的数据安全。针对前文提到的勒索病毒或者一些攻击，为了保护虚拟机的数据安全，避免不必要的异常流量，云服务管理员可以参照如下建议，对虚拟机加强安全防护：

- 尽量不要使用 root 权限运行 Web 应用程序，或直接禁止 root 账号登录虚拟机
- 增加密码的复杂度
- 修改 SSH/RDP 端口为非默认端口
- 使用证书登录
- 限制 IP 登录
- 在虚拟机内部部署防火墙或第三方防护工具，设置服务允许拒绝规则等，防止非法的访问。在 Linux 上，可以通过 tcp_wrappers 等实现
- 根据最少服务原则，在安装配置系统时，安装应用需要的最少的包，开启最少的服务
- 通过跳板机（Jumpbox）进行内部访问，特别是数据库和重要的业务服务器
- 及时打上重要的补丁，防止应用程序被漏洞利用入侵

15 深信服千里目安全实验室，“数千台 Linux 主机被勒索，该如何打好防御战？” https://www.freebuf.com/articles/system/214395.html

- Linux 虚拟机 - 开启 SELinux、AppArmor 等功能保护重要文件
- Linux 虚拟机 - 用户登录通知
- Linux 虚拟机 – 安全审计

(2) 通过身份验证和访问控制保护 VM

保护 VM 安全的关键因素是确保只有授权用户才能设置新 VM 以及访问 VM。若要提高 Azure 上的 Linux Vm 的安全性，降低人为引起的安全风险，可以与 Azure AD 身份验证集成。 将 Azure AD 身份验证用于 Linux vm 时，可以集中控制和强制允许或拒绝访问 VM 的策略。

最佳实践	详细信息
控制 VM 访问	使用 Azure 策略建立组织中的资源约定和创建自定义策略。 将这些策略应用于资源，如资源组。 属于该资源组的 VM 将继承该组的策略。 如果你的组织有多个订阅，则可能需要一种方法来高效地管理这些订阅的访问权限、策略和符合性。 Azure 管理组提供订阅上的作用域级别。 可将订阅组织到管理组（容器）中，并将管理条件应用到该组。 管理组中的所有订阅都将自动继承应用于该组的条件。 不管使用什么类型的订阅，管理组都能提供大规模的企业级管理。
减少 VM 的安装和部署的可变性	使用 Azure 资源管理器模板增强部署选项，使其更易理解并清点环境中的 VM。

保护特权访问	使用最低特权方法和内置 Azure 角色使用户能够访问和设置 VM： • 虚拟机参与者：可以管理 VM，但无法管理虚拟机连接的虚拟网络或存储帐户。 • 经典虚拟机参与者：可管理使用经典部署模型创建的 VM，但无法管理这些 VM 连接到的虚拟网络或存储帐户。 • 安全管理员：仅在安全中心内：可以查看安全策略、查看安全状态、编辑安全策略、查看警报和建议、关闭警报和建议。 • 开发测试实验室用户：可以查看所有内容，以及连接、启动、重新启动和关闭 VM。 订阅管理员和共同管理员可更改此设置，使其成为订阅中所有 VM 的管理员。请确保你信任所有订阅管理员和共同管理员，以登录你的任何计算机。

(3) 使用多个 VM 提高可用性

倘若恶意流量或软件确实作用到了某台 VM 并对服务造成了影响，特别是 VM 运行需要的是关键应用程序，强烈建议使用多个 VM 以提高可用性。在系统架构设计上，也推荐将不同功能放置在不同的虚拟机上。按功能对虚拟机划分安全组，并设置相应的访问控制规则。为了获得更好的可用性，请使用可用性集或可用性区域。

可用性集是一种逻辑分组功能，在 Azure 中使用它可以确保将 VM 资源部署在 Azure 数据中心后，这些资源相互隔离。Azure 确保可用性集中部署的 VM 能够跨多个物理服务器、计算机架、存储单元和网络交换机运行。如果出现硬件或 Azure 软件故障，只有一部分 VM 会受到影响，整体应用程序仍可供客户使用。如果想要构建可靠的云解决方案，可用性集是一项关键功能。

(4) 防范恶意软件

应在 VM 系统中安装反恶意软件保护以帮助识别和删除病毒、间谍软件和其他恶意软件，从而进一步提高 VM 安全性。

可安装 Microsoft 反恶意软件或 Microsoft 合作伙伴的终结点保护解决方案（Trend Micro、Symantec、McAfee、Windows Defender 和 System Center Endpoint Protection）。

Microsoft 反恶意软件包括实时保护、计划扫描、恶意软件修正、签名更新、引擎更新、

示例报告和排除事件收集等功能。 对于与生产环境分开托管的环境，可以使用反恶意软件扩展来帮助保护 VM 和云服务。

Microsoft 反恶意软件和合作伙伴解决方案可与 Azure 安全中心集成，以方便部署和内置检测（警报和事件）。

最佳实践	详细信息
安装反恶意软件解决方案，以防范恶意软件	安装 Microsoft 合作伙伴解决方案或 Microsoft 反恶意软件
将反恶意软件解决方案与安全中心集成，以监视保护状态	使用安全中心管理终结点保护问题

(5) 管理 VM 更新

新型的恶意软件和病毒在不断产生，利用当前系统漏洞进行攻击。定期更新操作系统也能很大成都封堵现有漏洞，将恶意软件拒之门外。由于 Azure 不会主动去推送 Windows 更新，需要用户去管理 VM 更新。

最佳实践	详细信息
使 VM 保持最新	使用 Azure 自动化中的更新管理解决方案，为部署在 Azure、本地环境或其他云提供程序中的 Windows 和 Linux 计算机管理操作系统更新。 可以快速评估所有代理计算机上可用更新的状态，并管理为服务器安装所需更新的过程。 由更新管理托管的计算机使用以下配置执行评估和更新部署： • 用于 Windows 或 Linux 的 Microsoft 监视代理 (MMA) • 用于 Linux 的 PowerShell 所需状态配置 (DSC) • 自动化混合 Runbook 辅助角色 • 适用于 Windows 计算机的 Microsoft 更新或 Windows Server 更新服务 (WSUS) 若使用 Windows 更新，请启用 Windows 自动更新设置。
在部署时，确保构建的映像包含最新一轮的 Windows 更新	每个部署的第一步应是检查和安装所有 Windows 更新。在部署自己或库中提供的映像时，采用此措施就特别重要。虽然默认情况下会自动更新 Azure 市场中的映像，但公开发布后可能会有延迟（最多几周）。

定期重新部署 VM 以强制刷新操作系统版本	使用 Azure 资源管理器模板定义 VM，以便轻松地重新部署。 使用模板可在需要时提供已修补且安全的 VM。
向 Vm 快速应用安全更新	启用 Azure 安全中心（免费层或标准层）来识别缺少的安全更新并应用这些更新。
安装最新的安全更新	客户移到 Azure 的部分首批工作负荷为实验室和面向外部的系统。 如果 Azure VM 托管需要访问 Internet 的应用程序或服务，则需要警惕修补。修补不仅仅包括操作系统。合作伙伴应用程序上未修补的漏洞还可能导致一些问题，而如果实施良好的修补程序管理，就可以避免这些问题。
部署并测试一个备份解决方案	需要按照处理任何其他操作的相同方法处理备份。这适合于属于扩展到云的生产环境的系统。

(6) 加密虚拟硬盘文件

有些恶意软件 / 后门进入 VM 后能对硬盘数据进行读写操作，危害极大，建议加密虚拟硬盘 (VHD)，以帮助保护存储中的静态启动卷和数据卷以及加密密钥和机密。

Azure 磁盘加密用于加密 Windows 和 Linux IaaS 虚拟机磁盘。 Azure 磁盘加密利用 Windows 的行业标准 BitLocker 功能和 Linux 的 DM-Crypt 功能，为 OS 和数据磁盘提供卷加密。 该解决方案与 Azure Key Vault 集成，帮助用户管理 Key Vault 订阅中的磁盘加密密钥和机密。 此解决方案还可确保虚拟机磁盘上的所有数据在 Azure 存储中静态加密。

下面是使用 Azure 磁盘加密的最佳做法：

最佳实践	详细信息
在 VM 上启用加密	Azure 磁盘加密将生成加密密钥并将其写入密钥保管库。 在 Key Vault 中管理加密密钥需要 Azure AD 身份验证。 为此，请创建 Azure AD 应用程序。 对于身份验证，可以使用基于客户端机密的身份验证或基于客户端证书的 Azure AD 身份验证。

使用密钥加密密钥 (KEK) 来为加密密钥提供附加的安全层。 将 KEK 添加到密钥保管库。	使用 Add-AzKeyVaultKey cmdlet 在 Key Vault 中创建密钥加密密钥。 还可从本地硬件安全模块 (HSM) 导入 KEK 以进行密钥管理。 有关详细信息，请参阅 Key Vault 文档。 指定密钥加密密钥后，Azure 磁盘加密会使用该密钥包装加密机密，然后将机密写入 Key Vault。 在本地密钥管理 HSM 中保留此密钥的托管副本，提供额外的保护，防止意外删除密钥。
在加密磁盘之前创建快照和 / 或备份。 如果加密期间发生意外故障，备份可提供恢复选项。	加密之前，需要备份包含托管磁盘的 VM。 进行备份后，可以使用 **AzVMDiskEncryptionExtension** cmdlet 通过指定 **-skipVmBackup** 参数来加密托管磁盘。 有关如何备份和还原已加密 VM 的详细信息，请参阅 Azure 备份一文。
为确保加密机密不会跨过区域边界，Azure 磁盘加密需要将密钥保管库和 VM 共置在同一区域。	在要加密的 VM 所在的同一区域中创建并使用密钥保管库。

Azure 磁盘加密可解决以下业务需求：

- 使用行业标准的加密技术轻松保护 IaaS VM，满足组织的安全性与合规性要求。
- IaaS VM 会根据客户控制的密钥和策略启动，客户可以在 Key Vault 中审核密钥和策略的使用方式。

除了以上 Azure 平台和 VM 层面的安全保障方法，虚拟机的安全也离不开用户本身的管理和操作。以下最佳实践能降低人为引起的安全风险。

(7) 做好数据的备份

建议对运行关键程序和业务的虚拟机做好备份。假设恶意软件对某台虚拟机产生影响，或人为错误将 bug 引入应用程序，或误操作都可能造成了数据无法访问或数据丢失。

➢ Azure 备份

若要备份运行生产工作负荷的 Azure VM，请使用 Azure 备份。 Azure 备份对 Windows 和 Linux VM 均支持应用程序一致性备份。 Azure 备份可创建恢复点，这些恢复点存储在异地冗余的恢复保管库中。 从恢复点还原时，可以还原整个 VM，也可以仅还原特定的文件。

- 教程：在 Azure 中备份和还原 Linux 虚拟机的文件
- 教程：在 Azure 中备份和还原 Windows 虚拟机的文件

➢ Azure Site Recovery

当整个区域因重大自然灾难或大规模服务中断而发生中断时，Azure Site Recovery 可以保护 VM，使其免受重大灾难影响。请参考将 Azure VM 复制到另一个 Azure 区域。

➢ 托管快照

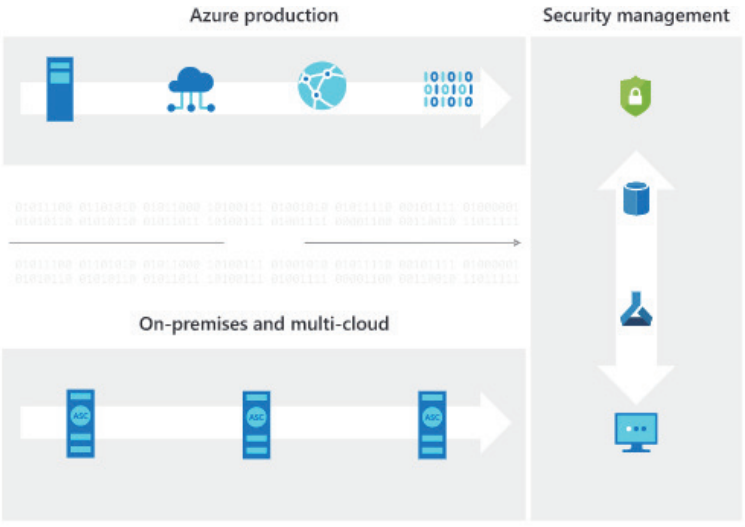
在 (6) 加密虚拟硬盘文件 中推荐在加密磁盘之前创建快照和 / 或备份。开发和测试环境中，快照为使用托管磁盘的 VM 备份提供快速而又简单的选项。 托管快照是托管磁盘的只读完整副本。快照独立于源磁盘而存在，并可用来新建用于重建 VM 的托管磁盘。 基于磁盘的已使用部分对快照进行计费。

- 使用 Windows 中的快照创建作为托管磁盘存储的 VHD 的副本
- 使用 Linux 中的快照创建作为托管磁盘存储的 VHD 的副本
- 通过递增快照备份 Azure 非托管 VM 磁盘

(8) Azure 安全中心 (Azure Security Center) 全面保驾护航

对于复杂的企业环境，建议使用 Azure Security Center。Azure 安全中心是一个统一的基础结构安全管理系统，能自动评估当前安全状态并作出建议，可以增强数据中心的安全态势，以及为云中（无论是否在 Azure 中）和本地的混合工作负荷提供高级威胁防护。

➢ Security Center 的工作原理



激活安全中心时，会在 Azure 虚拟机中自动部署一个监视代理。对于本地 VM，需手动部署代理。然后，安全中心开始评估你的所有 VM、网络、应用程序和数据的整体安全状态。分析引擎会分析数据，由机器学习来合成该数据。安全中心会提供建议和威胁警报来保护你的工作负载。如果出现攻击或异常活动，你将立即收到通知。另外，可在 Azure Monitor 工作区将安全信息进行聚合来实现大数据查询功能。也可通过 REST API、PowerShell cmdlet 或者与现有 SIEM 的集成（例如 Azure Sentinel）来查询数据。

➢ 体系结构

由于 Azure Security Center 本身是 Azure 的一部分，因此 Azure 中的 PaaS 服务（包括 Service Fabric、SQL 数据库和存储帐户）会受到安全中心的监视和保护，无需进行任何部署。

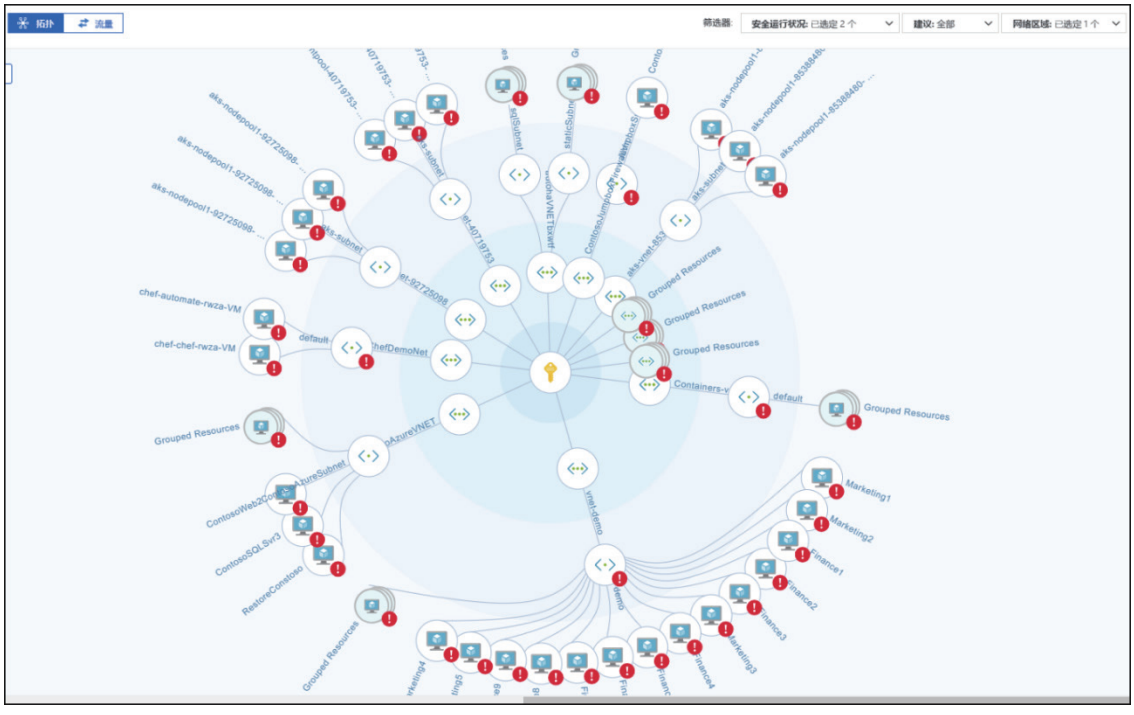
此外，Azure Security Center 通过在 Windows 和 Linux 服务器的云中或本地非 Azure 服务器和虚拟机上安装 Microsoft Monitoring Agent 来对它们进行保护。Azure 虚拟机是在安全中心中自动预配的。

从代理和 Azure 收集的事件在安全分析引擎中相关联，从而提供定制的建议（强化任务）（应遵循这些建议以确保工作负荷是安全的）以及威胁检测警报。应尽快调查此类警报以确保没有针对工作负荷发生的恶意攻击。

➢ 持续评估

Azure Security Center 会持续发现部署在工作负荷中的新资源并评估它们是否已根据安全最佳做法进行了配置，如果没有，则会将它们标记出来，并且你将获得一个按优先级排列的建议列表，便于你进行修复以保护计算机。

安全中心提供用于持续监视网络安全状态的强大工具之一——网络映射 。通过映射可以查看工作负荷的拓扑，从而可以查看是否已正确配置了每个节点。可以看到节点的连接方式，这有助于阻止不必要的连接，这些连接可能使攻击者更容易进行网络爬虫。



➢ Azure Security Center 管理 VM 安全状况

安全中心可用于查看虚拟机的安全设置，从而帮助保护 Azure 中的虚拟机数据。 当利用安全中心保护 VM 时，可使用以下功能：

- 应用包含建议的配置规则的 OS 安全设置。
- 识别并下载可能缺少的系统安全更新和关键更新。

- 部署终结点反恶意软件防护建议措施。
- 验证磁盘加密。
- 评估并修正漏洞。
- 检测威胁。

安全中心将数据存储在 Azure Monitor 日志中。 Azure Monitor 日志提供了查询语言和分析引擎，可让你深入了解应用程序和资源的操作，详见下节。 数据也是从 Azure Monitor、管理解决方案以及安装在虚拟机（云中或本地）上的代理收集的数据。

➢ 安全中心的漏洞评估

如前文所述，恶意软件能利用计算机漏洞渗透进操作系统，对用户造成威胁。而 Azure 安全中心提供了针对虚拟机的漏洞评估。 如果安全中心找不到安装在 VM 上的漏洞评估解决方案，它会建议你安装一个。 目前，漏洞评估功能由 Qualys 和 Rapid7 提供。可以在多个 VM 上安装此漏洞评估解决方案，但这些 VMs 必须属于同一订阅。

安全中心提供的其他服务和实践方法将在 2.1.4 一站式全方位管理进行介绍。

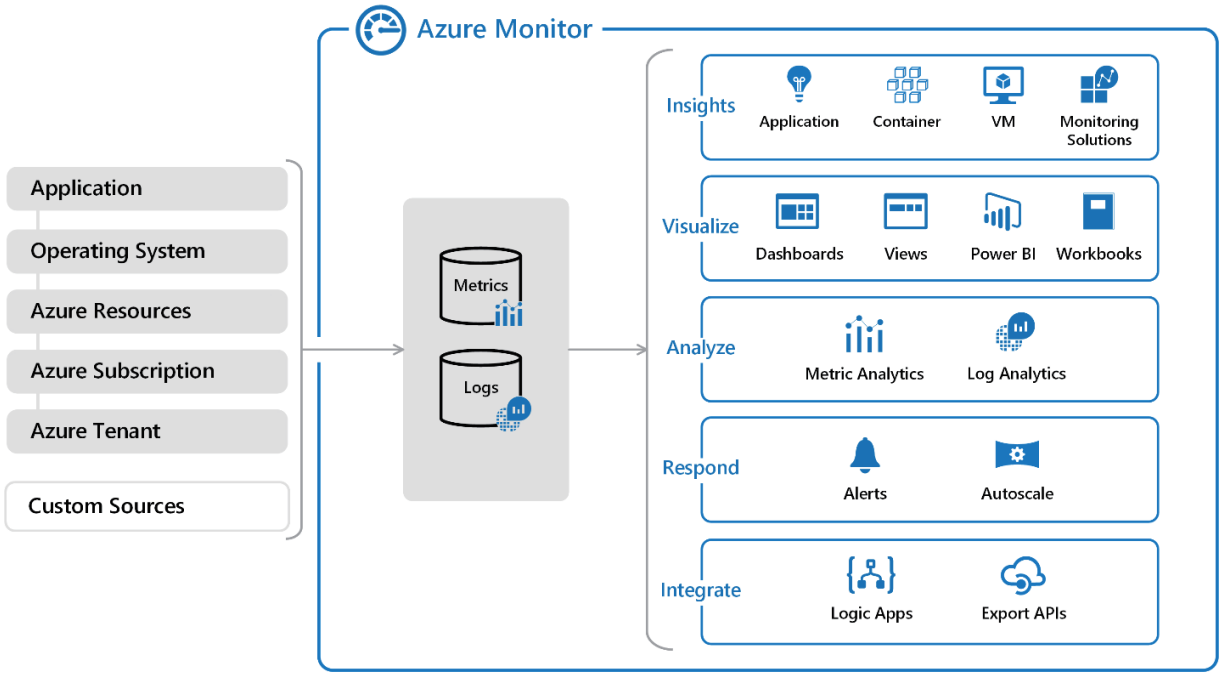
(9) Azure Monitor 监视 VM 性能指标

在全面提升了虚拟机和网络安全后，有效且实时的监控也是必不可少的。如若在 Azure 门户的 Dashboard 上发现某虚拟机 CPU 或内存占用较高，可能意味着该虚拟机遭到了拒绝服务 (DoS) 攻击。即使没有遭到恶意流量的攻击，如果 VM 进程消耗的资源多过实际所需的量，也可能会造成资源滥用的问题，而且 VM 性能问题可能会导致服务中断，从而违反可用性安全原则。这对于托管 IIS 或其他 Web 服务器的 VM 尤其重要。但是，如果只是不定期或偶然从 Azure 门户的 Dashboard 去发现问题，对于有组织的恶意攻击肯定是来不及应对的，所以不仅要在出现问题时被动地监视 VM 的访问，而且还要在 VM 正常运行期间针对基准性能进行主动地监视。

Azure Monitor 即是监控资源运行状况的利器。它提供了一个全面的解决方案，用于从云和本地环境收集、分析和操作遥测数据，从而最大程度地提高应用程序和服务的可用性和性能。它可以帮助你了解应用程序的性能，并主动识别影响应用程序及其所依赖资源的问题。

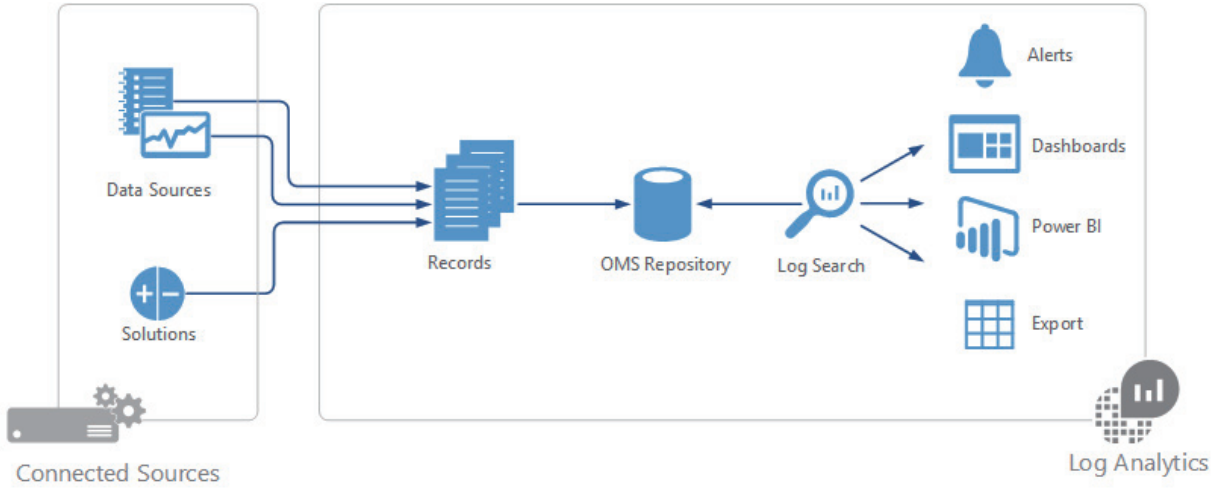
Azure Monitor 包括以下内容的几个示例：

- 通过 Application Insights 检测和诊断应用程序和依赖项中的问题。
- 将基础结构问题与容器的用于 VM 的 Azure Monitor 和 Azure Monitor 相关联。
- 利用 Log Analytics 进行故障排除和深度诊断，深入了解监视数据。
- 支持对智能警报和自动化操作进行大规模的操作。
- 通过 Azure 仪表板和工作簿创建可视化效果。



➢ Azure Monitor 日志

Azure Monitor 日志是 Azure 中的一项服务，可帮助收集和分析云和本地环境中资源生成的数据。使用集成的搜索和自定义仪表板，轻松分析所有工作负荷和服务器上的数百万记录，而无需考虑它们的物理位置，从而获得实时见解。



➢ 日志查询

日志查询可帮助你充分利用 Azure Monitor 日志中收集的数据的价值。 使用功能强大的查询语言，只需编写极少量的代码即可联接多个表中的数据、聚合大型数据集，以及执行复杂的操作。 只要收集了支持数据，并且你了解如何构造适当的查询，就几乎能够解答任何问题和执行分析。

2.1.3 数据安全

大数据时代，数据的挖掘、处理、运用，在给社会带来便利的同时，也造成了数据不合理使用和对个人信息造成威胁。2018 年，欧盟出台《通用数据保护条例》(GDPR)，目的在于遏制个人信息被滥用，保护个人隐私，并被称为史上最严的个人数据保护条例；2019 年 5 月 28 日，根据《中华人民共和国网络安全法》等法律法规，国家互联网信息办公室会同相关部门也研究起草了《数据安全管理办法（征求意见稿）》。国家对于网络安全问题的重视，进一步细化了数据安全管理办法和准则，助力网络环境健康发展。[16]

对于数据安全，全球研究机构 Gartner 分析师提出了三大挑战：

- 当前，在全球数字化业务开展得如火如荼时期，业务发展依赖于数据资产带来的金融机会，但同时缺乏对数据相关金融风险和负债规模和范围进行评估的意识或能力。
- 无论是存储在本地还是在公共云，数据使用的速度，数量，种类和价值都在不断增长，导致数字化业务投资决策的复杂性和风险急剧增加。
- 在风险敞口增加的时候，由于缺乏针对数据投资和安全性的整合业务策略将减少数据变现和价值创造的机会。

Azure 将数据安全列为重中之重。数据安全包括数据库安全，数据加密，硬盘加密，存储安全等。

(1) 数据库安全

安全性是管理数据库时的首要考虑因素，并且始终是微软数据库例如 Azure SQL 数据库、Cosmos DB、 Data Lake 等的优先事务。

Azure SQL 数据库安全

Azure SQL 数据库支持使用防火墙规则和连接加密的连接安全。 它支持使用用户名和密码进行身份验证，也支持使用 Azure Active Directory (Azure AD) 进行身份验证。 授权使用基于角色的访问控制。

Azure SQL 数据库通过对静态的数据库、关联备份和事务日志文件执行实时加密和解密来支持加密，而无需更改应用程序。

Microsoft 提供了加密企业数据的其他方法：

- 单元级加密可用于通过不同加密密钥来加密特定数据列甚至数据单元。
- 如需硬件安全模块或需集中管理加密密钥层次结构，请考虑对 Azure 虚拟机 (VM) 中的 SQL Server 使用 Azure Key Vault。
- Always Encrypted（目前为预览版）使加密对应用程序透明。 它还允许客户在客户端应用程序内加密敏感数据，无需与 SQL 数据库共享加密密钥。

16 数据安全管理办法 (征求意见稿)：保障个人信息和重要数据安全 .
https://www.freebuf.com/column/204800.html

Azure SQL 数据库审核使企业能够将事件记录到 Azure 存储中的审核日志。 SQL 数据库审核还与 Microsoft Power BI 集成，以帮助向下钻取报告和分析数据。严格保护数据库有助于满足大部分法规或安全要求，包括 HIPAA、ISO 27001/27002 和 PCI DSS Level 1。Microsoft 信任中心站点上提供了安全合规认证的最新列表。 也可以根据法规要求将数据库放置在特定的 Azure 数据中心。

本节逐步介绍保护 Microsoft Azure SQL 数据库的结构化、表格和关系数据的基础知识。 具体而言，本文介绍如何使用相应的资源来保护数据、控制访问和执行主动监视。

➢ 数据保护

SQL 数据库可提供加密功能来帮助保护数据：

- 通过传输层安全性 (TLS) 来保护动态数据。
- 通过透明数据加密保护来静态数据。
- 通过 Always Encrypted 来保护使用中的数据。

若要通过其他方法加密数据，请考虑：

- 使用单元格级加密，借助不同的加密密钥来加密特定的数据列甚至数据单元格。
- 如需硬件安全模块或需集中管理加密密钥层次结构，请参阅对 Azure VM 中的 SQL Server 使用 Azure Key Vault。

a) 动态加密

所有客户端 / 服务器应用程序有一个常见问题，即数据在公共和专用网络中传输时需要隐私。 如果通过网络传输的数据未加密，则数据有可能被未经授权的用户捕获和窃取。处理数据库服务时，请务必对在数据库客户端和服务器间传输的数据进行加密。 此外，还务必对在相互通信的数据库服务器间和中间层应用程序间传输的数据进行加密。

管理网络时存在一个问题：需要保护跨不可信网络在应用程序之间发送的数据。可以使用 TLS/SSL 验证服务器和客户端，然后使用它来加密经过身份验证的双方之间的消息。

在身份验证过程中，TLS/SSL 客户端会向 TLS/SSL 服务器发送消息。 服务器用验证服务器本身所需的信息进行响应。 客户端和服务器执行会话密钥的额外交换，身份验证对话结束。 完成身份验证后，可以通过在身份验证过程中建立的对称加密密钥在服务器和客户端之间开始 SSL 保护的通信。

在与数据库来回传输数据时，与 Azure SQL 数据库建立的所有连接都需要经过加密 (TLS/SSL)。 SQL 数据库使用 TLS/SSL 验证服务器和客户端，然后使用它来加密经过身份验证的双方之间的消息。

在应用程序的连接字符串中，必须指定参数来加密连接，而不是信任服务器证书。（如果将连接字符串从 Azure 门户中复制出来，则我们会代你完成此操作。）否则，连接不会验证服务器的身份，且容易受到“中间人”攻击。 例如，对于 ADO.NET 驱动程序，这些连接字

符串参数为 Encrypt=True 和 TrustServerCertificate=False。

b) 静态加密

可采取一些预防措施来帮助保护数据库。 例如设计安全系统、加密机密资产、围绕数据库服务器构建防火墙。 但如果物理媒体（如驱动器或备份磁带）失窃，恶意方可能会还原或附加数据库并浏览数据。

一种解决方法是加密数据库中的敏感数据，并使用证书保护用于加密数据的密钥。 此解决方案可防止没有密钥的人使用数据，但这种保护必须经过精心规划。

为解决此问题，SQL Server 和 SQL 数据库支持透明数据加密。 透明数据加密可加密 SQL Server 和 SQL 数据库数据文件，这称为静态加密数据。

透明数据加密有助于防范恶意活动的威胁。 它可执行静态数据库、关联备份和事务日志文件的实时加密和解密，无需更改应用程序。

透明数据加密使用称为数据库加密密钥的对称密钥来加密整个数据库的存储。 在 SQL 数据库中，数据库加密密钥由内置服务器证书保护。 内置服务器证书对每个 SQL 数据库服务器都是唯一的。

如果数据库处于 Geo-DR 关系中，则会受到每个服务器上不同的密钥的保护。 如果两个数据库连接到同一个服务器，则它们共用相同的内置证书。 Microsoft 每隔 90 天自动轮换这些证书至少一次。

有关详细信息，请参阅透明数据加密。

c) 使用中的加密（客户端）

大部分数据泄漏涉及窃取关键数据，如信用卡号或个人身份信息。 数据库可能是宝贵的敏感信息。其中可能包含客户的个人数据（如身份证号码）、机密的竞争信息和知识产权。数据丢失或被盗（尤其是客户数据）可能会使企业形象受损，让企业落于竞争劣势，遭受严重罚款甚至面临诉讼。

Always Encrypted 功能旨在保护存储在 Azure SQL 数据库或 SQL Server 数据库中的敏感数据。 通过 Always Encrypted，客户可在客户端应用程序中加密敏感数据，永远不会向数

据库引擎（SQL 数据库或 SQL Server）透露加密密钥。

Always Encrypted 将数据所有者与数据管理者区分开来，前者可查看数据，而后者无权访问数据。 它有助于确保本地数据库管理员、云数据库操作员或其他拥有高级特权但未经授权的用户无法访问加密数据。

此外，Always Encrypted 使加密对应用程序透明。 在客户端计算机上安装启用了 Always Encrypted 的驱动程序，以便自动加密和解密客户端应用程序中的敏感数据。 将数据传输到数据库引擎前，驱动程序会对敏感列中的数据进行加密。 驱动程序会自动重写查询，以便保留应用程序的语义。 同样，该驱动程序透明地解密存储在查询结果中包含的加密数据库列中的数据。

➢ 访问控制

为确保安全性，SQL 数据库通过以下方式来控制访问：

- 采用通过 IP 地址限制连接的防火墙规则。
- 采用身份验证机制，要求用户表明其身份。
- 采用授权机制，限制用户执行特定操作，访问特定数据。

a) 数据库访问

数据保护从控制对数据的访问开始。 由承载数据的数据中心管理物理访问。 可配置防火墙来管理网络层的安全。 此外，还可以通过配置用于身份验证的登录信息并定义服务器和数据库角色的权限来控制访问。

○ 防火墙和防火墙规则

Azure SQL 数据库为 Azure 和其他基于 Internet 的应用程序提供关系数据库服务。 为了保护数据，在指定哪些计算机具有访问权限之前，防火墙将禁止所有对数据库服务器的访问。 防火墙基于每个请求的起始 IP 地址授予数据库访问权限。 有关详细信息，请参阅 Azure SQL 数据库防火墙规则概述。

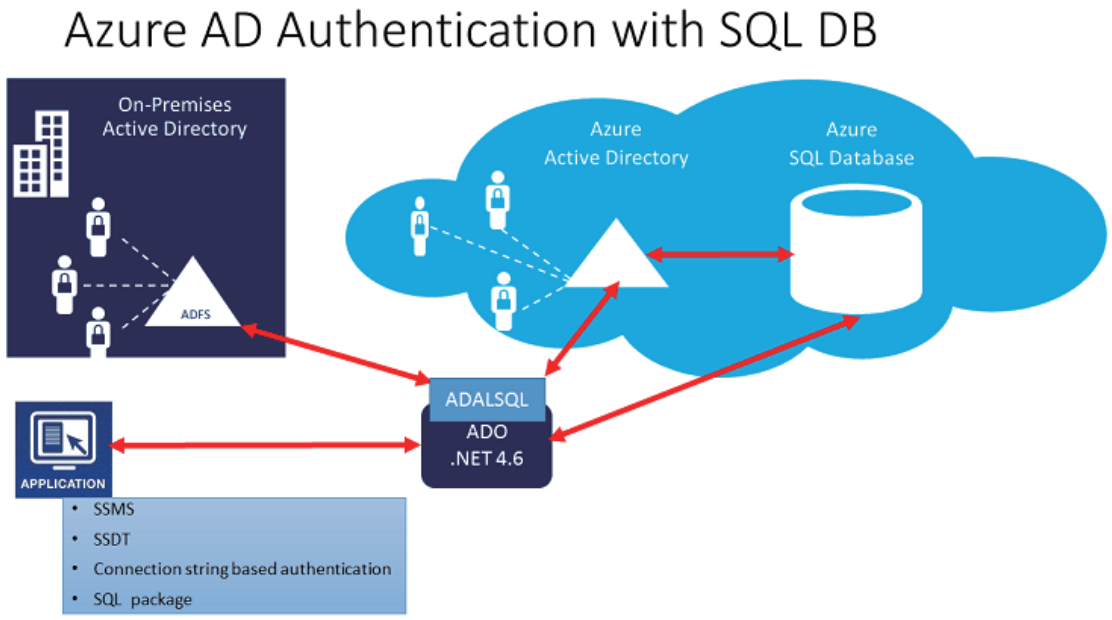
只能通过 TCP 端口 1433 使用 Azure SQL 数据库服务。 若要从计算机访问 SQL 数据库，请确保客户端计算机防火墙允许 TCP 端口 1433 上的传出 TCP 通信。 如果其他应用程序不需入站连接，则阻止 TCP 端口 1433 上的入站连接。

○ 身份验证

身份验证是指连接到数据库时如何证明身份。 SQL 数据库支持两种类型的身份验证：

- SQL Server 身份验证：创建逻辑 SQL 实例时会创建单个登录帐户，称为“SQL 数据库订户帐户”。 此帐户通过 SQL Server 身份验证（用户名和密码）进行连接。 此帐户为管理员，负责管理逻辑服务器实例以及所有附加到该实例的用户数据库。 不能限制订户帐户的权限。 此类帐户只能存在一个。
- Azure Active Directory 身份验证：Azure AD 身份验证是使用 Azure AD 中的标识连接

到 Azure SQL 数据库和 Azure SQL 数据仓库的一种机制。 可通过它集中管理数据库用户的身份。



Azure AD 身份验证的优点包括：

- 提供一个 SQL Server 身份验证的替代方法。
- 它有助于阻止跨数据库服务器的用户身份的扩散，且允许在一个地方进行密码轮换。
- 可使用外部 (Azure AD) 组管理数据库权限。
- 它可通过启用集成的 Windows 身份验证和 Azure AD 支持的其他形式的身份验证来消除存储密码。

Authorization

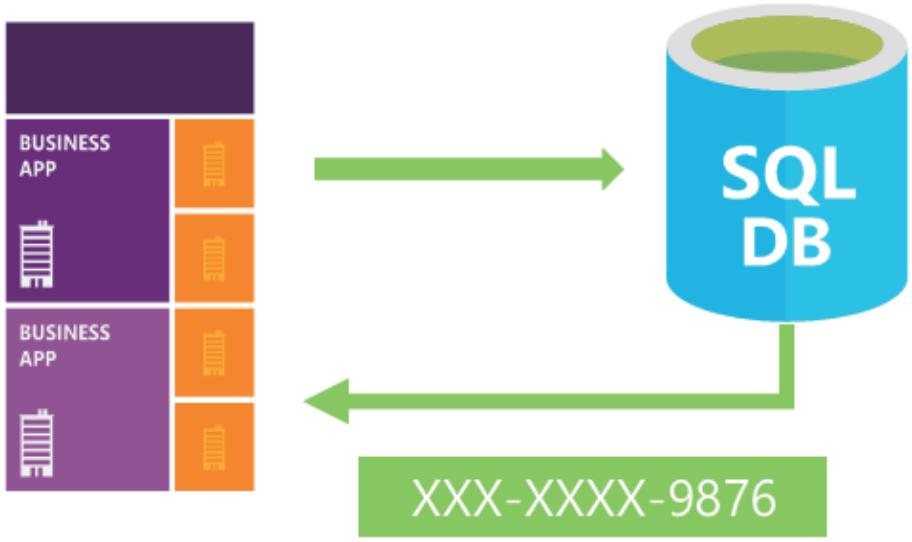
授权是指用户可在 Azure SQL 数据库中执行的操作。 授权由用户帐户的数据库角色成员资格和对象级权限控制。 授权是确定主体可以访问哪些安全对象资源以及哪些操作允许用于这些资源的过程。

b) 应用程序访问

- 动态数据掩码

呼叫中心的服务代表可能会通过呼叫者社会安全号码或信用卡号中的几位数字来识别呼叫者。 但不应向服务代表完全公开这些数据项。

可定义掩码规则，遮掩任何查询结果集中除身份证号或信用卡号后四位数以外的其他所有数字。



再举一个例子，可定义合适的数据掩码来保护个人身份信息。 然后开发人员可查询生产环境，进行故障排除，而不违反法规。

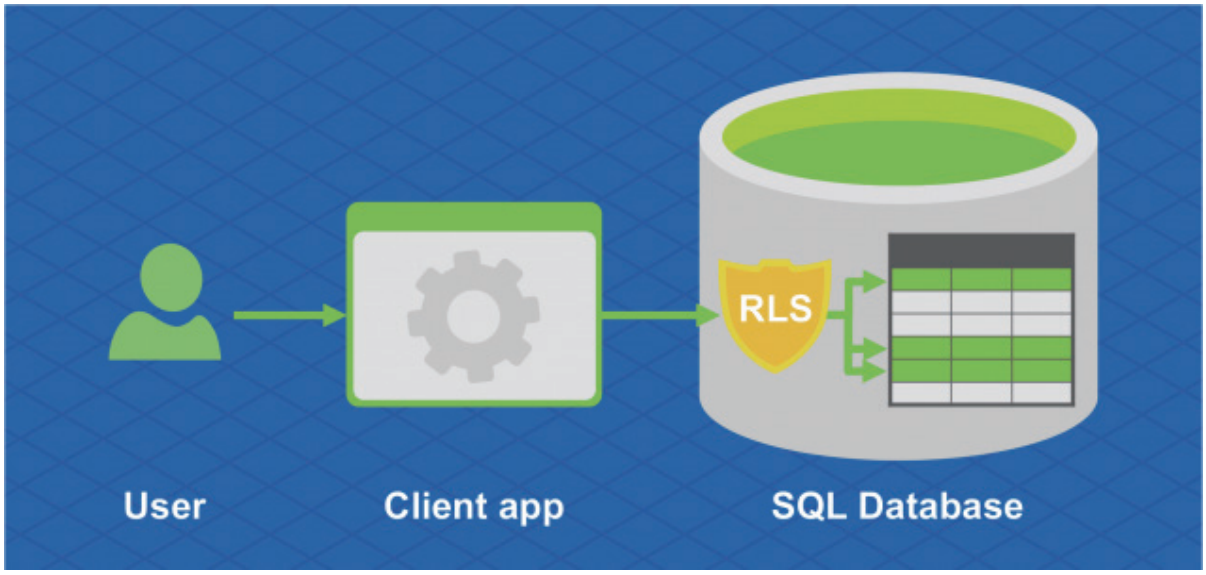
SQL 数据库动态数据掩码通过对非特权用户模糊化敏感数据来限制此类数据的泄露。V12 版的 Azure SQL 数据库支持动态数据屏蔽。

动态数据屏蔽允许用户指定在对应用层产生最小影响的前提下可以透露的敏感数据量，从而帮助防止未经授权的用户访问敏感数据。 它是一种基于策略的安全功能，会在针对指定的数据库字段运行查询后返回的结果集中隐藏敏感数据，同时保持数据库中的数据不变。

需要注意的是，只有 Azure 数据库管理员、服务器管理员或安全主管角色可以配置动态数据屏蔽。

- 行级安全性

多租户数据库的另一个常见安全要求是行级安全性。 可使用此功能根据执行查询的用户的特征控制对数据库表中的行的访问。 （特征可以是组成员身份或执行上下文等。）



访问限制逻辑位于数据库层，而不会脱离另一应用程序层中的数据。 每当从任一层尝试访问数据时，数据库系统就会应用访问限制。 这样就会通过减少安全系统的外围应用，使安全系统变得更加可靠和稳健。

行级安全性引入了基于谓词的访问控制。 它可进行灵活的集中式评估，能考虑元数据或管理员根据需要确定的任何其他标准。 谓词用作判断用户是否对基于用户属性的数据具有适当访问权限的标准。 可通过使用基于谓词的访问控制来实现基于标签的访问控制。

➢ 主动监视

SQL 数据库可提供"审核"和"威胁检测"功能，有助于保护数据。

a) 审核

Azure SQL 数据库审核可提高用户深入了解数据库中发生的事件和更改的能力。 示例包括针对数据的更新和查询。

SQL 数据库审核可跟踪数据库事件，并将事件写入 Azure 存储帐户中的审核日志。 审核可帮助你遵守法规、了解数据库活动，以及深入了解可以指明业务考量因素或疑似安全违规的偏差和异常。 审核有助于遵从法规标准，但不能保证遵从法规。

可使用 SQL 数据库审核来：

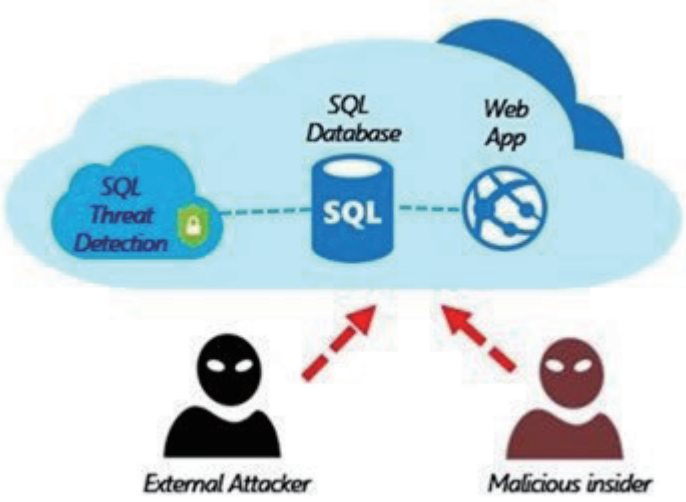
- 保留选定事件的审核痕迹。 可以定义要审核的数据库操作的类别。
- 报告数据库活动。 可以使用预配置的报告和仪表板快速开始使用活动和事件报告。
- 分析报告。 可以查找可疑事件、异常活动和趋势。

有两种审核方法：

- Blob 审核：日志将写入到 Azure Blob 存储。 这是一种较新的审核方法。 这种方法可提供更高的性能，支持更高粒度的对象级审核，且更具成本效益。
- 表审核：日志将写入到 Azure 表存储。

b) 威胁检测

Azure SQL 数据库的高级威胁防护可检测到指示潜在安全威胁的可疑活动。 可使用威胁检测响应数据库中发生的可疑事件，例如 SQL 注入。 它可提供警报，并允许使用 Azure SQL 数据库审核来探查可疑事件。



SQL 高级威胁防护 (ATP) 提供一组高级 SQL 安全功能，包括数据发现和分类、漏洞评估和威胁检测。

- 数据发现和分类
- 漏洞评估
- 威胁检测

Azure Database for PostgreSQL 高级威胁防护提供了一个新的安全层，可以通过提供异常活动的安全警报来检测和响应可能发生的威胁。 出现可疑数据库活动、潜在漏洞以及异常数据库访问和查询模式时，用户将收到警报。 Azure Database for PostgreSQL 的高级威胁防护将警报与 Azure 安全中心集成。 警报类型包括：

- 来自异常位置的访问
- 来自异常 Azure 数据中心的访问
- 来自陌生主体的访问
- 来自可能有害的应用程序的访问
- 暴力破解 Azure 数据库的 PostgreSQL 凭据

Azure Database for MySQL 高级威胁防护提供类似于 PostgreSQL 高级防护的保护功能。

➢ 集中的安全管理

Azure 安全中心可帮助防范、检测和应对威胁。 它为 Azure 订阅提供集成的安全监控和策略管理。 它有助于检测可能会被忽视的威胁，适用于各种安全解决方案生态系统。

安全中心通过为所有服务器和数据库提供安全性的可见性来帮助保护 SQL 数据库中的数

据。 通过安全中心，可以：

- 定义 SQL 数据库加密和审核的策略。
- 跨所有订阅监视 SQL 数据库资源的安全性。
- 快速识别和修复安全问题。
- 集成来自 Azure SQL 数据库威胁检测的警报。

安全中心支持基于角色的访问。

➢ SQL 信息保护

SQL 信息保护自动发现潜在的敏感数据并将其进行分类，提供标记机制，用于通过分类属性永久标记敏感数据，并提供显示数据库分类状态的详细仪表板。

此外，它还会计算 SQL 查询的结果集敏感性，以便可以显式审核提取敏感数据的查询，并且可以保护数据。 有关 SQL 信息保护的更多详细信息，请参阅 Azure SQL 数据库数据发现和分类。

可以在 Azure 安全中心配置 SQL 信息保护策略。

➢ Azure Marketplace

Azure Marketplace 是一个在线应用程序和服务市场，初创公司和独立软件供应商 (ISV) 能够通过它为全球 Azure 客户提供解决方案。 Azure 市场与 Microsoft Azure 合作伙伴生态系统结合为一个统一的平台，以便更好地服务于客户和合作伙伴。 可运行搜索，查看 Azure 市场中可用的数据库安全产品。

有关更多 Azure SQL 数据库安全相关文档，请参考 Azure 数据库安全性最佳做法和 Azure 数据库安全性清单。

Cosmos DB 数据库加密

Azure Cosmos DB 由 Microsoft 提供，是全球分布式多模型数据库。 存储在非易失性存储（固态硬盘）中的 Cosmos DB 中的用户数据默认加密。 无法将其打开或关闭。 静态加密是通过许多安全技术实现的，其中包括安全密钥存储系统、加密网络以及加密 API。 加密密钥由 Microsoft 管理，并根据 Microsoft 的内部指南进行轮换。

Data Lake 中的静态加密

Azure Data Lake 是在正式定义需求或架构之前，在单个位置收集的每种类型数据的企业级存储库。Data Lake Store 支持默认启用透明加密静态数据，可以在创建帐户期间设置。默认情况下，Azure Data Lake Store 替你管理密钥，但你可以选择自己管理密钥。

有三种类型的密钥用于加密和解密数据：主加密密钥 (MEK)、数据加密密钥 (DEK) 和块加密密钥 (BEK)。 MEK 用于加密存储在永久性介质上的 DEK，BEK 派生自 DEK 和数据块。 如果管理自己的密钥，可以轮换 MEK。

(2) Azure 数据加密与存储安全

本节概述可与 Azure 存储配合使用的 Azure 安全功能。 Azure 存储是依赖于持续性、可用性和伸缩性来满足客户需求的现代应用程序的云存储解决方案。 Azure 存储提供全面的安全功能。 你可以：

- 使用基于角色的访问控制 (RBAC) 和 Azure Active Directory 对存储帐户进行安全保护。
- 使用客户端加密、HTTPS 或 SMB 3.0 对应用程序和 Azure 之间传输的数据进行安全保护。
- 可将数据设置为在写入 Azure 存储时使用存储服务加密自动进行加密。
- 将虚拟机 (VM) 使用的 OS 和数据磁盘设置为使用 Azure 磁盘加密进行加密。
- 使用共享访问签名 (SAS) 授予对 Azure 存储中数据对象的委派访问权限。
- 使用分析来跟踪某人访问存储时使用的身份验证方法。

有关 Azure 存储中安全性的详细信息，请参阅 Azure 存储安全指南。 本指南深入介绍了 Azure 存储的安全功能。 这些功能包括存储帐户密钥、传输中和静态中的数据加密以及存储分析。

基于角色的访问控制

可使用基于角色的访问控制来帮助保护存储帐户。 对于想要实施数据访问安全策略的组织而言，必须根据需要知道和最低权限安全策略限制访问权限。 这些访问权限是通过将相应的 RBAC 角色分配给特定范围内的组和应用程序来授予的。 可以使用内置 RBAC 角色（例如存储帐户参与者）将权限分配给用户。

了解更多：

- Azure Active Directory 基于角色的访问控制

存储对象的委托访问权限

共享访问签名对存储帐户中的资源提供委托访问。 使用 SAS，意味着可以授权客户端在指定时间段内，以一组指定权限有限访问存储帐户中的对象。 可以授予这些有限的权限，而不必共享帐户访问密钥。

SAS 是一个 URI，在其查询参数中包含对存储资源已验证访问所需的所有信息。 要使用 SAS 访问存储资源，客户端只需将 SAS 提供给相应的构造函数或方法。

了解更多：

- 了解 SAS 模型
- 创建 SAS 并将其用于 Blob 存储

传输中加密

传输中加密是通过网络传输数据时保护数据的一种机制。 在 Azure 存储中，可使用以下功能保护数据：

- 传输级别加密，例如将数据传入或传出 Azure 存储时使用的 HTTPS。

- 线路加密，例如 Azure 文件共享的 SMB 3.0 加密。
- 客户端加密，在将数据传输到存储之前加密数据，以及从存储传出数据后解密数据。

了解有关客户端加密的详细信息：

- 适用于 Microsoft Azure 存储的客户端加密
- 云安全控制系列：加密传输中的数据

静态加密

对许多组织而言，静态数据加密是实现数据隐私性、符合性和数据所有权的必要措施。可通过三种 Azure 功能进行静态数据加密：

- 存储服务加密始终处于启用状态，并在数据写入 Azure 存储时自动加密数据。
- 客户端加密也提供静态加密功能。
- Azure 磁盘加密允许加密 IaaS 虚拟机使用的 OS 磁盘和数据磁盘。

了解有关存储服务加密的详细信息：

- Azure 存储服务加密适用于 Azure Blob 存储。 有关其他 Azure 存储类型的详细信息，请参阅 Azure 文件存储、表存储、队列存储。
- 静态数据的 Azure 存储服务加密

Azure 磁盘加密

适用于虚拟机的 Azure 磁盘加密有助于解决组织安全性和符合性要求。 它使用 Azure Key Vault 中控制的密钥和策略来加密 VM 磁盘（包括启动盘和数据磁盘）。

适用于 VM 的磁盘加密可用于 Linux 与 Windows 操作系统。 它也使用密钥保管库帮助你保护、管理和审核磁盘加密密钥的使用。 在 Azure 存储帐户中使用行业标准加密技术，对 VM 磁盘中的所有数据进行静态加密。 适用于 Windows 的磁盘加密解决方案是基于 Microsoft BitLocker 驱动器加密技术，Linux 解决方案基于 dm-crypt。

了解详细信息

- Azure 磁盘加密概述

Azure 存储的防火墙和虚拟网络

Azure 存储允许你为存储帐户启用防火墙规则。 启用后，它们将阻止传入的数据请求，包括来自其他 Azure 服务的请求。 可以配置例外以允许流量。 可以在现有存储帐户上或在创建时启用防火墙规则。

应该使用此功能将存储帐户保护到一组特定的允许网络。

有关 Azure 存储防火墙和虚拟网络的详细信息，请查看文章配置 Azure 存储防火墙和虚拟网络

Azure Data Box

Data Box、Data Box Disk 和 Data Box Heavy 设备可在网络不可用时将大量数据传输到

Azure。 这些脱机数据传输设备在组织和 Azure 数据中心之间往返运输。 它们使用 AES 加密来帮助保护传输中的数据，还在上传后执行一个清理过程，从设备中删除你的数据。

Data Box Edge 和 Data Box Gateway 是联机数据传输产品，它们用作网络存储网关来管理站点和 Azure 之间的数据。 Data Box Edge 是一种本地网络设备，可将数据传入和传出 Azure，并使用支持人工智能 (AI) 的边缘计算来处理数据。 Data Box Gateway 是具有存储网关功能的虚拟设备。

了解更多：

- Azure Data Box
- Azure Data Box Edge
- Azure Data Box Gateway

高级威胁防护

Azure 存储提供了高级威胁防护来实现额外的一层安全智能，用于检测试图访问或利用你的存储帐户的异常或可能有害的企图。 高级威胁防护监视 Azure 存储诊断日志来获取针对 Blob 存储的可疑读取、写入或删除请求。

可以从 Azure 安全中心查看高级威胁防护警报。 Azure 安全中心会提供有关检测到的任何可疑活动的详细信息，并提供用于针对潜在威胁进行调查和补救的建议操作。

了解更多：

- Azure 存储高级威胁防护概述

Azure Key Vault

Azure Disk Encryption 使用 Azure Key Vault 来帮助控制和管理 Key Vault 订阅中的磁盘加密密钥和机密。 它还可确保虚拟机磁盘上的所有数据在 Azure 存储中静态加密。 应使用密钥保管库来审核密钥和策略的使用。

了解详细信息

- 什么是 Azure 密钥保管库？

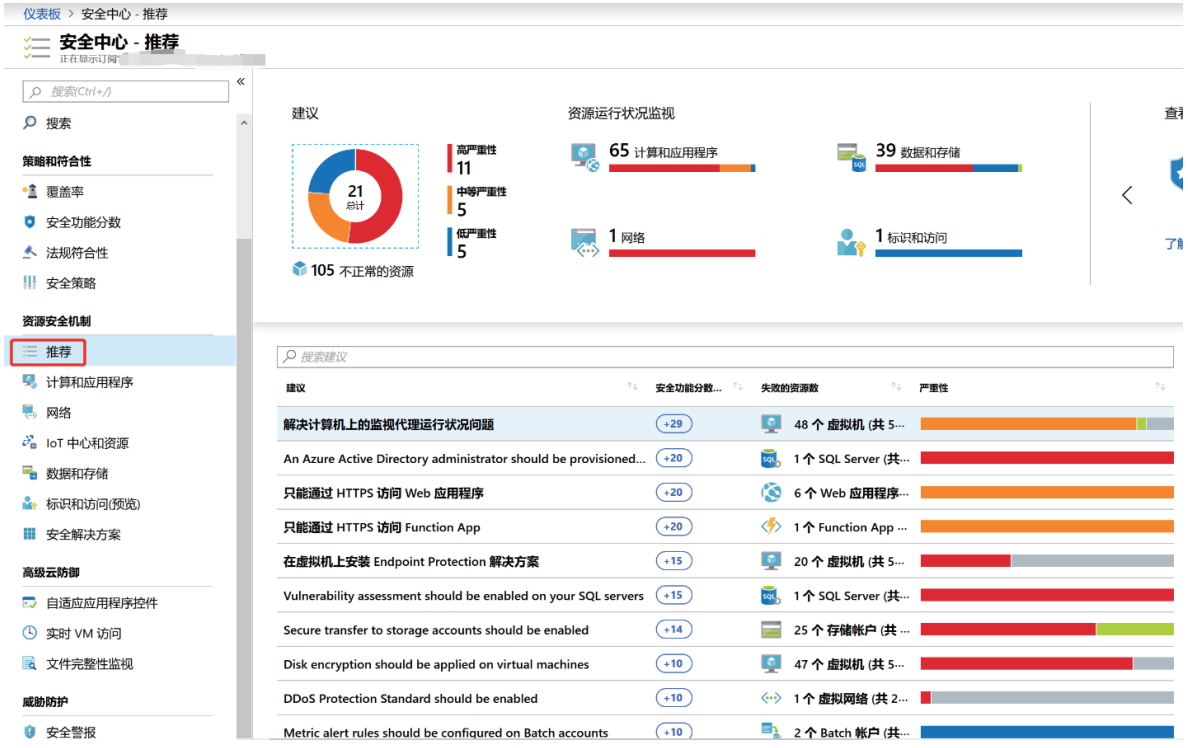
2.1.4 一站式全方位管理

根据以上针对不同环境的加固策略，企业可以拥有相对安全的环境。考虑到企业规模的不同，云端业务系统的不同。IT 往往会面临业务系统上线周期短，不同系统的安全策略不同等问题。特别是在上云的初期，没有掌握安全上云的方法，从而可能导致云端系统的端口暴露，误用公网 IP 地址等问题，需要一个更好的安全指引的方式。

在 Azure 端，基于对以上业务场景需求的考量，Azure Security Center 承担起了引导客户对系统及部分应用层面的安全防护，给出建议及策略，帮助客户快速搭建云端的安全防护体系。

客户只需要一键给所需要管控的订阅安全代理，就可以在几分钟以后对云端机器的安全情况有个全面的了解：

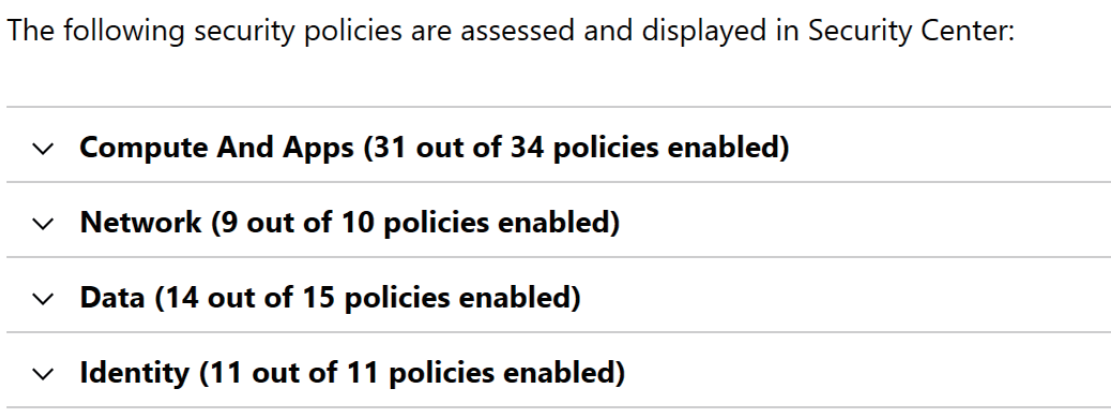
安装完代理以后，用户就可以在'资源安全机制'里，从虚拟机，网络，数据存储，身份等维度，看到云端业务环境目前所可能面临的问题：



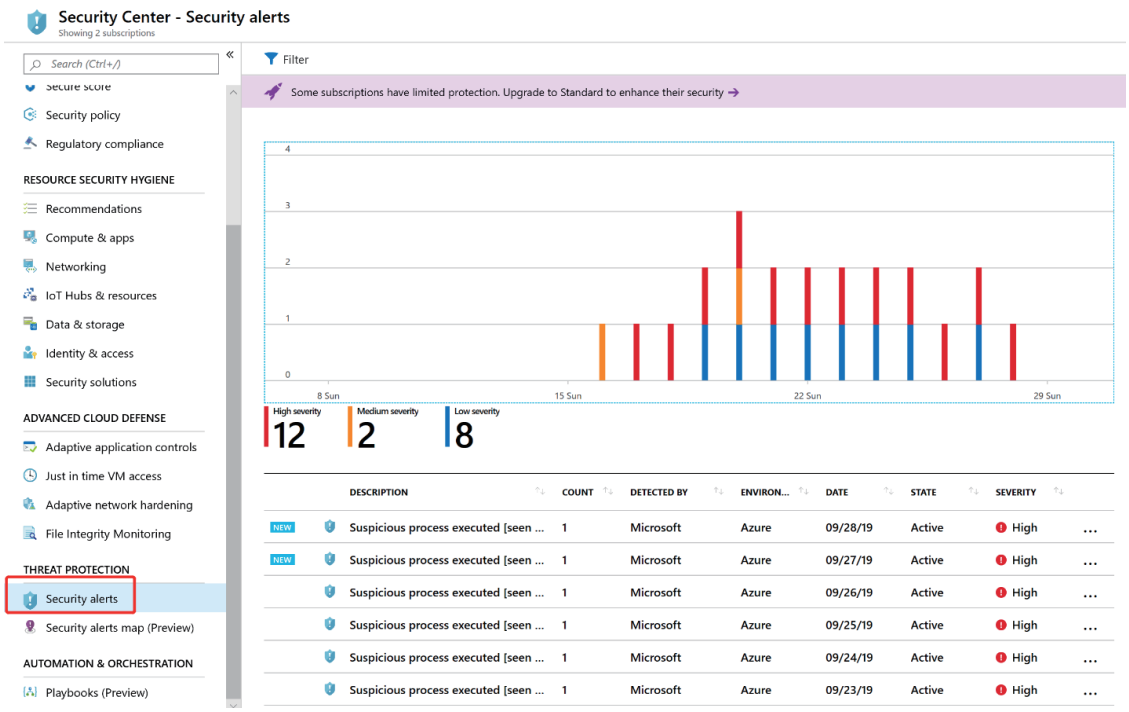
安全往往不是一蹴而就的事情，企业环境每一层安全策略的提升可能就意味着会给业务带来一定的阻碍，所以安全的提升需要 IT 部门的规划，来整合，考量每一步的安全提高。因此 Azure 安全中心也顺应安全或者 IT 部门的需求，建立了安全功能分数的体系，在一开

始给企业安全进行打分的基础上，通过每个建议，给出相应的严重性，覆盖的面，以及对应实行安全防护后所提高的安全功能分数，来帮助企业决策，优先完成哪方面的安全提升，帮助企业梳理构建安全框架的路线图。

微软通过一方团队，Microsoft Security Response Center(MSRC),Microsoft Cyber Defense Operations Center(CDOC), Digit Crime Unit(DCU) 等团队的经验及发现，从合规的调度，为客户定义了四个角度，共 70 条建议，帮助客户可以在一开始，建立起初步的安全防御体系。

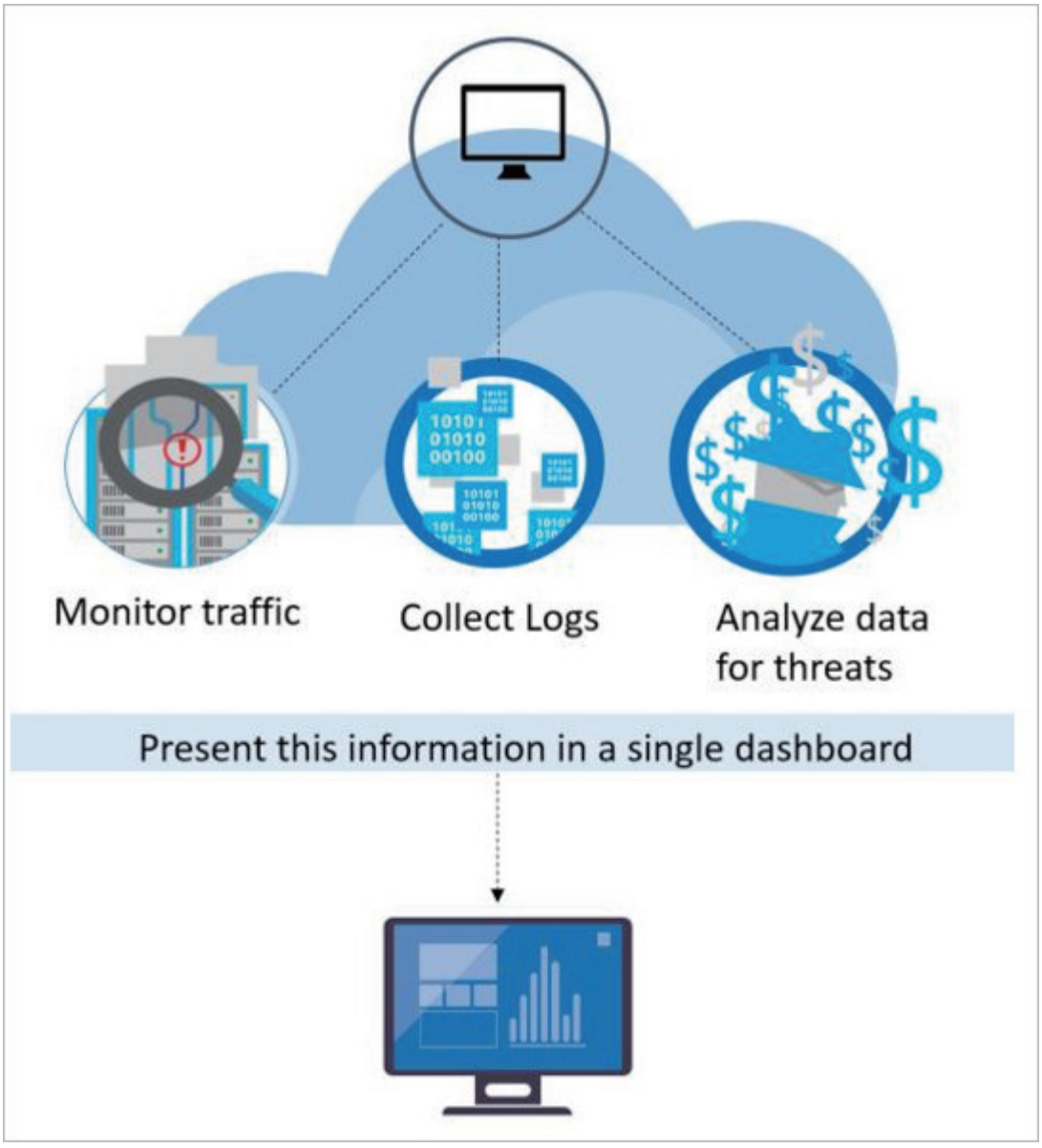


再建立完整套体系以后，企业还需要一套监控平台，基于所建立的安全策略，来监控是否存在一些可疑行为，试图攻破设定的安全边界。这里就可以通过 Azure 安全中心的安全警报功能，实时监控云端的环境：



正如前文所提到的，现如今的攻击者攻击的目的以及他们的群体规模及产业的影响，使

得攻击者的行为和手段也越来越先进，企业如果继续依照以往的方式，根据自身团队的经验及市面上所了解到的工具，组合使用来抵御现在的入侵将变得异常困难。



正是在这样的大环境下，安全中心因此使用各种高级安全分析，不仅仅针对目前成熟的一些攻击方式例如 Kill Chain 模型，还充分利用大数据和机器学习技术的 . 跨整个云平台结构对事件进行评估，检测那些使用人工排查方式不可能发现的威胁，并预测攻击的发展方式。现如今，安全中心会利用的微软大平台中的分析有如下几个方面：

- 集成威胁智能：利用 Microsoft 产品和服务、Microsoft 数字犯罪部门（DCU）、Microsoft 安全响应中心（MSRC）以及外部源提供的全球威胁情报，查找已知的不良执行组件。
- 行为分析：运用已知模式发现恶意行为。
- 异常检测：使用统计分析生成历史基线。 如果出现与已知基线偏离的情况，并且这

些情况符合潜在攻击载体的行为，则会发出警报。

正是因为 Microsoft 安全研究人员始终在不断地寻找威胁，应对威胁，不论是 Microsoft 在云中遇到的，或者是本地环境通过安全工具所接收到的，每时每刻，微软的安全人员都需要面对大规模的遥测数据，通过丰富的数据集和多样化的集合，发现新的攻击模式以及其本地使用者和企业产品以及其联机服务的趋势。 因此，当攻击者发布新的越来越复杂的漏斗利用方式时，安全中心就可以快速更新其检测算法。 从而可以让用户始终跟上变化莫测的威胁环境。

2.2 利用大数据分析赋能应用环境进行主动防御

介绍完上述针对不同资源的建议事件，我们来继续深入看在防御的功能点上，如何才能真正做到不同程度对于云端生产环境的保护。

在现在的企业环境中，为了做到更好的防御，企业首先需要做到的就是减少自己攻击面，不暴露自身的任何信息到外部，也正是出于这样的一个概念，企业中开始流行一个概念叫做“Zero Trust”，即对于每一个访问企业服务器，应用或数据的访问者保持零信任。每台服务器在被访问时就应该询问访问者：“你是谁？”，“你为什么要来？”，“你要去哪里？”。

2.2.1 你是谁（Who？）

在对企业发起任何的攻击之前，拿到访问凭据是所有事件的开始，因此企业需要在一些关键的账号和环境中，建立零信任体系（会在 Chapter 3 中做详细介绍），对所有来访者都要结合不同的条件进行验证，比如访问者做多因子认证来做身份的二次校验，或者需要来自信任的 IP 源等。此部分将会在 Chapter 3 中做更详细的展开。

2.2.2 “你为什么要来？”

当攻击者凭着初始凭据进到企业内部以后，他们会进行长时间的潜伏，其首要目标，就是获得企业超级管理员的凭据，从而可以直奔企业的核心数据。而有些防范疏忽的企业往往一个超级管理员就可以登录企业大部分的服务器，或者很多服务器的管理员账号的用户名和密码的组成有很大的相似之处。从而让攻击者可以肆意地在企业环境中游动。

因此，对于所有的服务器或者数据的访问都推荐依照 JIT（Just In Time）原则来进行访问。其道理就是，针对核心的服务器，首先需要减少所有不必要的超级管理员的账号，其次，相关操作人员再登录时，需要额外审批才能在有限时间内进行访问等操作，这样才能有效的降低企业生产环境所暴露出的攻击面。

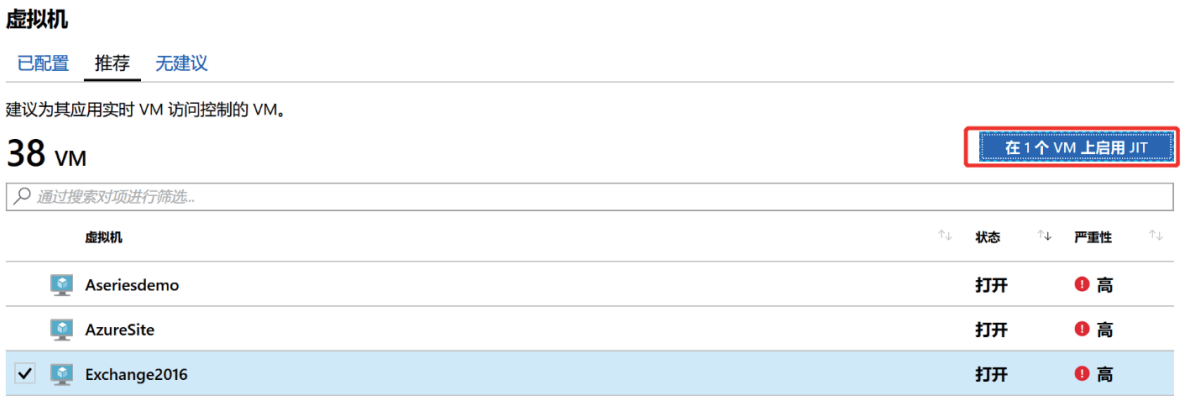
作为 Azure 安全中心的核心功能之一，实时 VM 访问，就是为了给到客户最直接的管理

企业云端核心虚机的访问控制的方式。

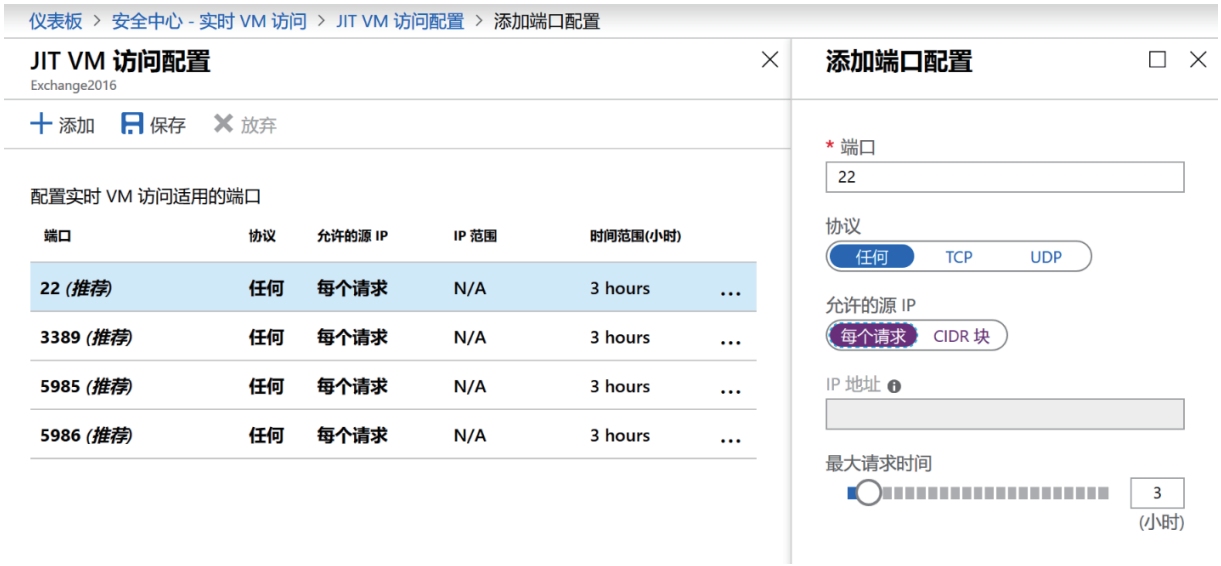
其原理是通过根据客户设定的 JIT 的策略，来实时改变虚机上的网络安全组（NSG）的策略，保证特定端口和访问来源的 IP 保持关闭状态，只有在来访的理由得到了企业相关人员允许，才会对运维窗口期进行有限的开放。

接下来我们一起来看下如何通过 Azure 安全中心来实现 JIT 管控 .

首先选择你的目标管理虚机，点击"在 X 个 VM 上启用 JIT":



之后，你就可以配置如下图，对每个端口，访问来源的 IP 地址进行可用访问时效的限定，



再设置完毕后，点击保存之后，那虚机就会对于设定的端口从 NSG 规则上设定为关闭状态，我们回到上一页就可以看到，虚机会转移到"已配置"的数据下面。之后如果需要对于 JIT 策略中规定的端口进行连接和访问，就需要从安全中心中，选中该虚机，"请求访问"。

并且只有如下图所示，指定访问的源 IP，才能开启 NSG 规则，让该端口只对你需要针对的 IP 可访问：

并且，再有效的时间到期后，该端口又会关闭，但已经连接的访问不会受到影响，将可以继续访问该虚机。

2.2.3 "你要去哪里？"

当用户在经过层层审核，进入到服务器以后，我们仍旧需要秉持"Zero Trust"原则，对于用户的行为进行有效的约束。我们从服务器自身来看，企业中的每台服务器都应该各司其职，跑着某一些特定的应用，特别在云端，用户可以通过对于 CPU 和内存的拆分，将原先运行在本地同一台物理机上的几个应用分隔到云端的不同机器上，相关之间的环境完全独立。那即使用户登录到其中的一台服务器上，也需要主动阻止其访问比如游览器或者其他应用，减少引入其他的危害。

Azure 安全中心中的"自适应应用程序控件"就可以帮助企业管理云端 Windows 服务器中，建立应用的规则，从而加强虚机对于恶意软件的防御能力。

接下来我们进入"自适应应用程序控件"来看下如何对虚机的可访问的应用进行控制。

如果你刚开始使用此功能，则在推荐的目录下不会有任何的组别出现，因为安全中心需要至少两周的数据，学习每个虚机的行为，才能为虚机创建基线，并将行为类似的虚机归纳成一个虚机组给出建议。

我们监控了一台 Exchange 2016 的 Server（生产环境推荐使用 Exchange Online）为例，来看下安全中心推荐的规则控制，我们点击"GROUP1"。

我们可以看到，在这一组别中包含的虚拟机以及改虚拟机上频繁使用的应用，点击创建以后，安全中心就可以借助 AppLocker 为以下应用针对某一些用户开启白名单访问规则。

等待片刻后，规则生成完成，该组别就会转到"已配置"目录下，我们接着来看下该组别虚机的监控情况：

对于自动创建的应用程序控制规则，用户可以选择"审核"，即不强制实行规则，而是监控 VM 上的行动，如果企业在初始实施过程中，建议对于大多数的机器应用此项规则。"强制"则自然是明确阻止不允许的应用程序，建议再实行一段时间"审核"状态下的 VM 后，对于特定的虚机进行强制管控。

如果客户觉得自动学习到的虚机上的应用程序白名单不够完善，也可以手动通过"策略扩展"部分，手动添加允许的应用程序的路径。

根据虚机上应用的属性的不同，以及访问用户的不同，Azure 安全中心会按照"发布服务器允许列表规则"，"路径允许列表规则"以及"哈希白名单规则"将不同的的被允许的应用自动归类。如果对于允许的用户有不同的设置，用户也可以通过右侧点击相应的规则来勾选不同的允许的用户。

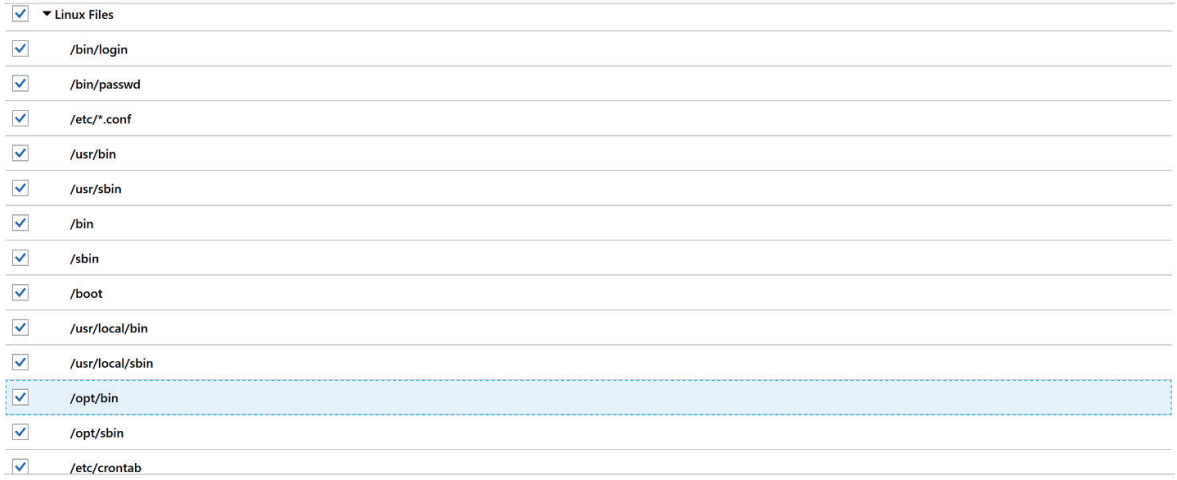
在对虚拟机的访问和行为进行控制后，实际对于机器自身的监控也是必不可少的，例如定时 check 注册表的变化，或者操作系统级别是否有更改。

在 Azure 的安全中心里，就提供了对于这些可能代表了遭受攻击后所造成的更改的监控模块—文件完整性监视（FIM），在启用了 FIM 以后，安全中心会对以下文件的活动进行监视:

- 文件和注册表的创建与删除
- 文件修改（文件大小、访问控制列表和内容哈希的更改）
- 注册表修改（大小、访问控制列表、类型和内容的更改）

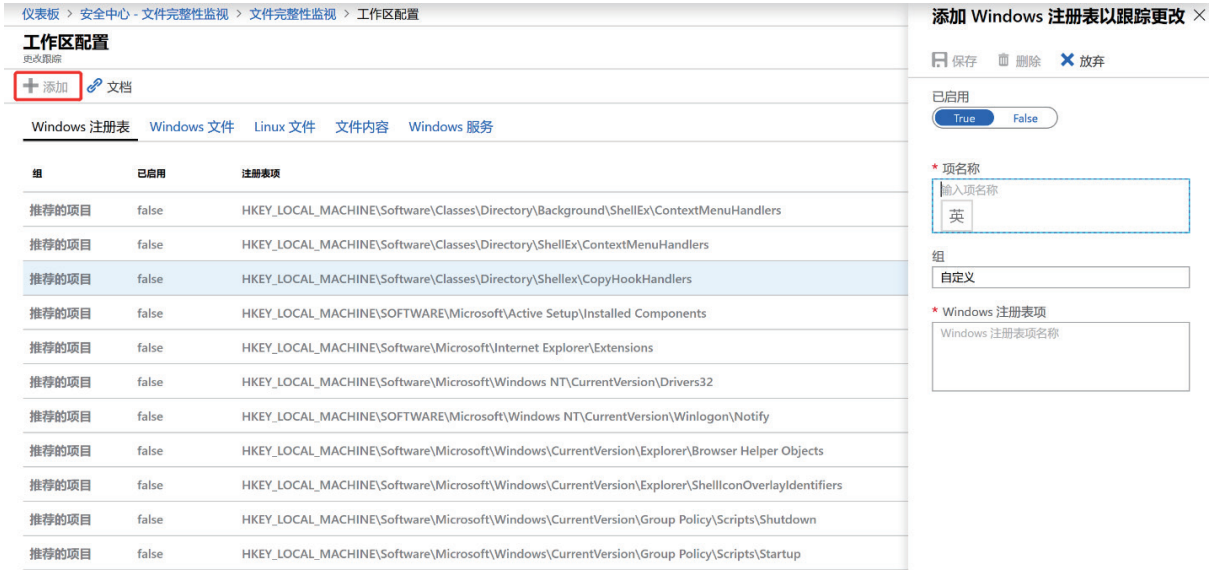
这里，我们以一台 Linux 的虚机为例

在这个工作区中，我们来细看下，对于工作区内的 Linux 虚机会查看哪些文件地址：



勾选完所需要追踪的文件路径，点击启用 FIM 后，就会对所应用的虚机进行更改追踪。

如果想要对自定义的一些文件路径也进行追踪，可以点击“设置”，来添加某个注册表或者文件的改动。



2.3 企业环境之 BYOD 设备管控

随着下一代移动网络提供更高的速度和更低的延迟，我们使用技术的方式将发生巨大变化。虽然网络连接性的改善带来了新的挑战和风险，但网络安全领导者仍在不停研发各种各样的新技术，以提高跨设备的安全性。一直以来，企业都困扰于怎样管控各种各样的企业设备。尤其在电子设备日新月异的现代生活中，BYOD 作为员工改善办公体验的重要手段之一，怎样管理大量的 BYOD 设备给 IT 部门带来了大量的挑战。Gartner 预测，2019 年全球在信息安全产品和服务上的支出将达到 $ 124B，比 2018 年投资的 $114B 增长 8.7%[17]。在 4G 业务的全面推进之下，移动信息化已经把移动端设备变成员工使用邮件周知、协同办公、差旅

17 Top 10 Cybersecurity Companies To Watch In 2019，https://www.forbes.com/sites/louiscolumbus/2019/06/16/top-10-cybersecurity-companies-to-watch-in-2019/#4c5860276022

办公和信息交互的至关重要的入口。IT 团队必须能够解决移动设备管理所带来的各项挑战，以充分保护企业组织，但同时仍然需要留有足够的灵活性来保障移动办公带来的便利和收益。基于移动设备的特点，IT 需要从各个方面提供安全策略，包括软件、系统、硬件等，在保证安全的前提下，做到有条件的访问，对外部人员封闭，而内部人员开放。那么 IT 部门经常会思考，“哪个产品适合我的组织、移动应用程序管理 (MAM) 还是移动设备管理 (MDM) 呢？”答案可能是两者都有，也可能是二者之一，这取决于实际的应用场景。

2.3.1 MDM,MAM 管理

- 移动设备管理（MDM）

在以往的办公环境中，出于安全角度考虑同时也为了方便统一管理，公司经常会给员工发放指定的电子设备，如电脑、手机和平板等。移动设备管理（Mobile Device Management，即 MDM）可以帮助 IT 实现完整的设备管控，包括：设备注册、设备配置、管理和保护、设备退役等等。MDM 除了完成终端配置，还可以对于设备中的应用程序和文件进行保护。

通常来说，企业使用 MDM 会出于以下原因：

1) WIFI/VPN – 需要链接企业网络实现高效工作，可以在 MDM 上进行无缝配置
2) 应用程序 – 可以帮助 IT 部门将需要的 app 推送至终端设备，实现高效管理，指派相应的办公软件，比如安全防护应用等。
3) 安全需求 – 某些组织需要设备符合相应的法律规范，或者需要指定相应的设备实现其对于设备方面的策略需求。例如，需要使用 MDM 加密整个设备，或者定期查看某个设备上的应用程序报告。

- 移动应用管理（MAM）

移动应用管理（Mobile Application Management，即 MAM）可以通过与云结合，向终端用户发布授权的应用，同时还可以对与敏感数据进行管理和保护。MAM 的主要功能包括为用户发布、推送、配置、保护、监视和更新移动应用等。

MAM 可保护应用程序内组织的数据。 通过无需注册的 MAM (MAM-WE)，可以在几乎任何设备上管理包含敏感数据的工作或学校相关应用，包括自带设备办公 (BYOD) 场景下的个人设备。许多生产型应用，例如 Microsoft Office 应用，都可以通过 Intune MAM 进行管理。

对支持 BYOD 的组织而言，不进行 MDM 而进行 MAM 是非常普遍的。 通过在 Exchange Online 上部署条件访问策略，可让用户从支持 MAM 保护的 Outlook Mobile 中访问电子邮件。 下面是可能只需要管理个人设备上的应用的原因：

1) 用户体验 - MDM 注册包括许多由平台强制执行的警告提示，这些提示通常会导致用户最终决定不在其个人设备上访问电子邮件。 MAM 大大减少了用户的担忧，因

为他们一次只会收到一个弹出窗口，以知晓 MAM 保护已到位。

2) 符合性 - 某些组织需要符合一些策略的要求，这些策略对个人设备需要较少的管理功能。 例如，MAM 只能删除应用中的公司数据，与此相反，MDM 能够删除设备中的所有数据。

➢ MDM 和 MAM 的场景对比

如上所述，条件访问可以通过注册设备或者使用特定 App 实现。同时还可以设定很多的附加条件，比如：

1) 用户身份识别
2) 位置是否可信任
3) 登录的风险级别
4) 设备平台

除此之外，还会有很多其他的常见风险，下表列出了常见的一些风险，以及 MDM 和 MAM 应对该风险的方法：

表 2.3.1 MDM 和 MAM 应对常见风险的方法

风险	MDM	MAM
数据访问未经授权	需要组成员身份	需要组成员身份
	需要注册设备	需要受保护的应用
	需要采用特定位置	需要采用特定位置
用户帐户遭到泄露	需要进行 MFA	需要进行 MFA
	阻止高风险用户	阻止高风险用户
	设备 PIN	应用 PIN
设备或应用遭到泄露	需要兼容设备	在应用启动时进行越狱检查
	加密设备数据	加密应用数据
设备丢失或被盗	删除所有设备数据	删除所有应用数据

意外共享数据，或将数据保存到不安全的位置	限制设备数据备份	限制剪切 / 复制 / 粘贴
	限制另存为	限制另存为
	禁用打印	n/a

2.3.2 如何进行移动端设备安全管控（Mobile）

对于任何的 IT 管理员来说，保护组织的资源和数据的安全都是头等任务，那么设备管理就是其中的主要任务之一。在现代的办公环境中，每个员工都拥有很多的移动设备，比如手机、平板或者便携电脑，而在几乎每台设备上，都可以打开或者共享文件，访问网站以及安装应用程序，这就大大增加了 IT 人员的维护负担。移动端设备安全管控就是十分必要的。

使用移动设备安全管控，组织会授权指定的人员和设备才能访问特定信息，而同样的，由于设备符合相应的安全规定，设备用户也可以轻松的从手机方案工作数据。Microsoft Intune 可以帮助企业管理并保护移动端设备安全。Intune 可以提供 MDM 和 MAM，做到以下一些方面：

1) 支持多种移动环境，并且可以安全管理 iOS，Android，Windows 和 macOS 设备。
2) 确保设备和应用符合组织的安全要求。
3) 创建有助于确保组织数据在公司拥有的和个人设备上安全的策略。
4) 使用移动解决方案来实施这些策略，并帮助管理设备，应用程序，用户或者组。

Intune 包含在 Microsoft 365 中，并与 Azure Active Directory（Azure AD）集成。Azure AD 帮助控制谁有权访问以及他们有权访问什么。

提到移动设备安全管控，那么第一步来说，一定是设备的分发和配置，当员工发放公司设备时，需要确保该设备是注册的、可管控的，并且该设备上的数据是安全的，这是 IT 在日常的工作环境中经常碰到的场景之一。那么 Intune 是如何帮助企业进行设备的发放和并且进行设备生命周期管理的呢？

- 设备生命周期管理

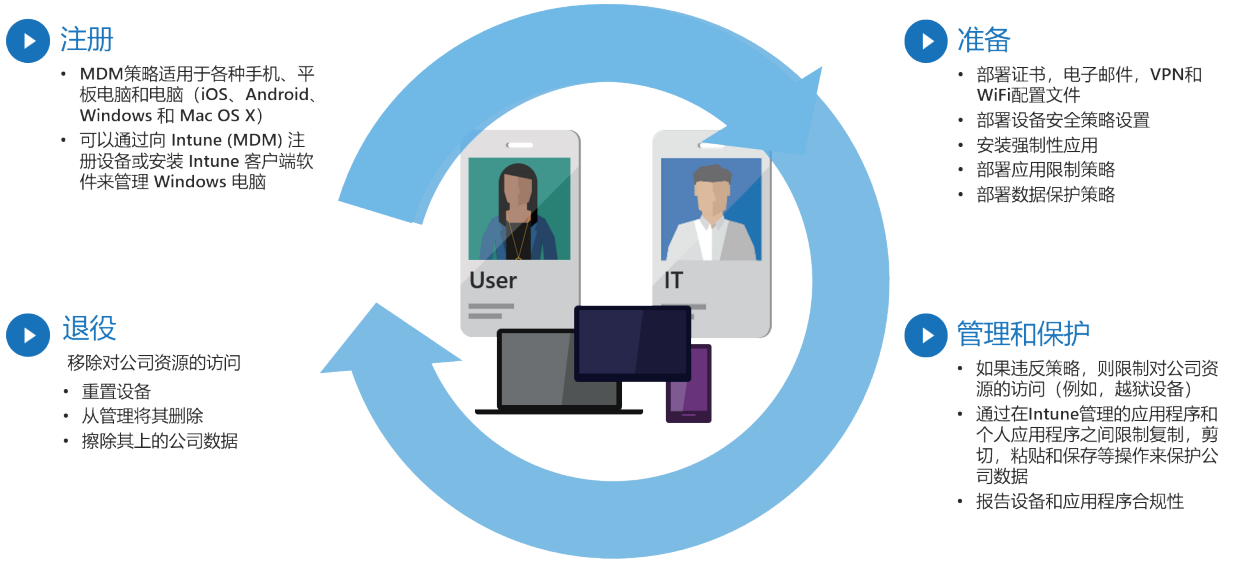


图 2.3.1 设备生命周期管理

设备生命周期管理主要分为 4 个阶段，从注册设备到配置和保护，再到设备退役时停用设备。

注册：移动设备管理 (MDM) 策略适用于各种手机、平板电脑和电脑（iOS、Android、Windows 和 Mac OS X）。 如果企业需要能够管理设备（比如公司拥有的设备），第一步便是设置设备注册。 注册可以通过向 Intune (MDM) 注册设备或安装 Intune 客户端软件来管理 Windows 电脑。

配置策略：将设备注册只是第一步。 若要充分利用所有 Intune 功能并确保设备安全且符合公司标准，IT 人员可以从 Intune 提供的各种策略中选择。 这些策略可以帮助配置受管理设备运作方式的方方面面。 例如，对于含有公司数据的设备，用户是否应该有密码？ 是否设置公司 Wi-Fi？ 以下是可用的配置选项类型：

a) 设备配置：能够配置所管理设备的特性和功能。 例如，可以要求在 Windows Phone上使用密码，或禁用 iPhone 的照相机。
b) 公司资源访问权限。Intune 可以自动配置你管理的设备来访问公共公司资源，从而减少各种负担。
c) Windows 电脑管理策略（使用 Intune 客户端软件）。向 Intune 注册 Windows 电脑会提供给用户最多的设备管理功能。

管理和保护： 在现代 IT 世界中，保护设备免受未经授权的访问是一项非常重要的任务。 除了设备生命周期的配置步骤中的项之外，Intune 还提供以下功能来帮助保护你管理的设备免受未经授权的访问或恶意攻击：

a) Multi-Factor Authentication。 对用户登录添加一层额外的身份验证可以帮助增强设备安全性。 很多设备支持多重身份验证，这要求提供第二重身份验证（如电话呼叫或短信），用户才能获得访问权限。

b) Windows Hello 企业版设置。 Windows Hello 企业版是一种备用登录方法，可让用户使用"手势"（如指纹或 Windows Hello）进行登录，而无需密码。

c) 保护 Windows 电脑的策略（使用 Intune 客户端软件）。当你使用 Intune 客户端软件管理 Windows 电脑时，可以使用允许你在所管理的电脑上控制 Endpoint Protection、软件更新和 Windows 防火墙的设置的策略。

停用设备：设备丢失是企业最不希望发生的事情，这意味着设备上的数据将会面临非法访问的危险，如何保护丢失的设备上的数据是一个必须要面临的问题。或者是设备使用年限到期需要更换时，也同样面临着设备退役的问题。Intune 提供了多种方法来停用设备，例如：重置设备、擦涂设备上公司的数据等等。

设备生命周期管理实现了管控硬件设备的生命周期，并确保该设备的合规性及安全性。那么在管理设备的同时，Intune 也提供了整套的应用程序生命周期管理，来帮助企业管理应用程序，同时确保应用程序上的数据信息安全。

➢ 应用程序生命周期管理

应用程序生命周期管理主要由 5 个阶段组成：应用程序的添加、部署、配置、保护和停用。

添加：应用部署的第一步是添加需要管理的应用并将其分配到 Intune 中。使用 Intune，可以添加不同的应用类型，包括内部编写的应用（业务线）、应用商店中的应用、内置应用以及 Web 应用。 有关应用类型的详细信息，请参阅如何将应用添加到 Microsoft Intune。

部署：在将应用添加到 Intune 后，就可以将其分配到你管理的用户和设备。 Intune 让这一过程变得十分简单，部署应用后，可以在 Azure 门户中监视 Intune 中的部署是否成功。 此外，在一些应用商店中，如 Apple 和 Windows 应用商店，可以为公司批量购买应用许可证。Intune 可以同步这些商店的数据，从而让你直接从 Intune 管理控制台部署应用，并跟踪许可证使用情况。

用户密码重置策略：作为应用生命周期的一部分，应用程序将定期发布新版本。 Intune 提供一些工具，可轻松地将应用更新到较新版本。 此外，还可以为一些应用配置额外的功能，例如：

a) iOS 应用配置策略为应用运行时所使用的兼容 iOS 应用提供设置。 例如，某个应用可能需要设置必须连接的服务器的名称。

b) Managed Browser 策略帮助你为 Intune Managed Browser 配置设置，该浏览器将取代默认设备浏览器并且可以限制用户可以访问的网站。

图 2.3.2 应用程序生命周期管理

保护：Intune 提供了许多方法来帮助保护应用中的数据。 主要方法是：

a) 条件访问，根据指定的条件控制对电子邮件和其他服务的访问。 条件包括设备类型或者是否符合设备合规性策略。

b) 应用保护策略作用于各个应用，以帮助保护它们使用的公司数据。 例如，你可以限制在非托管应用和你管理的应用之间复制数据，或者可以阻止应用在已越狱或取得 root 权限的设备上运行。

停用：最后，当部署的应用过期时，并且需要将其删除。Intune 使得从服务停用应用变得简单。

➢ 移动应用程序管理策略

由于电子设备的快速迭代，终端用户通常喜欢使用自己的电子设备进行移动办公，那么在非 MDM 的设备上，如何保证公司的数据安全呢？

假设一个场景，一个职员使用自己的移动设备进行办公，他的手机中有大量的应用程序，有他熟悉的办公应用程序，也有工作之外的个人的应用程序，甚至可能考虑使用这些个人应用程序来提高工作效率。随着 Intune 的加入，IT 专业人员对个人设备有了一个不同的视角。通过新的多身份管理功能，用户可以使用相同的办公移动应用程序访问他们的个人和工作帐户，同时只将 MAM 策略应用于他们的工作帐户，在保障员工办公体验的同时，保证了公司的数据安全。

对于 IT 专业人员来说，管理的企业应用程序和用户的个人应用程序之间仍然存在明显的分离。但是，这并不影响用户对应用程序的访问。通过在应用程序级别应用 MAM，IT 专业人员可以在支持移动生产力的同时，仍然能够使用统一管理的 Office 移动应用程序保护公司数据和资源。

那在 MDM 管理设备上应用 MAM 策略和非 MDM 设备上应用 MAM 策略有何不同呢?

在 MDM 管理设备上应用 MAM 策略时，MAM 策略可以提供以下额外功能：

a) 保护公司数据不泄露给个人的应用程序和服务

b) 对移动应用程序应用限制 (save-as、剪贴板、PIN 等)

c) 在不删除设备上的应用程序的情况下，擦涂应用程序上的公司数据

对于没有注册任何 MDM 解决方案的 BYOD 设备，MAM 策略可以帮助在应用程序级别保护公司数据。通过身份验证管理，可以保证只有在工作账户下才可以访问公司数据，然而，也有一些限制需要注意，比如：

a) 无法将应用程序部署到设备上。最终用户必须从商店获得应用程序。

b) 不能在这些设备上提供证书配置文件。

c) 不能在这些设备上提供公司 Wi-Fi 和 VPN 设置。

2.3.3 如何进行本地端设备安全管控（Windows 10） （Windows Defender ATP）

本地端无疑是现代工作环境的重要场所之一。员工处理各种纷杂的事务、开发、沟通都离不开本地端的设备。而由于本地端通常存有大量的敏感且重要的信息，本地端的设备安全也是企业日常非常重视的工作。保护企业客户从未像今日这样富有挑战性，安全威胁日益明目张胆且具有高度复杂性。即使企业可能拥有最好的防御，老练的黑客们也会使用各种各样的工具、零日漏洞、甚至是错误配置来攻击公司的网络，入侵公司的整个体系。攻击者会破坏公司网络，窃取数据，侵犯隐私，破坏客户的可信任度，这些攻击所造成的成本损失往往令人难以置信，并且不止是成本上的损失，间接对于公司声誉所造成的影响会更大。

近日，保险咨询公司 Marsh 发布了携手微软展开的一项调查，显示大多数企业高管已将网络攻击视作其面临的最大问题，且远超对经济的不确定性预期、以及品牌和监管的损益。这项调查涉及全球 1500 多名企业领导人，其职责涵盖了对瞬息万变的组织风险采取适当的应只书昔施。然而受访者普遍表示，涉及网络安全的保险政策，已较过去两年变得更为常见。2017 年的时候，Marsh 和微软发现有 62% 的受访者将网络攻击视作前五大风险。但是今年，这一数字已提升至 79%[18]。

McAfeeLabs 在 2019 第一季度的最新威胁报告中称，平均每分钟在网络空间发现 504 个新的威胁，而伴随着犯罪分子采取新的策略和代码创新，勒索软件正在不断复苏。这一季度，地下网络犯罪分子盗取了超过 22 亿个账户凭证。68%的目标攻击利用鱼叉式网络钓鱼进行初始访问，77%则依靠用户操作来执行[19]。

18 Microsoft: Cyberattacks now the top risk, say businesses, https://www.zdnet.com/article/microsoft-cyber-attacks-now-the-top-risk-say-businesses/

19 网络犯罪分子采取新策略，勒索软件增长超 118 %，https://mp.weixin.qq.com/s?__biz=MjM5NjA0Njgy-MA==&mid=2651077646&idx=4&sn=ede30e8f96260cd4a6a3db6aa3fc1d8c&chksm=bd1fae858a6827931270387eb13493e6f63b-c581f1989b30ed6638602cc8fd103de809f68fba&mpshare=1&scene=1&srcid=&sharer_sharetime=1569118309770&sharer_sha-

面对演化的越来越高级的攻击，微软一直致力研究于怎样对抗这些日益成熟且完善的黑客攻击。Windows Defender ATP 是微软推出的一款企业级安全防护服务，它可以帮助企业客户检测、调查和响应针对其网络的高级和有针对性的攻击。 Windows Defender ATP 平台是将多个产品的功能集合在一处的平台，从而使安全操作团队能够有效地管理组织的网络。基于 Windows 10 今天提供的现有安全特性和服务（预入侵），Window Defender ATP 为 Windows 10 安全栈提供了一个新的后入侵层保护。结合 Windows 10 内置的客户端技术和强大的云服务，它还可以检测出能够通过其他防御的目标威胁和攻击，为企业提供跨端点调查入侵的信息，并提供响应建议。

Windows Defender ATP 可以支持 6 大功能，分别为：减少攻击面、下一代防护技术、端点检测及回应、自动检测及补救、安全状态和高级侦察。下面将会对每一个功能进行详细介绍。

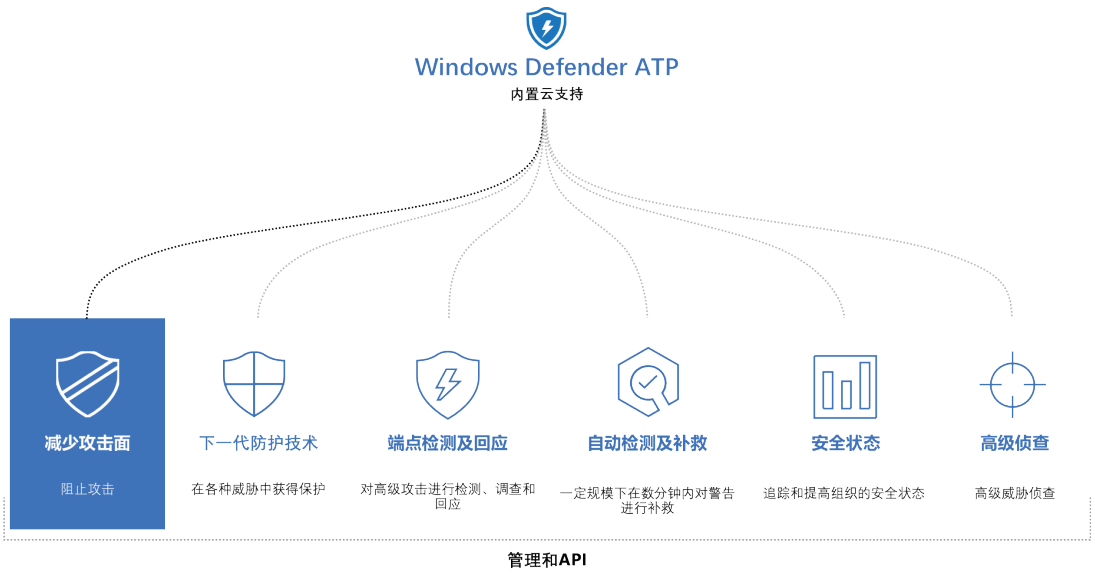


图 2.3.3 Windows Defender ATP 功能概览

1) 减少攻击面

➢ 应用程序防护

应用程序防护专为 Windows 10 和 Microsoft Edge 设计，可以帮助隔离企业定义的不受信任的站点，从而在员工浏览 Internet 时为公司提供防护。 作为企业管理员，需要定义哪些是受信任的网站、云资源和内部网络。 而列表上的所有内容均被视为不受信任。如果员工通过 Microsoft Edge 或 Internet Explorer 访问不受信任的网站，则 Microsoft Edge 将在启用 Hyper-V 的隔离容器中打开这些网站，这将与主机操作系统隔离开来。 这种容器隔离意味着如果不受信任的网站为恶意网站，则主机电脑

reid=4fa412564b200431377831cde0421046#rd

将会受到保护，并且攻击者无法获得企业数据。 例如，此方法可让隔离容器成为匿名容器，因此，攻击者无法获得你员工的企业凭据。

应用程序防护可应用于如下四种设备：

a) 企业台式机：这些台式机已加入域并由组织管理。配置管理主要通过 System Center Configuration Manager 或 Microsoft Intune 完成。 员工通常具有标准用户权限并且使用有线企业网络。

b) 企业移动笔记本电脑：这些笔记本电脑已加入域并由组织管理。 配置管理主要通过 System Center Configuration Manager 或 Microsoft Intune 完成。 员工通常具有标准用户权限并且使用无线企业网络。

c) 自带办公设备 (BYOD) 移动笔记本电脑：这些个人拥有的笔记本电脑未加入域，但由你的组织通过 Microsoft Intune 之类的工具管理。 员工通常为设备上的管理员，工作时使用无线企业网络，在家时使用个人网络。

d) 个人设备：这些由个人拥有的桌面或移动便携式计算机不是由组织加入或管理的。 用户是设备上的管理员，并在外部使用无线个人网络，而不是在家中或可比较的公共网络。

- 应用程序控制

  由于每天都会有数千个新的恶意文件产生，使用传统的方法，如反病毒解决方案，对新的攻击的防御并不充分。在大多数组织中，信息是最有价值的资产，确保只有经过批准的用户才能访问这些信息是非常必要的。然而，当用户运行一个程序时，该程序具有与用户相同的数据访问级别。因此，如果用户有意或无意地运行恶意软件，敏感信息很容易被删除或传输出组织。考虑到当今的威胁环境，应用程序控制是保护企业的重要防线，并且相对于传统的防病毒解决方案具有很大的优势。具体地说，应用程序控制从传统的应用程序信任模型（默认情况下假定所有应用程序都是可信的）转向应用程序必须得到许可才能运行的模型。Windows Defender 应用程序控制 (WDAC) 可以通过限制允许用户运行的应用程序和在系统内核（内核）中运行的代码来帮助减轻这些类型的安全威胁。

- 网络保护：网络保护有助于减少设备来自基于 Internet 的攻击面。 它防止员工使用任何应用程序访问可能托管欺诈邮件、攻击和 Internet 上的其他恶意内容的危险域。

- 受控文件夹：受控文件夹访问权限帮助你保护重要数据免受恶意应用和威胁（如勒索软件）的损害，它通过查看已知的受信任应用列表来保护文件夹内的数据。 如果应用包含在受信任的软件列表中，则受控文件夹访问仅允许应用访问受保护的文件夹。 如果应用不在列表中，则受控文件夹访问将阻止其对受保护文件夹内的文件进行更改。受控文件夹可以通过 Windows 安全应用，或者从 System Center

Configuration Manager (SCCM) 和 Intune (对于托管设备) 打开。

- 攻击面减少规则：攻击表面减少规则有助于防止恶意软件使用恶意代码感染计算机的行为。该行为包括 :
  a) Office 应用或 Web 邮件试图下载或运行文件时使用的可执行文件和脚本
  b) 模糊脚本或其他可疑脚本
  c) 应用在正常的日常工作期间通常不会启动的行为。
- 网络防火墙：具有高级安全性的 Windows Defender 防火墙是分层安全模型的重要部分。 通过为设备提供基于主机的双向网络流量筛选 , Windows Defender 防火墙将阻止未经授权的网络流量流入本地设备。 网络防火墙可以给公司带来如下的益处：
  a) 降低网络安全威胁的风险： Windows Defender 防火墙减少了设备的受攻击面 , 从而为纵深防御模型提供了一个额外的层。 减少设备的受攻击面会增加易管理性并减少成功攻击的可能性。
  b) 保护敏感数据和知识产权：它提供对受信任网络资源的可伸缩的分层访问 , 帮助加强数据的完整性 , 并有选择地帮助保护数据的机密性。
  c) 扩展现有投资的价值：由于 Windows Defender 防火墙是操作系统附带的基于主机的防火墙 , 因此不需要其他硬件或软件。Windows Defender 防火墙还可以通过应用程序编程接口 (API) 来补充现有非 Microsoft 网络安全解决方案。

2) 下一代保护

下一代保护功能增强了安全性，还提供了更传统的安全措施。 下一代服务使用机器学习和云计算保障企业网络上的所有设备安全。

下一代保护服务包括：

a) 始终进行扫描（也称为 “实时保护”），用于高级文件和进程行为监视
b) 基于云提供近乎实时的检测，屏蔽新的或者紧急的威胁
c) 由机器学习、大数据分析和深入威胁抵抗研究提供的专用保护更新

3) 端点检测及相应

端点检测及相应功能提供几乎实时的高级攻击检测，安全分析专家可以有效地对警报进行优先级设置，了解安全漏洞的完整范围，并且提供相应的措施来进行补救。检测到威胁时 , 系统会在系统中创建警报 , 供分析人员调查。具有相同攻击技术或指向相同攻击者的警报将聚合到同一实体中，以这种方式聚合警报使分析员能够轻松地调查和响应威胁。

4) 自动检测及补救

Windows Defender ATP 服务在多台计算机上具有广泛的可见性。服务会每天产生大量的警报，对于典型的安全运营团队而言，生成的警报的数量是巨大的。为了应对

这一挑战，Windows Defender ATP 使用自动调查来显著减少需要单独调查的警报量。自动调查功能利用各种检查算法和分析（如行动手册）使用的流程来检查警报，并采取即时补救措施来解决违规行为。 这将显著减少警报音量，使安全操作专家能够专注于更复杂的威胁和其他高价值计划。

5) 安全状态

安全状态仪表板可以帮助用户更深入地了解组织的整体安全状况。 从该仪表板中，可以快速评估组织的安全状态，查看需要注意的计算机，以及为了进一步减少组织中的攻击面所需的操作的建议。Microsoft 安全分数磁贴反映了 Windows 和 Office 365 控件配置的所有安全控件的总和。同时该磁铁还可以保留一段时间内的安全分数，跟踪组织的安全状况。针对于当前的安全状态，Windows Defender ATP 会提供相应的热门建议，以帮助组织提高安全性。

6) 高级侦察

高级的搜索允许组织使用功能强大的搜索和查询工具搜寻的潜在威胁。用户还可以创建自定义检测规则，具体取决于 surface Microsoft Defender 安全中心中的警报的查询。

使用高级搜索，组织可以利用以下功能：

a) 使用功能强大的查询语言 intellisense：灵活性，用户需要转到下一级别的搜索查询。

b) 查询存储的遥测数据：遥测数据可以在表中访问，以便查询。例如，您可以查询流程创建、网络通信和许多其他事件类型。

c) 链接到门户：返回查询结果，例如计算机名称和文件名称是实际直接链接到门户，合并高级的搜索查询体验和现有的门户调查体验。

d) 查询示例 - 欢迎页提供相应实例，帮助用户熟悉表格和查询语言。

Windows Defender ATP 是 Microsoft 威胁保护解决方案的一部分，Windows Defender ATP 还可以结合 Office ATP 和 Azure ATP 实现端到端的安全防护，为组织提供强大的保护屏障。

2.3.4 Kill Chain 模型以及微软对抗 Kill Chain 攻击的 3 个 ATP

Kill Chain 是网络攻击结构化模型之一，黑客会利用各种手段渗透到组织内部，窃取组织内部信息，攻击组织的网络和系统。一般来说，Kill Chain 模型包含有侦查阶段、侵害机器、内部侦查和横向移动、域优势、数据整合和渗透 5 个阶段。[20]

20 "Kill Chain Approach". Chief of Naval Operations. April 23, 2013. Archived from the original on June 13, 2013.

7 个阶段的详细内容如下：

- 侦查阶段：在此阶段，攻击者通常会搜索可公开获取的资源，以找出尽可能多的有关其目标的信息。这将包括有关目标 IP 地址范围，业务运营和供应链，员工，主管和所使用技术的信息。此阶段的目标是开发足够的情报以增加成功攻击的机会。如果攻击者先前已经侵入您的环境，则他们可能还会引用先前入侵期间收集的情报。
- 侵害机器: 攻击者继续使用社交工程攻击来初步了解受害者的网络，因为这些攻击（尤其是针对性强且基于良好情报的攻击）具有极高的成功率。在此阶段，攻击者将向组织内经过精心选择的员工发送定向的网络钓鱼电子邮件。该电子邮件将包含恶意附件或将收件人定向到水坑攻击的链接。一旦用户执行附件或访问水坑，另一种称为后门的恶意工具将安装在受害者的计算机上，从而使攻击者可以远程控制计算机。

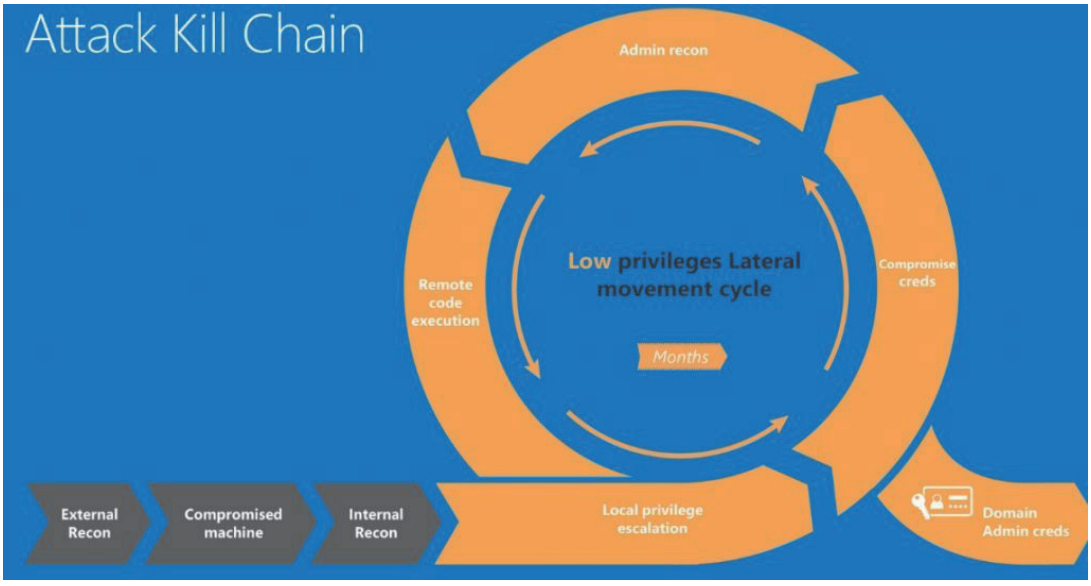


图 2.3.4 Kill Chain 模型攻击过程

- 内部侦查和横向移动：攻击者现在已在组织网络中立足，现在将开始收集以前无法从外部获得的信息，包括执行主机发现扫描，映射内部网络和系统以及尝试安装网络共享。攻击者还将开始使用免费提供的但非常有效的工具，例如 Mimikatz 和 WCE，以收集最初存储在最初受感染计算机上的凭据，并开始计划下一阶段的攻击。
- 域优势：在此阶段，攻击者将尝试将其访问级别提升到网络中更高的受信任状态。攻击者的最终目标是访组织的数据，并且域管理员的特权凭据为他们提供了多种访问有价值的数据的方式。一旦发生这种情况，攻击者将开始在整个网络中旋转，以寻找有价值的数据或安装勒索软件以用于将来的勒索企图或两者兼而有之。
- 数据整合和渗透：到这个阶段时，攻击者可以访问组织系统中的宝贵数据，因此，他或她必须对于数据进行整合，在不被检测到或阻止的情况下打包并将其发送到网

络之外。通常，这可以通过协议（例如 DNS，FTP 和 SFTP 或基于 Internet 的文件传输解决方案）对数据进行加密并将其传输到由攻击者控制的外部系统来实现。

Microsoft Secure and Productive Enterprise 提供了一整套的方案来破解 Kill Chain 模型，提供安全的办公环境，从而提高员工的生产力。下面的部分将会介绍一下 Office ATP、Windows Defender ATP 和 Azure ATP 是如何破解该模型从而保障企业安全的。

- Office ATP：该技术旨在破坏"初始危害"阶段，并提高成功使用网络钓鱼攻击的成本。大多数攻击者利用包含恶意附件或指向水坑站点的链接的网络钓鱼电子邮件。Office 365 中的高级威胁防护（ATP）提供针对电子邮件中已知和未知恶意软件和病毒的保护，针对恶意 URL 提供实时（单击时间）保护，以及增强的报告和跟踪功能。邮件和附件不仅会根据由 Microsoft 的 Intelligent Security Graph 提供的多个反恶意软件引擎和情报提供的签名进行扫描，而且还会被路由到特殊的引爆室，运行，并使用机器学习和高级分析技术对结果进行分析，以查找恶意行为的迹象检测并阻止威胁。
- Windows Defender ATP：该技术通过提高破坏和保留对用户 PC 的控制的难度，并保护在设备上存储和使用的帐户和凭据，从而破坏了受损的机器和横向移动阶段。如果攻击者仍设法通过某种其他机制（例如，通过个人电子邮件）将恶意软件传递给组织的一名员工，则 Windows 10 的安全功能可以对最初的感染进行防护，并且如果被感染，还可以防止进一步的横向移动。具体来说，Windows Defender 应用程序防护使用基于硬件的新虚拟化技术在 Edge 浏览器周围包裹保护性边界。即使恶意软件在浏览器中执行，它也无法访问底层操作系统，并且一旦关闭浏览器就可以从计算机中清除恶意软件。Windows Device Guard 提供了额外的保护层，以确保仅加载并运行受信任的程序以防止恶意程序的执行，并且 Windows Credential Guard 使用前面讨论的基于硬件的虚拟化技术，以防止设法获得最初立足点的攻击者从获取存储在端点上的其他凭证。最后，Windows Defender 高级威胁防护是公司安全团队的 DVR。它提供了对端点上发生的所有事件的近乎实时的记录，并使用内置签名，机器学习，通过引爆即服务进行的深入文件分析以及 Microsoft 智能安全图检测威胁的功能。它还使安全团队可以远程访问调查复杂攻击所需的重要法证数据。
- Azure ATP：该技术通过尽早检测横向运动攻击技术来中断横向运动阶段，从而实现快速响应。Azure 高级威胁防护 (ATP) 是一个基于云的安全解决方案，可利用本地 Active Directory 信号识别、检测并调查针对组织的高级威胁、身份盗用和恶意内部操作。Azure ATP 提供有关标识配置和建议的安全最佳实践的建议。通过安全报告和用户配置文件分析，Azure ATP 可以显着减少组织攻击面，使入侵用户凭据和推进攻击更加艰难。Azure ATP 的可视横向移动路径有助于快速准确地了解攻击者如何在组织内横向移动以入侵敏感帐户并协助提前预防这些风险。 Azure ATP 安全报

告有助于识别使用明文密码进行身份验证的用户和设备，并提供其他见解以改善组织安全状况和策略。

- Cloud App Security，Intune，Azure 信息保护和 Windows 10 信息保护

  Microsoft 安全企业套件提供了很多重要的功能来分类和保护数据并防止其丢失。Microsoft Cloud App Security 可以识别和控制未经认可的云应用程序的使用。这有助于组织通过基于云的应用程序防止数据丢失。Intune 和 Windows 10 信息保护可防止公司数据与个人数据混合或被未经批准的应用程序使用，无论是在 Windows 10 设备上还是在基于 iOS 或 Android 的移动设备上。最后，Azure 信息保护使组织及其员工能够使用数字版权管理技术对数据进行分类和保护。企业现在可以实施和实施需要知道的策略，从而在攻击者获得对其网络的访问权限时，显著减少可用的未加密数据量。

总而言之，针对于 Kill Chain 的攻击模型，微软提供了一整套的解决方案来保障企业的安全，从初始阶段通过 Office ATP 进行拦截，到通过 Windows Defender ATP 提高破坏和保留对用户 PC 的控制的难度，到通过 Azure ATP 及早检测横向渗透，微软提供的整个产业链可以大幅提高企业的网路安全、信息安全，提供高度安全的企业办公环境，提升员工工作效率。

Chapter 3
企业级安全边界搭建

在赛门铁克《互联网安全威胁报告》中，对全球威胁活动、网络犯罪趋势和攻击者动机进行了深入剖析，提出了自己的最新见解。其中，分析数据来自全球最大的民用威胁情报网络，即赛门铁克全球情报网络。该网络覆盖全球 1.23 亿个攻击传感器，日均拦截威胁数量达 1.42 亿个，有效跟踪全球 157 多个国家 / 地区的威胁活动。

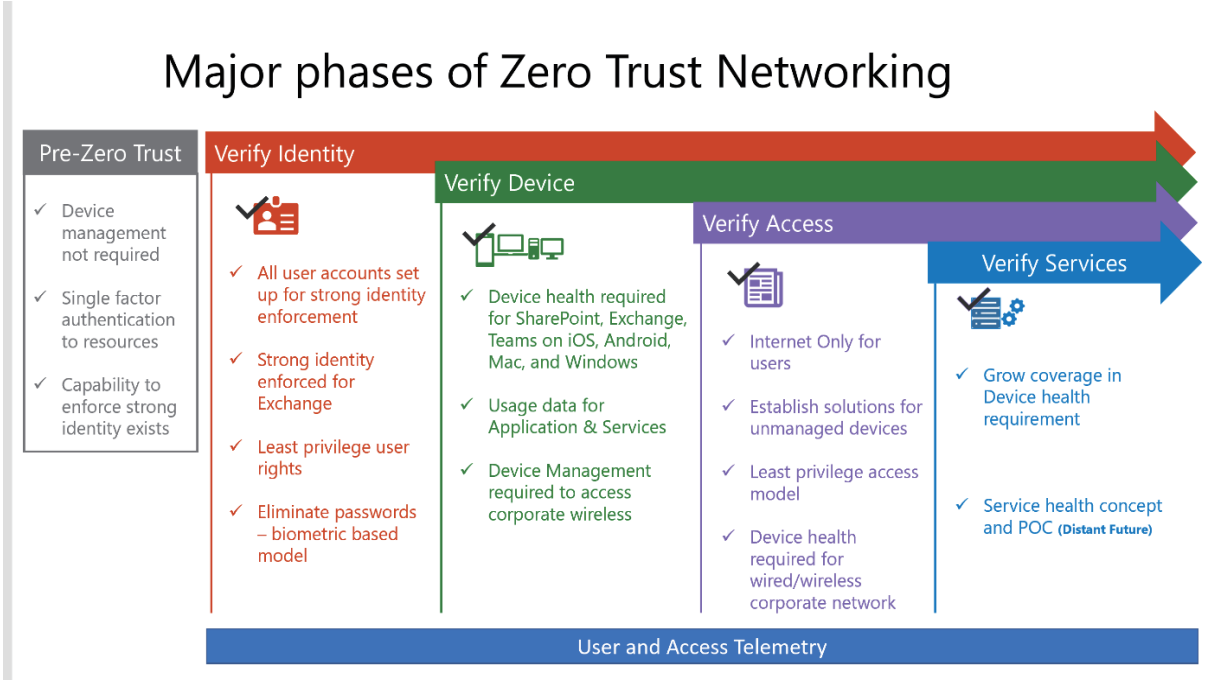
随着您公司组织当中的网络，应用程序以及云中的用户数量不断增加，给黑客攻击组织提供了更大的可攻击面，越来越多的用户，设备和应用程序服务器让系统的威胁持续增加。如何在越来越复杂网络环境当中，确保每个用户获得正确的访问权限，如何对企业中的设备和人员发挥控制作用同时减少整体的攻击面。如何在应用程序、服务器和数据库都互相通讯的情况下，了解潜在的安全漏洞？这些都是现代企业面临的巨大挑战。

3.1 Zero Trust 模型

面对这些挑战，一篇由 Forrest Group 发表在 NIST 上题为"制定一个框架来改善关键基

础设施网络安全"的文章开起了网络安全 Zero Trust 的时代。该模型遵循"永不信任，始终验证"的原则。虽然不是一个全新的理论，但大多数企业安全模型都倾向于采用验证，然后信任模型。这意味着，如果某人拥有正确的用户凭据，他们就可以使用他们请求的任何网站、应用程序或设备。这种模型在当今的商业环境中并不适用。因此，许多组织遭受了恶意软件和勒索软件攻击，以及影响品牌和最终效益的数据泄露。

新的业务计划和流程新增了遭受攻击的可能性，同时企业外围防御不再具有意义。应用程序、用户和设备正在向外扩展，这让曾经值得信赖的企业外围防御名存实亡。现在，需要在应用程序、数据、用户和设备所在的位置提供保护。



3.2 身份的定义及 RBAC

我们在互联网当中所有的操作都是基于我们的身份，就像现实生活中的身份一样，以医院为例，医生负责诊断治疗，护士负责实施护理，每个人根据自己的身份拥有不同的职责。互联网中的身份也是一样，每个人都基于他们的身份不同，在互联网组织当中行使他们不同的职责。

1996 年一篇发表在《computer》上的文章提到，美国国家标准学会对 28 个组织的最新研究和 Technology（NIST）证明 RBAC 解决了许多不同的问题 - 商业和政府部门的需求。

RBAC 的提出就是解决了互联网当中不同身份的人行使不同职责的问题。RBAC（Role-Based Access Control ）是基于角色的访问控制在 RBAC 中，权限与角色相关联，用户通过成为适当角色的成员而得到这些角色的权限。这就极大地简化了权限的管理。这样管理都是层级相互依赖的，权限赋予给角色，而把角色又赋予用户，这样的权限设计很清楚，管理起来很方便。

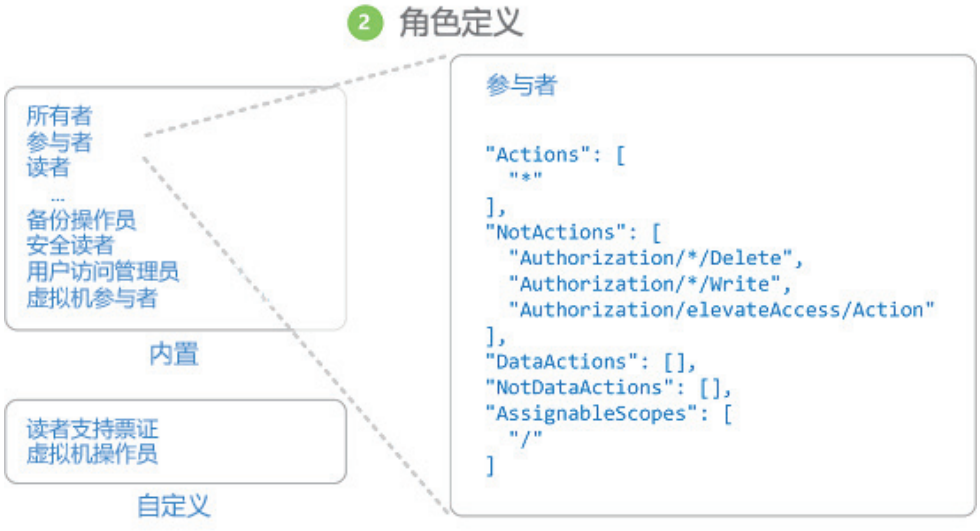
3.2.1 RBAC 的工作原理

使用 RBAC 控制资源访问权限的方式是创建角色分配。这是一个需要理解的重要概念 —它涉及到如何强制实施权限。角色分配包含三个要素：安全主体、角色定义和范围。

安全主体：是一个对象，表示请求访问的用户、组、服务主体或托管标识。

- 用户 - 在 Azure Active Directory 中具有配置文件的人员。 也可以将角色分配到其他租户中的用户。
- 组 - 在 Azure Active Directory 中创建的一组用户。 将某个角色分配到某个组时，该组中的所有用户都拥有该角色。
- 服务主体 - 应用程序或服务用来访问特定 Azure 资源的安全标识。 可将服务主体视为应用程序的用户标识（用户名和密码或证书）。
- 托管标识 - Azure Active Directory 中由 Azure 自动托管的标识。 在开发云应用程序时，通常使用托管标识来管理用于向 Azure 服务进行身份验证的凭据。

角色定义：是权限的集合。它有时简称为角色"。角色定义列出可以执行的操作，例如读取、写入和删除。 角色可以是高级别的（例如所有者），也可以是特定的（例如虚拟机读取者）。



Azure 包含多个可用的内置角色。 下面列出了四个基本的内置角色。前三个角色适用于所有资源类型。

- 所有者 - 拥有对所有资源的完全访问权限，包括将访问权限委派给其他用户的权限。
- 参与者 - 可以创建和管理所有类型的资源，但无法将访问权限授予其他用户。
- 读取者 - 可以查看现有的资源。
- 用户访问管理员 - 允许你管理用户对资源的访问。

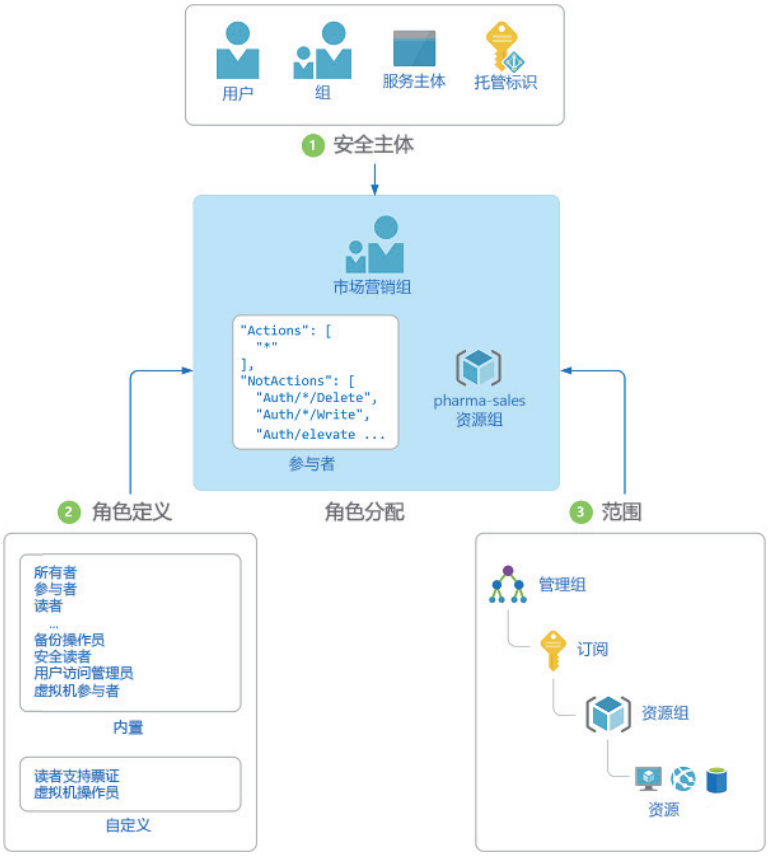
范围：是访问权限适用于的资源集。分配角色时，可以通过定义范围来进一步限制允许的操作。如果你想要将某人分配为网站参与者，但只针对一个资源组执行此分配，则使用范围就很有帮助。

范围采用父子关系结构，在父范围授予访问权限时，这些权限会继承到子范围。 例如：

- 如果将所有者角色分配给管理组范围的用户，则该用户可以在管理组中管理所有订阅中的一切内容。
- 如果在订阅范围向某个组分配了读取者角色，则该组的成员可以查看订阅中的每个资源组和资源。
- 如果在资源组范围向某个应用程序分配了参与者角色，则该应用程序可以管理该资源组中所有类型的资源，但不能管理订阅中的其他资源组资源。

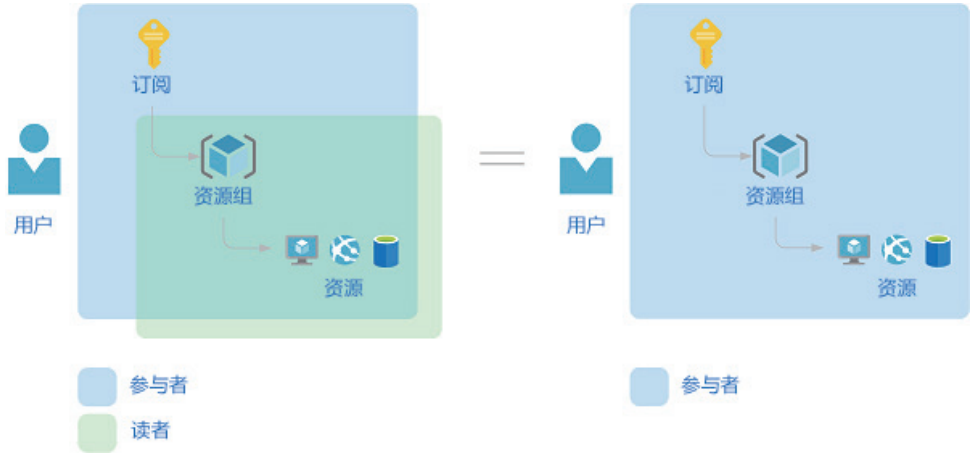
角色分配：是出于授予访问权限的目的，将角色定义附加到特定范围内的用户、组、服务主体或托管标识的过程。 通过创建角色分配来授予访问权限，通过删除角色分配来撤销访问权限。

下图显示了角色分配的示例。 在此示例中，为“营销”组分配了医药销售资源组的参与者角色。 这意味着，“营销”组中的用户可以在医药销售资源组中创建或管理任何 Azure 资源。 “营销”用户无权访问医药销售资源组外部的资源，除非他们属于另一个角色分配。



3.2.2 多角色分配

如果有多个重叠的角色分配，将会发生什么情况？ RBAC 是一个加法模型，因此，生效的权限是角色分配相加。请考虑以下示例，其中在订阅范围内向用户授予了"参与者"角色，并且授予了对资源组的"读者"角色。"参与者"权限与"读者"权限相加实际上是资源组的"参与者"角色。 因此，在这种情况下，"读者"角色分配没有任何影响。



进入在安全 & 合规中心中使用功能所需的权限可以查看所有安全和合规中心所需的权限。

3.3 基于 RBAC 的安全防护（涉及 EMS 中的 AIP，DLP，MCAS）

根据赛门铁克发布的《数据泄露剖析：数据泄露的原因及应对措施》报告，数据泄露的原因可以分为以下三种："粗心"的内部人员、目标性攻击和恶意的内部人员。Verizon 的报告显示，67% 的数据泄露事件都是由于部分"粗心"的内部人员出现"重大失误"而引发的，Ponemon Institute 对 43 家发生数据泄露事件的企业进行了调查，结果发现超过 88% 的企业数据泄露事件都是因为工作疏忽所引发的。

该报告还支出，由于员工无心导致的数据泄露主要有五个主要的原因分别是：

由于使用未受传输保护的服务器、台式机和笔记本电脑导致的信息泄露。

电子邮件、Web 邮件和可移动设备导致的信息泄露。

第三方业务合作伙伴和供应商传递信息导致的信息泄露。

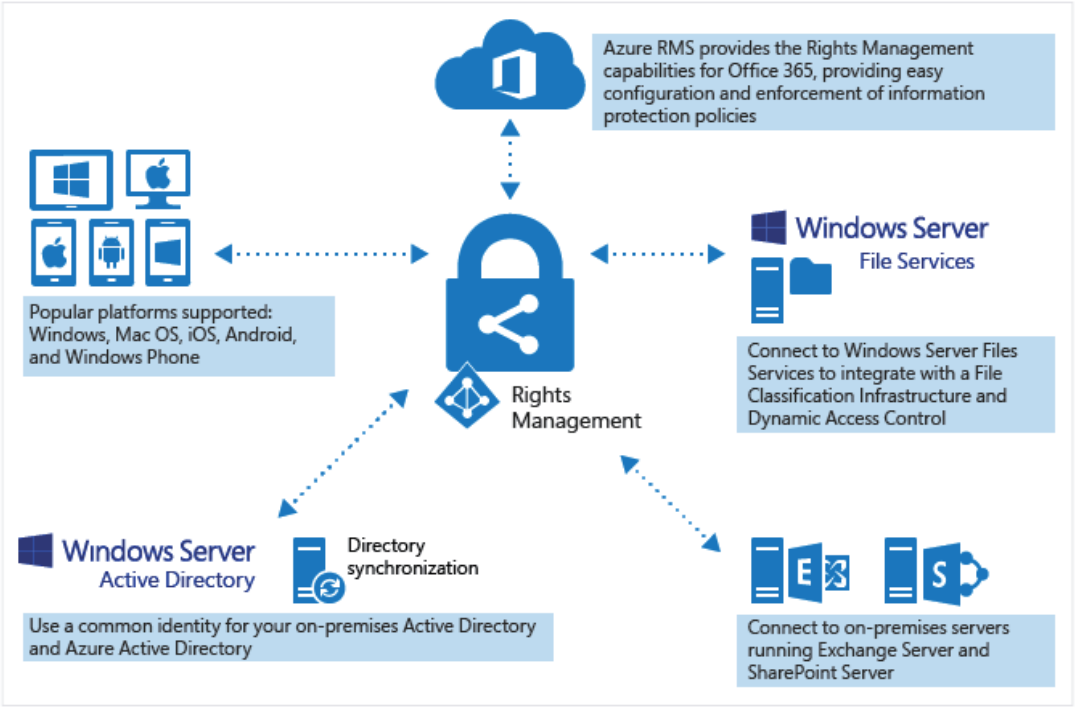
笔记本电脑丢失导致的信息泄露。

业务流程不当或者过时导致的信息泄露。

然而所有我们提到的信息泄露的情况都可以用通过采用我们的 Microsoft 上面的安全解决方案进行有效规避。其核心就是利用我们上文所提到的 RBAC 模型。基于 RBAC 的 AIP，DLP 和 MCAS 针对不同的对象和应用场景，提供了完整的解决方案。下面就对这三种解决方案进行逐一介绍。

3.3.1 Azure Information Protection

Azure Information Protection 简称 AIP 是 EMS 当中的于云的信息保护解决方案，有助于组织通过应用标签对其文档和电子邮件进行分类和有选择地保护。 标签可以由定义规则和条件的管理员自动应用、由用户手动应用或是二者组合应用（在这种情况下会向用户提供建议）。



AIP 的出现很好的解决了上面五个信息泄露场景当中，因为第三方业务合作伙伴和供应商传递信息导致的信息泄露、由于使用未受传输保护的服务器、台式机和笔记本电脑导致的信息泄露和由于业务流程不当或者过时导致的信息泄露。

在与合作伙伴或者供应商传递信息时，会因为信息没有加密传输，导致了第三方业务合作伙伴，有意或者无意的将公司的机密文件，向下泄露。Verizon 报告显示，业务合作伙伴泄露的数据量占数据泄露总量的 32%。

“粗心”内部人员在存储、发送或复制未加密的机密数据时，无意中违反了安全策略，引发了的数据泄露事件。很多企业在无感知的情况下，已经有 38% 的数据被转移到个人未受保护的设备当中，而其中 67% 的数据已经能被披露。

由于业务流程不当或者过时导致的信息泄露。当数据自动传输到未授权的个人用户或未受保护的系统上，而在这种情况下，数据可能很容易遭到黑客的攻击。

那么 AIP 是怎么保护文件即使被泄露也不会被打开，这就要提到 AIP 当中一项关键的技术 RMS（Azure Rights Management，RMS）。这项技术与 Microsoft 云服务和应用程序（例如 Office 365 和 Azure Active Directory）集成。此保护技术使用加密、标识和授权策略。与应用的标签类似，使用权限管理能够始终为文档和电子邮件提供保护，而不受其位置的影响 – 不管是在组织、网络、文件服务器和应用程序的内部还是外部。信息保护解决方案让你可以始终控制你的数据。

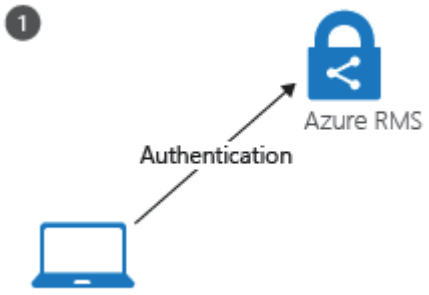
例如，可以配置报告文档或销售预测 Excel，以便仅允许组织内人员进行访问，并且可以控制是否可以编辑该文档、是否将其限制为只读，以及是否禁止打印它。 同样，你也可

以配置电子邮件，并禁止转发电子邮件或使用"全部答复"选项。此时第三方业务合作伙伴就算再想将这封电子邮件转给其他人，没有办法执行这样的操作，甚至这封邮件里的内容不能复制，窗口也不能投屏。而这份数据就算是到了你个人的电脑上，除你之外的其他人也无法打开这份电子邮件。

那 RMS 是如何保护我们的文件不被泄露的呢？接下来介绍 RMS 的技术原理。RMS 对文件加密和文件解密的流程如下所示。Azure RMS 工作原理包括三个部分：首次使用、内容保护、和内容使用三个阶段。

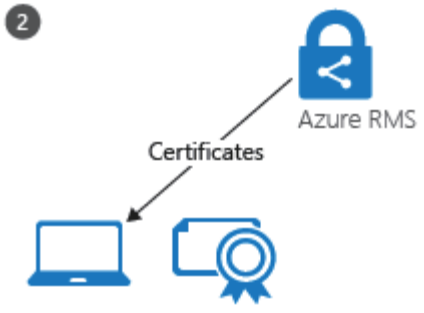
初始化用户环境：

在用户可以保护内容或使用 Windows 计算机上的受保护内容之前，必须在设备上准备用户环境。 这是一次性的过程，当用户尝试保护或使用受保护内容时会自动发生，无需用户干预：



步骤 1 验证过程：计算机上的 RMS 客户端首先连接到 Azure Rights Management 服务，并通过使用其 Azure Active Directory 帐户对用户进行身份验证。

将用户的帐户与 Azure Active Directory 联合时，会自动进行这种身份验证，并且不会提示用户输入凭据。



步骤 2 证书颁发过程：对用户进行身份验证后，连接将自动重定向到组织的 Azure 信息保护租户，该租户将颁发证书，让用户在 Azure Rights Management 服务上进行身份验证，以便使用受保护内容并脱机保护内容。

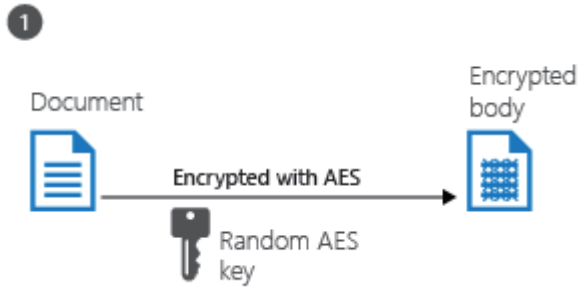
其中一个证书是通常缩写为 RAC 的权限帐户证书。 此证书对 Azure Active Directory 用

户进行身份验证，有效期为 31 天。 如果用户帐户仍然在 Azure Active Directory 中并且启用了该帐户，RMS 客户端将自动续订证书。 该证书不可由管理员进行配置。

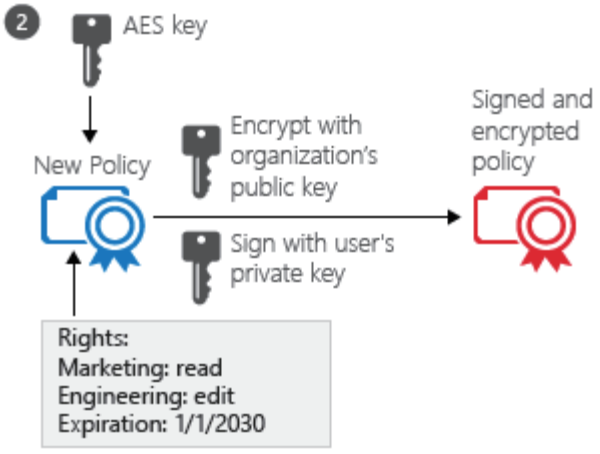
证书副本存储在 Azure 中，因此，如果用户转移到另一台设备，将使用相同的密钥创建证书。

内容保护：

当用户保护文档时，RMS 客户端将对未受保护的文档执行以下操作：



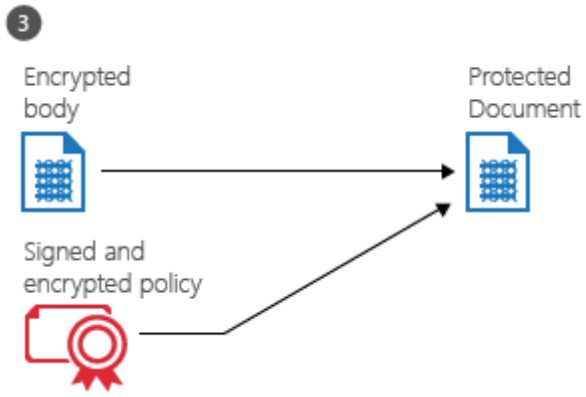
步骤 1 内容加密过程：RMS 客户端创建一个随机密钥 （内容密钥），并结合使用此密钥与 AES 对称加密算法来加密该文档。



步骤 2 密钥加密过程：RMS 客户端随后会为文档创建一个包含策略的证书，策略包括用户或组的使用权和其他限制，例如过期日期。 这些设置可在管理员之前配置的模板中进行定义，或在内容受保护时进行指定（有时称为“临时策略”）。

用于标识所选用户和组的主要 Azure AD 属性是 Azure AD proxyAddresses 属性，该属性用于存储用户或组的所有电子邮件地址。 但是，如果用户账户的 AD ProxyAddresses 属性中没有任何值，则改用用户的 UserPrincipalName 值。

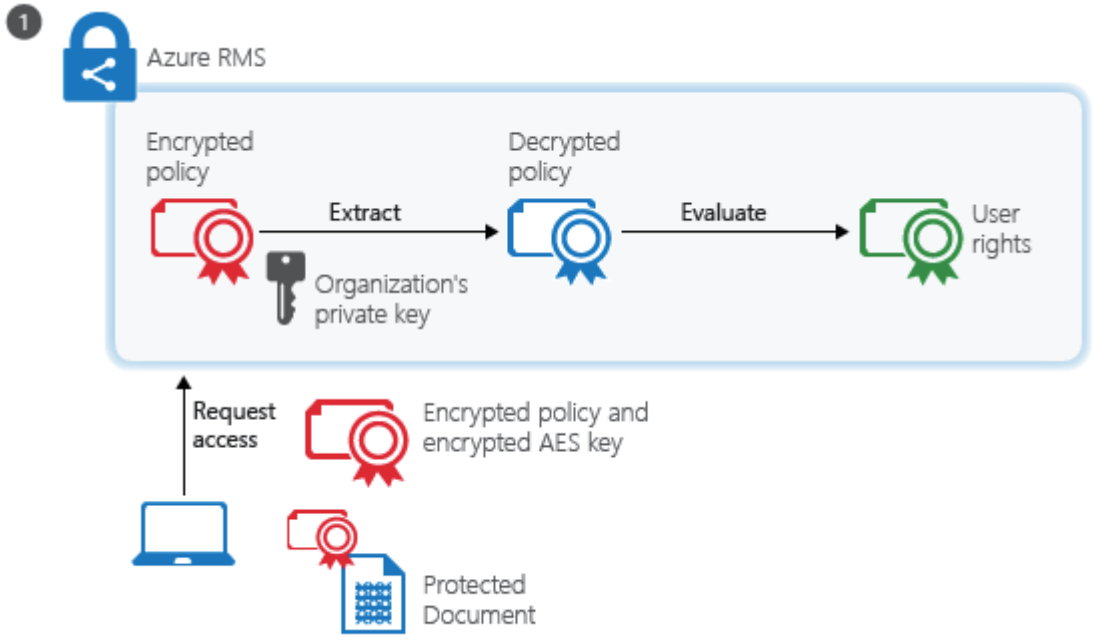
然后，RMS 客户端使用初始化用户环境时获取的组织密钥，并使用此密钥来加密策略和对称内容密钥。 RMS 客户端还使用初始化用户环境时获得的用户证书对策略进行签名。



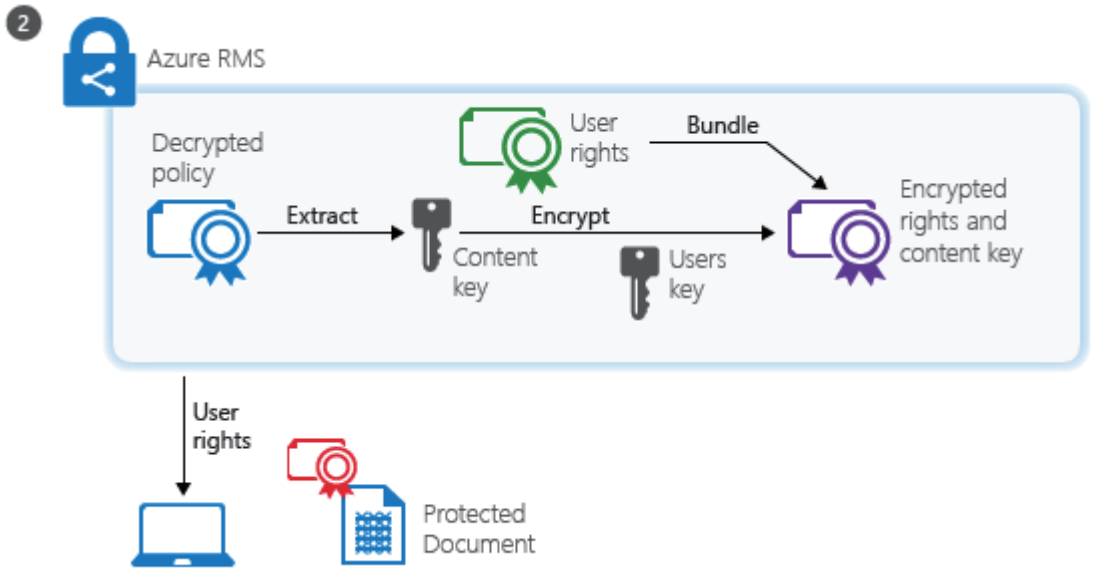
步骤 3 验证过程：最后，RMS 客户端将该策略嵌入到一个文件中，该文件包含以前已加密的文档的正文，并与该文档共同构成了受保护文档。

可将此文档存储在任意位置，或者使用任何方法将其共享，加密的文档始终附带该策略。内容使用：

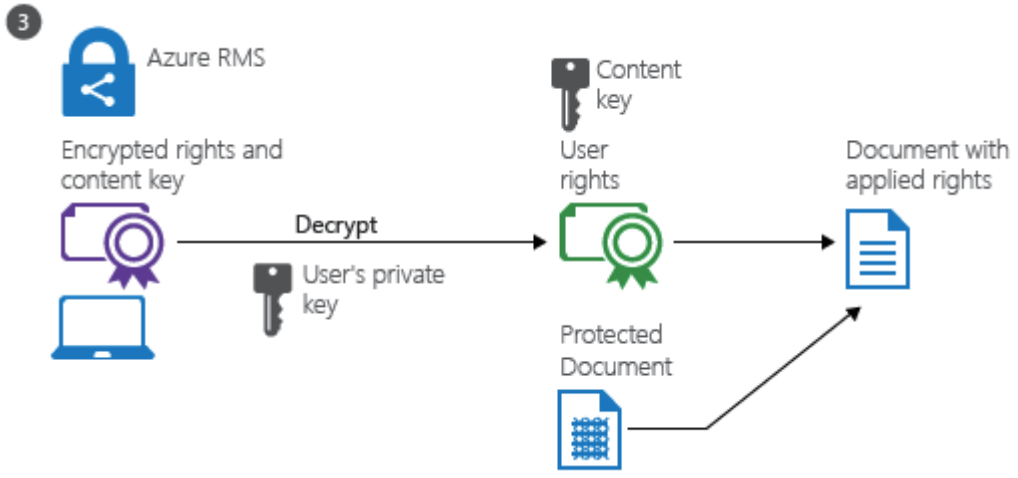
当用户想要使用受保护的文档时，将通过请求对 Azure Rights Management 服务的访问来启动 RMS 客户端：



步骤 1 获取用户权限过程：经过身份验证的用户将文档策略和用户的证书发送到 Azure Rights Management 服务。服务解密并评估该策略，并生成用户对该文档拥有的权限列表（如果有）。 若要标识用户，可将 Azure AD ProxyAddresses 属性用于用户的账户和该用户所属的组。 出于性能原因，会缓存组成员身份。 如果用户账户的 Azure AD ProxyAddresses 属性中没有任何值，则改用 Azure AD UserPrincipalName 中的值。



步骤 2 密钥加密传输过程：然后，服务将从已解密的策略中提取 AES 内容密钥。 然后，使用通过请求获取的用户公共 RSA 密钥来加密此密钥。



重新加密的内容密钥将连同用户权限列表一起嵌入到加密的使用许可证中，随后使用许可证将返回到 RMS 客户端。

步骤 3 验证过程：最后，RMS 客户端将采用加密的使用许可证，并使用其自身的用户私钥来解密该许可证。 这样，RMS 客户端便可以根据需要解密文档的正文，并在屏幕上呈现其内容。客户端还将解密权限列表，并将其传递到应用程序，应用程序将在应用程序的用户界面中强制实施这些权限。

3.3.2 Data Loss Prevention

赛门铁克在报告当中提到的物种泄露方式当中最常见的电子邮件、Web 邮件和可移动设

备导致的信息泄露。赛门铁克对潜在用户展开的多项风险评估结果显示，平均每 400 封电子邮件中就约有 1 封电子邮件会包含未加密机密数据。这些数据就成为黑客攻击的目标。但是因为我们很难预测那封邮件会因为我们的误发送导致泄露，我们就不可能为我们的每封邮件加密，如果我们对封邮件都采取加密的手段会导致很多日常的邮件转发协同工作没办法进行。

DLP 正是为了应对这种情况而生的解决方案，DLP 可以帮助企业守住数据流出每一个出口，在 Exchange、Teams、SharePoint、OneDrive 当中保护数据的安全。

DLP 保护数据的原理是，使用深入内容分析（而不仅仅是简单的文本扫描）来检测敏感信息。这种深入内容分析使用关键字匹配、字典匹配、正则表达式评估、内部函数以及其他方法来检测匹配 DLP 策略的内容。您的数据中可能只有小部分数据被视为敏感数据。DLP 策略可以只识别、监视和自动保护那些敏感数据，而不会妨碍或影响处理您的内容的其余部分的人员。

具体来说 DLP 的策略包含以下内容：

- 在何处保护内容：Exchange Online、SharePoint Online 和 OneDrive for Business 网站等位置，还包括 Microsoft Teams 聊天和频道消息。
- 何时以及如何通过强制执行由以下部分组成的规则来保护此内容：
    - 在强制执行规则之前内容必须满足的条件。例如，可将规则配置为只查找包含与组织外部人员共享的社会保险号的内容。
    - 找到满足条件的内容时你希望规则自动执行的操作。例如，可将规则配置为阻止访问文档，以及向用户和合规部主管发送电子邮件通知。

可使用规则来满足特定保护要求，然后使用 DLP 策略将常见保护要求组合在一起，例如符合特定规则所需的所有规则。

位置：

无论信息位于 Exchange Online、SharePoint Online、OneDrive for Business 还是 Microsoft Teams 中，DLP 策略均可查找和保护 Office 365 中的敏感信息。 你可以选择保护 Exchange 电子邮件、Microsoft Teams 聊天和频道消息以及所有 SharePoint 或 OneDrive 库中的内容，或为策略选择特定位置。

如果你选择包含或排除特定的 SharePoint 网站或 OneDrive 帐户，则 DLP 策略可包含不超过 100 个此类包含和排除项。 尽管存在此限制，你可应用组织范围策略或位置整体策略来超出此限制。

规则：

规则用于对组织的内容强制执行业务要求。 策略包含一条或多条规则，每条规则由多个条件和操作组成。 对于每条规则，只要满足了条件，就会自动执行操作。 规则按顺序执行，

从每个策略中优先级最高的规则开始。

规则还提供一些选项，用于通知用户（使用策略提示和电子邮件通知）和管理员（使用电子邮件事件报告）内容与规则相匹配。

规则包括了条件，就是触发执行的 trigger，敏感信息的类型以及操作。

处理规则的优先级：

在策略中创建规则时，每条规则都按创建顺序分配了优先级—这意味着，首先创建的规则具有第一优先级，创建的第二条规则具有第二优先级，以此类推。

对照规则评估内容时，按优先级顺序处理规则。 如果内容符合多个规则，按优先级顺序处理规则，并强制实施最严格的操作。例如，如果内容符合以下所有规则，将实施规则 3，因为它具有最高优先级且最严格。

当我们创建了规则之后可能会遇到两类问题，一是因为规则太松导致的很多非敏感信息的内容与规则匹配，进而产生的误报；二是因为规则太严导致的，敏感信息泄露。

DLP 当中设置了提高匹配准确的规则，包括实例计数还有匹配准确度。

实例计数：

实例计数是指若要使内容与规则匹配，某类敏感信息必须出现的次数。 例如，如果将美国或英国护照号码标识为 1 到 9，则内容将与如下所示的规则匹配。

请注意，实例计数仅包括敏感信息类型和关键字的唯一匹配项。 例如，如果一个电子邮件中相同的信用卡号码出现了 10 次，则这 10 次计为信用卡号码的单个实例。

若要使用实例计数来调整规则，则指南非常简单：

- 若要使规则更易匹配，减少“最小”计数和 / 或增加“最大”计数。 也可以通过删除数值，将“最大”设置为“任意”。
- 若要使规则更难匹配，增加“最小”计数。

匹配准确度：

如上文所述，使用不同类型的证据组合定义并检测敏感信息类型。 敏感信息类型通常由多个此类组合（称为模式）定义。 需要越少证据的模式匹配准确度（即置信水平）越低，而需要越多证据的模式匹配准确度（即置信水平）更高。 若要了解每种敏感信息类型使用的实际模式和置信水平，请参阅使用敏感信息类型查找什么。

例如，名为“信用卡号”的敏感信息类型由两种模式定义：

- 置信度为 65% 的模式需要：
    - 信用卡号格式的数字。
    - 传递校验和的数字。
- 置信度为 85% 的模式需要：
    - 信用卡号格式的数字。

- 传递校验和的数字。
- 格式正确的关键字或到期日期。

可在规则中使用这些置信水平（或匹配准确度）。 在匹配准确度较低的规则中通常使用较为宽松的操作，如发送用户通知。 在匹配准确度较高的规则中使用更严格的操作，如限制访问内容且不允许用户替代。

3.3.3 Microsoft Cloud App Security

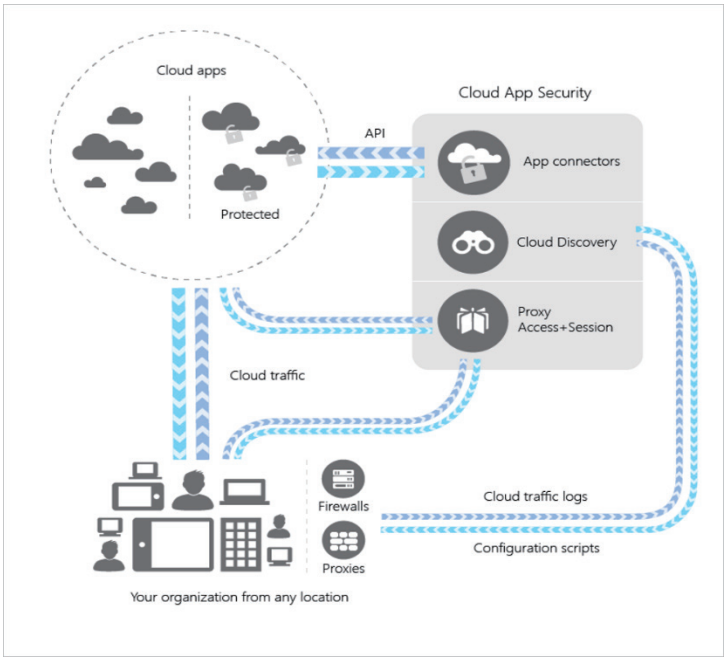
在腾讯安全与互联网安全新媒体 FreeBuf 联合出品《2019 年上半年云安全趋势报告》当中指出在对 2019 年上半年的漏洞检测脚本中，平均每月检测漏洞 & 安全基线数量 14.8 万个，以漏洞对服务器哪部分影响进行分类，其中安全基线占比 59%，系统组件漏洞占比 22%，Web 应用漏洞占比 19%。这些 Web 应用非常容易造成个人账户信息的泄露，而黑客则可以利用这些数据对企业信息进行盗窃。

因此，仅仅在事后了解云环境中发生的情况往往是不够的。你希望在员工有意或无意中将数据和组织置于风险中之前，就能够及时阻止安全漏洞和泄密。让组织中的用户能够充分利用云应用中提供的服务和工具，并让他们自己的设备运行起来也非常重要。同时，需要工具来实时帮助保护组织免受数据泄漏、数据窃取的侵害。Microsoft Cloud App Security 与 Azure Active Directory 一起提供这些功能，结合条件访问应用控制带来全面综合的一站式体验。

在 OALib 的论文"使用消毒技术的反向代理框架用于数据库中的入侵预防"，也提到了在代理服务器上，数据清理使用清理应用程序触发算法。在这个框架包括检测和消毒被污染的信息被发送到数据库，用于预防现在流行的注入式 SQL 攻击。

MCAS 是支持各种部署模式的云访问安全代理，包括日志集合、API 连接器和反向代理。它提供了丰富的显示效果、数据旅程控制和成熟分析服务，用于跨所有 Microsoft 和第三方云服务发现和防范网络威胁。MCAS 与领先的 Microsoft 解决方案本机集成，并在设计时考虑到安全专家。 它提供了简单的部署、集中管理和创新的自动化功能。

- 发现和控制影子 IT 的使用：标识组织使用的云应用、IaaS 和 PaaS 服务。调查使用模式，并针对超过 80 种风险评估超过 16，000 个 SaaS 应用的风险级别和业务就绪情况。开始管理它们，以确保安全性和合规性。
- 保护云中任意位置处的敏感信息：了解、分类和保护静态公开的敏感信息。利用现成策略和自动化流程来跨所有云应用实时应用控制。
- 防范网络威胁和异常：跨云应用检测异常行为，以发现勒索软件、已遭入侵的用户或未授权应用，分析高风险用法，并自动修正，以限制组织所面临的风险。



评估云应用的合规性：评估云应用是否符合相关合规性要求，包括法规合规性要求和行业标准。 防止数据泄露给不合规的应用，并限制对受管制数据的访问。

MCAS 的工作原理是：条件访问应用控制使用反向代理体系结构，并与 Azure AD 条件访问唯一集成。Azure AD 条件访问允许根据特定条件对组织的应用强制执行访问控制。 这些条件定义了应用条件访问策略的人员（用户或用户组）、对象（哪个云应用程序）和位置（哪个位置和网络）。确定条件后，可以将用户路由到 Microsoft Cloud App Security，你可以在其中通过应用访问和会话控制使用条件访问应用控制来保护数据。

借助条件访问应用控制，可根据访问和会话策略实时监视并控制用户应用访问和会话。在 Cloud App Security 门户中使用访问和会话策略，以进一步优化筛选器并设置要对用户执行的操作。使用访问和会话策略，可以：

- 阻止数据渗透：你可以阻止在上下载、剪切、复制和打印敏感文档，例如非托管设备。
- 下载时保护：你可以要求文档通过 Azure 信息保护进行标记和保护，而不是阻止对敏感文档的下载。 此操作可确保文档受到保护，并且在可能存在风险的会话中限制用户访问。
- 阻止上传未标记的文件：在上载、分发和使用敏感文件之前，请务必确保文件具有正确的标签和保护。 可以确保在用户对内容进行分类之前，阻止上载包含敏感内容的未标记文件。
- 监视用户会话的符合性：有风险的用户在登录应用时会受到监视，并且在会话内记录其操作。 你可调查和分析用户行为，了解将来应用会话策略的位置和条件。
- 阻止访问：你可以根据多个风险因素，以粒度方式阻止特定应用和用户的访问。例如，

如果使用客户端证书作为设备管理形式，则可以阻止它们。

- 阻止自定义活动：某些应用程序具有可携带风险的独特方案，例如，在 Microsoft 团队或时差等应用程序中发送包含敏感内容的消息。 在这种情况下，你可以对敏感内容的消息进行扫描，并实时将其阻止。

会话控制的工作原理是：使用条件访问应用控制创建会话策略使你能够控制用户会话，方法是通过反向代理重定向用户，而不是直接重定向到应用。 然后用户请求和响应将通过 Cloud App Security 而不是直接发送到应用。

如果会话受代理保护，则所有相关的 Url 和 cookie 都将替换 Cloud App Security。例如，如果应用返回的页面包含一个链接，该链接的域以 myapp.com 结尾，则链接会被替换为以类似于 myapp.com.cas.ms 结尾的域。

此方法不要求在设备上安装任何内容，使其在监视或控制来自非管理的设备或合作伙伴用户的会话时非常理想。

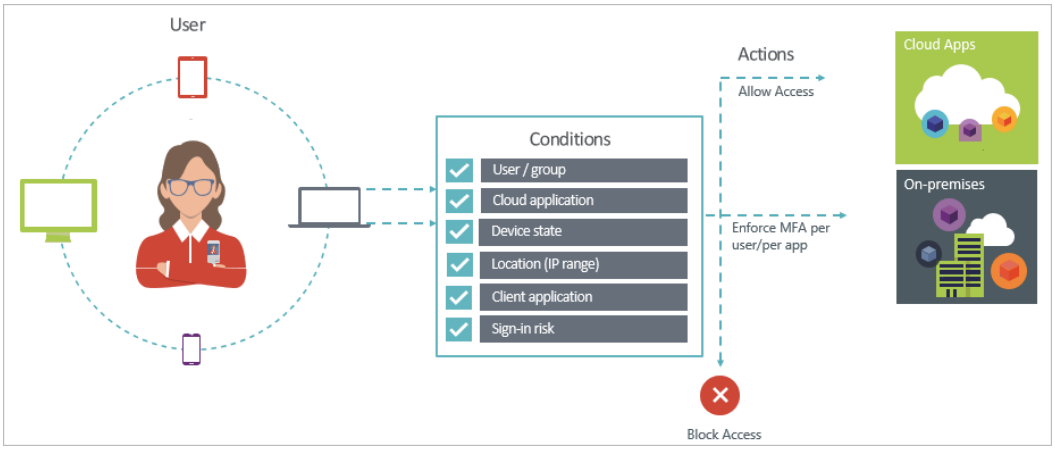
受管理设备标识

通过条件访问应用控制，可以创建考虑是否管理设备的策略。 要识别设备是否为受管理设备，该功能使用：

- 兼容设备
- 已加入域的设备
- 客户端证书部署

3.4 基于 Zero Trust 模型的安全防护（AAD P1 中的 conditional access）

赛门铁克报告当中最后一个导致数据泄露的原因。笔记本电脑丢失导致的信息泄露。根据 Ponemon Institute 研究报告显示，丢失的笔记本电脑是导致数据泄露最主要的原因，占接受调查的企业的 35%。但是就算是在电脑丢失且电脑没有设置密码的情况下，也可以使用 Azure Active Directory (Azure AD) 条件访问起到对关键数据保护的作用，而不用担心公司机密泄露。基于 Azure AD 条件的访问在完成第一因素身份验证后将强制执行条件访问策略。条件访问是 Azure Active Directory 的一项功能。 使用条件访问，可以实现基于条件访问云应用的自动访问控制决策。



那么什么是 Azure AD 什么又是基于条件的访问，什么又是 Azure AD 基于条件的访问呢？

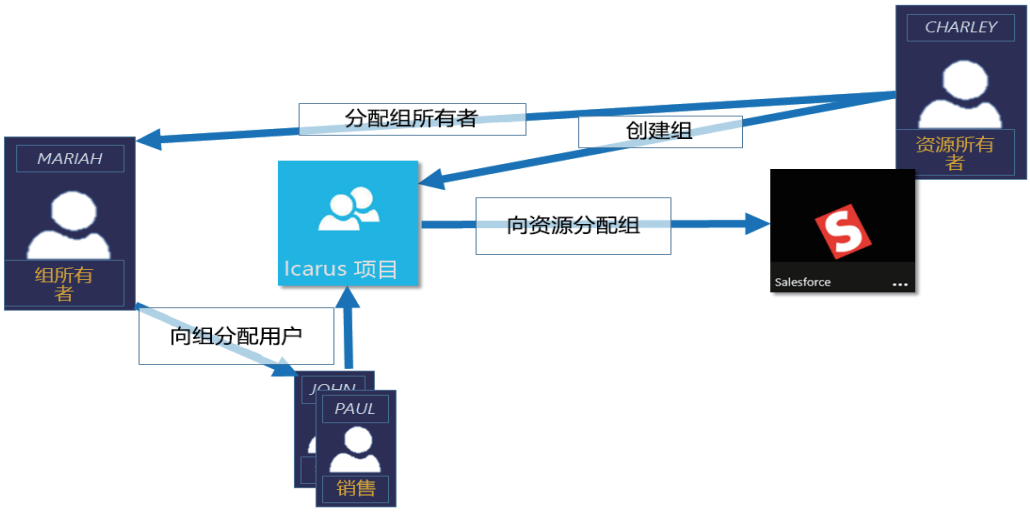
3.4.1 Azure Active Directory

Azure AD 是 Microsoft 推出的基于云的标识和访问管理服务，可帮助员工登录及访问以下位置的资源：

- 外部资源，例如 Microsoft Office 365、Azure 门户以及成千上万的其他 SaaS 应用程序。
- 内部资源，例如公司网络和 Intranet 上的应用，以及由自己的组织开发的任何云应用。
- 使用 Azure Active Directory 组管理应用和资源访问

Azure Active Directory (Azure AD) 可以帮助你使用组织的组来管理基于云的应用、本地应用和资源。 资源可以是目录中的资源（例如用于通过目录中的角色管理对象的权限）、目录外部的资源（例如软件即服务 (SaaS) 应用、Azure 服务和 SharePoint 站点）和本地资源。Azure AD 中的访问管理的工作原理：

Azure AD 通过向单个用户或整个 Azure AD 组提供访问权限，帮助你授予组织资源的访问权限。 资源所有者（或 Azure AD 目录所有者）可以使用组将一组访问权限分配给组的所有成员，而无需逐个地提供权限。资源或目录所有者还可将成员列表的管理权限授予其他某人（例如部门经理或支持管理员），让此人根据需要添加和删除成员。



分配访问权限的方式：

- 直接分配。 资源所有者直接将用户分配到资源。
- 组分配。资源所有者将 Azure AD 组分配到资源，这会自动向所有组成员授予对该资源的访问权限。 组成员身份由组所有者和资源所有者管理，允许任一所有者在该组中添加或删除成员。
- 基于规则的分配。资源所有者创建一个组，并使用一条规则来定义要将哪些用户分配到特定的资源。 该规则基于分配给单个用户的属性。资源所有者管理该规则，确定需要提供哪些属性和值才能访问该资源。
- External authority assignment（外部机构分配）。访问来自外部源，例如本地目录或 SaaS 应用。在这种情况下，资源所有者将分配一个组以提供资源访问权限，外部源将管理组成员。

3.4.2 条件访问

新式安全外围网络现已超出组织网络的范围，其中涵盖了用户和设备标识。 在做出访问控制决策过程中，组织可以利用这些标识信号。

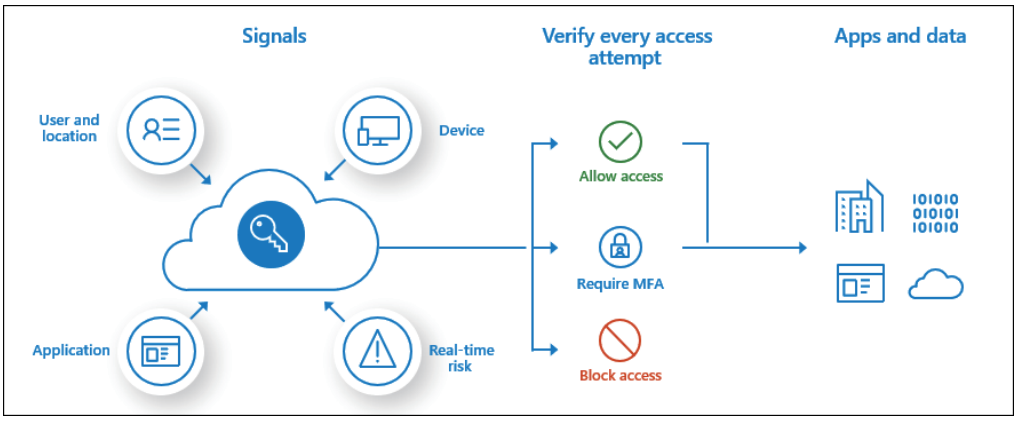
Azure Active Directory 使用条件访问作为一种工具来统合信号、做出决策，以及实施组织策略。条件访问是新的标识驱动控制平面的核心。

最简单地讲，条件访问策略是一些 if-then 语句：如果用户想要访问某个资源，则必须完成某个操作。示例：薪资管理人员想要访问薪资应用程序，而需要执行多重身份验证才能访问。

管理员面临着两个主要目标：

- 使用户能够随时随地保持高效的工作

- 保护组织的资产



使用条件访问策略，可以在必要时应用适当的访问控制来确保组织的安全，并在不必要应用这些控制时，避免为用户造成阻碍。

常见信号：

在做出策略方面的决策时，条件访问可以考虑的常见信号包括：

- 用户或组成员身份
  - 策略可以针对特定的用户和组，并为管理员提供精细的访问控制。
- IP 定位信息
  - 组织可以创建在做出策略决策时使用的受信任 IP 地址范围。
  - 管理员可以指定要阻止或允许的整个流量来源国家 / 地区的 IP 范围。
- 设备
  - 实施条件访问策略时，用户可以使用的装有特定平台或标有特定状态的设备。
- 应用程序
  - 尝试访问特定应用程序的用户可以触发不同的条件访问策略。
- 实时风险和计算风险检测
  - 将信号与 Azure AD 标识保护相集成可让条件访问策略识别有风险的登录行为。然后，策略可以强制用户执行密码更改或多重身份验证，以降低其风险级别，或者在管理员采取手动措施之前阻止其访问。
- Microsoft Cloud App Security (MCAS)
  - 实时监视和控制用户应用程序的访问和会话，提高云环境中执行的访问和活动的透明度与控制度。

常见决策：

- 阻止访问
  - 最严格的决策

- 授予访问权限
    - 最不严格的决策仍可要求以下一个或多个选项：
        - 需要多重身份验证
        - 要求将设备标记为合规
        - 要求使用加入混合 Azure AD 的设备
        - 需要批准的客户端应用
        - 需要应用保护策略（预览版）

3.4.3 Azure Active Directory 中的条件访问

Microsoft 付费云服务（如 Office 365、企业移动性 + 安全性、Dynamics 365 及其他类似产品）需要许可证。这些许可证将分配给需要访问这些服务的每个用户。若要管理许可证，管理员可以使用某种管理门户（Office 或 Azure）和 PowerShell cmdlet。Azure Active Directory (Azure AD) 是支持所有 Microsoft 云服务的标识管理的底层基础结构。Azure AD 存储有关用户许可证分配状态的信息。

到目前为止，只能在单个用户级别分配许可证，因此，大规模管理可能会变得困难。例如，若要根据组织变化（例如用户加入或离开组织或部门）添加或删除用户许可证，管理员通常必须编写一个复杂的 PowerShell 脚本。此脚本对云服务进行单独的调用。

为了解决这些难题，Azure AD 现在提供基于组的许可功能。可将一个或多个产品许可证分配给某个组。 Azure AD 确保将许可证分配给该组的所有成员。将向加入该组的任何新成员分配适当的许可证。 在这些成员离开组时，将删除相应的许可证。使用此许可管理功能后，将不再需要通过 PowerShell 自动执行许可证管理以反映每个用户的组织和部门结构变化。

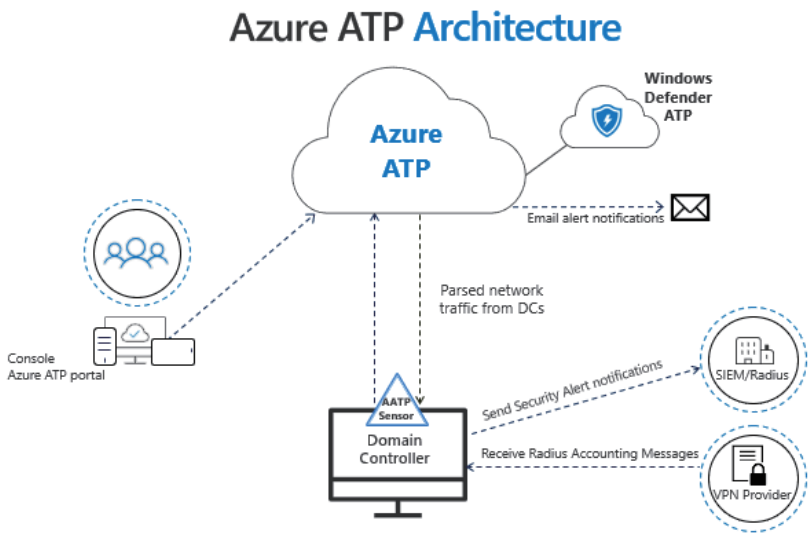
1.5 身份信用体系建立（Azure Advanced Threaten Protection）

CLOUDMARK 的一份报告中显示平均一次一次鱼叉式网络钓鱼攻击所造成的平均损失是 160 万美元。Fireeye 的一项调查报告指出，从渗透到发现的中间间隔时间长达 99 天。在组织当中的关键人账号密码被泄露之后有很长的时间可以用来发现这个威胁，并进行相应的措施阻止数据泄露的事情发生，而在这个虽然已经泄露，但并没有直接对企业造成伤害的过程中，是否有一些手段可以来帮助企业去发现这样的在目前低影响，但今后会造成重大影响的威胁呢?

Azure ATP 正是这样的一款解决方案，他可以帮助企业监控企业当中用户的异常行为，并采取相应的措施。帮助企业减少网络数据窃取带来的伤害。Azure 高级威胁防护 (ATP) 是一个基于云的安全解决方案，可利用本地 Active Directory 信号识别、检测并调查针对组织

的高级威胁、身份盗用和恶意内部操作。 Azure ATP 可以使 SecOp 分析员和安全专业人员能够在混合环境中检测高级攻击，以便：

- 使用基于学习的分析监视用户、实体行为和活动
- 保护存储在 Active Directory 中的用户标识和凭据
- 识别并调查整个杀伤链中的可疑用户活动和高级攻击
- 提供关于简单时间线的明确事件信息，以进行快速会审

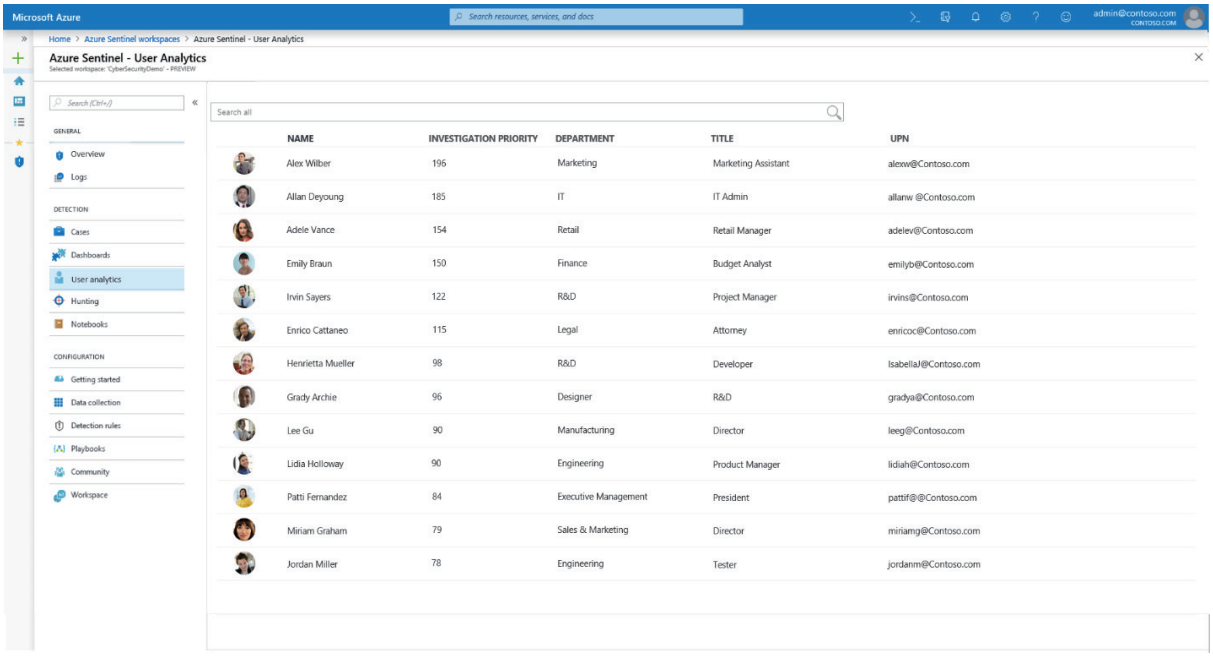


Azure ATP 通过直接从域控制器捕获和分析网络流量及利用 Windows 事件来监控域控制器，然后分析数据是否受到攻击和威胁。 Azure ATP 利用分析、确定性检测、机器学习和行为算法，可了解你的网络，启用异常检测，并在出现可疑活动时发出警告。

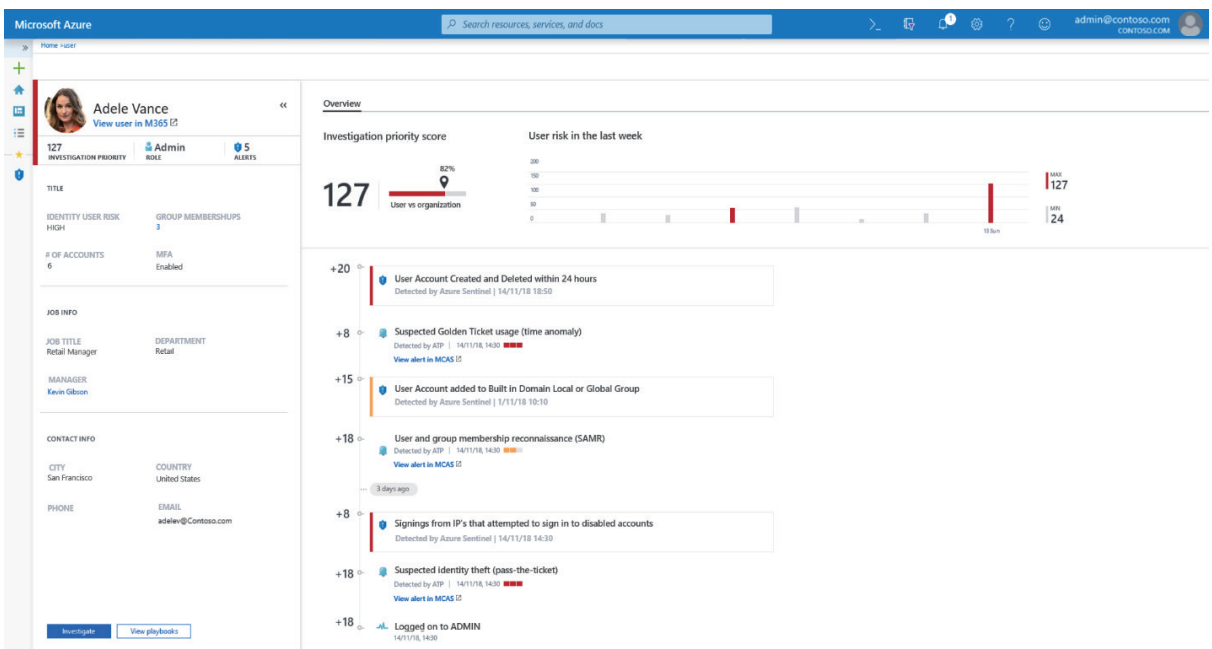
Azure ATP 包括以下组成部分：

- Azure ATP 门户，借助 Azure ATP 门户，可创建 Azure ATP 实例，显示从 Azure ATP 传感器接收的数据，还可监视、管理和调查网络环境中的威胁。
- Azure ATP 传感器，直接在域控制器上安装 Azure ATP 传感器。 传感器直接监控域控制器流量，无需专用服务器或端口镜像配置。
- Azure ATP 云服务，Azure ATP 云服务在 Azure 基础结构上运行，目前在美国、欧洲和亚洲进行部署。 Azure ATP 云服务已连接到 Microsoft 的 Intelligent Security Graph。

基于 Azure ATP 整套对于 Azure AD 用户的监控功能下，Azure Sentinel 构建了一套用户分析的信用体系，在 Sentinel 中只要接入了 Azure ATP 的信息，就可以自动根据用户过往发生的行为，对其进行打分，如果您发现了特定用户的分析出现了异常的波动，平台就会提高对于这个用户的"需要调查的优先级"的分数，帮助企业的安全团队及时发现可能泄露的账号。



当你点开某个需要调查的用户，您就可以依据时间线，看到他一系列的异常行为的情况，您就可以根据对应的猜测的逻辑进行判断，之后依靠 Sentinel 中的其他功能（在第四章中会做具体介绍），如 Hunting 或者调查，更全面的了解整个事件的起因和影响面。



Chapter 4

基于安全框架的安全事件的控件及响应

4.1 SIEM+SOAR 市场分析

在过去的 2017 年里，市场上对 SIEM 技术的需求一直强劲。SIEM 市场从 2016 年的 19.99 亿美元增长到 2017 年的 21.80 亿美元（参见"市场份额分析：全球安全软件，2017 年"）[21]。其中威胁管理是主要驱动因素，常规监视和合规性仍然是次要因素。在北美，即使有些组织在安全上资源十分有限，但他们仍然对 SIEM 平台进行了部署，因为它们需要改进监控的方式和方位，以及进行违规检测，这些通常是只有大型客户或业务合作伙伴才能坚持运行的。另外，合规报告也继续作为客户所需的必备要素之一，但大多数买家将其视为一个 SIEM 系统的必备项。

近些年来， 受威胁管理和合规性要求共同推动，欧洲和亚太地区对 SIEM 技术的需求保持稳定增长。其中，市场上对 SIEM 又有了新的要求，即在采集特性信息的过程中，可以通过访问控制和数据屏蔽来满足在隐私相关的合规性要求。此外，亚太区域和拉丁美洲这两处较不成熟市场的增长率远高于较成熟的北美和欧洲市场的增长率。

根据最新的 Gartner 象限 2018 年的情况可以看到，其越发重视 SIEM 平台在威胁管理里的能力，另外对于 SIEM 前景的期望，Gartner 象限尤其重视 SIEM 中的以下两个维度：在高级安全分析领域特别重视对用户的行为分析，也就是 UEBA（User and Entity Behavior Analytics），在安全响应领域特别重视安全事件的响应及自治，也就是 SOAR（Security Orchestration and Automation）。

21 https://www.gartner.com/doc/reprints?id=1-5WEZABX&ct=181205&st=sb

从 UEBA 方面，这个十分需要数据的导入以及上层的深度分析的功能，而象限中的，像 Exabeam 软件，就倡导并建立了一种数据驱动 + 专家驱动的混合系统，如果说基于规则的关联分析是 SIEM 的核心功能，那么 UEBA 就是 SIEM 的关键功能，Exabeam 和 Securonix 杀入了 SIEM 的领导者象限这两家公司能杀入 Gartner 领导力象限，就是依靠底层大数据架构开发的 UEBA 功能，他们家得其他功能并不突出。因此，对于传统，本地的厂商它们出于维护存量客户和已有投资等原因，无法快速将基于传统 RDBMS 的数据架构转换成大数据架构，因此无法在 UEBA 领域有突破性的进展，其所能做的，就是在已有产品的基础上进行收购合并，来补足自身在其他几个领域的劣势。像 RSA，10 年前凭借 envision 位居 SIEM 三甲，后来渐渐荒废，眼看不行又收购了 NetWitness，从 2012 年开始就一直固定在挑战者象限。然后在 2018 年，突然跳到了领导者象限且位居 McAfee 之上。仔细对比这两年的 MQ 报告，初略可以找到这个跳变的原因：因为 RSA 收购了 UEBA 厂商 Fortscale，同时在 SOAR 方向 OEM 了 Demisto，教科书般的遵循了 Gartner 的"教导"，如此这般才依旧保持在领导者的象

限中。

除了以上几点在近年来的象限中所突出和引导的亮点功能以外，我们再来看看市场上提到 SIEM，所需要它完成的工作的几大方面：

- 架构能力：包括产品形态的多样性（软件、硬件、云）、部署的可伸缩性和可扩展性，分布式部署能力、级联部署能力。
- 部署、运维和支持能力：众所周知，SIEM 的成功远非技术平台和工具所能达成，因此 SIEM 的部署、运维和支持的能力十分重要，包括如何快速高效部署和扩展，如何让用户在人员短缺的情况下高效运维，提供什么样的原厂支持，都很重要。
- 日志与数据管理能力：包括对日志事件以及非日志数据（如资产、漏洞、情报、报文等）的采集、处理与存储管理的能力。
- 实时监控能力：这对于威胁检测与事件调查至关重要。这里包括各种实时安全分析的能力，各种可视化呈现能力、仪表板，各种预置的规则、模型、分析策略等。
- 分析能力：安全分析时 SIEM 的核心功能。包括规则关联等经典分析功能，以及包括行为分析在内的高级安全分析功能。多种分析方式不是互相排斥的，而是叠加使用的，实现所谓“纵深分析”。
- 数据与应用监控能力：主要是指针对数据和应用的安全监控，核心是采集并综合分析来自专门的数据与应用安全检测设备的日志，譬如 DAP、DAM、CASB、DLP、FIM、EDR 等安全系统，还有 ERP 等各种业务系统。
- 威胁与情境感知能力：主要是指对各种情境数据的采集与运用，包括威胁情报、弱点、资产信息等。
- 用户感知与监控：这里就是 UEBA 功能，尤指 UBA。还包括采集和分析 IAM、PAM 的日志。
- 事件管理：主要是安全响应相关的能力，包括案件管理、响应工作流等，还可以包括编排与自动化的能力。
- 威胁检测工具：主要是指与各种高级威胁检测工具的集成，譬如 NTA、EDR、沙箱、FPC、FIM、取证工具、欺骗工具等。

以上是目前 Gartner 及市场对于 SIEM 平台的定位及方向。那我们回头来看，为什么企业需要 SIEM 平台。SIEM 作为企业信息和事件的管理平台，其最初的目的就是为了服务于企业客户，对公司内的所有日志信息，设备信息等进行统一的管理，从而便于企业的安全团队或者使用的安全产品来提取可能给企业造成危害的事件。

但如今的社会，随着数据本身的价值的提升以及其可交易性，结合市场上对于企业安全漏洞攻击体系的成熟及完善，社会工程学攻击的出现及爆发。企业已经不可能像以前那样，通过自身的安全团队的经验，来应对来自外部以及内部的各类全新且复杂的攻击。

在现实中，如今想要从来自不同系统，设备，安全管控软件的各类日志中，通过调度企

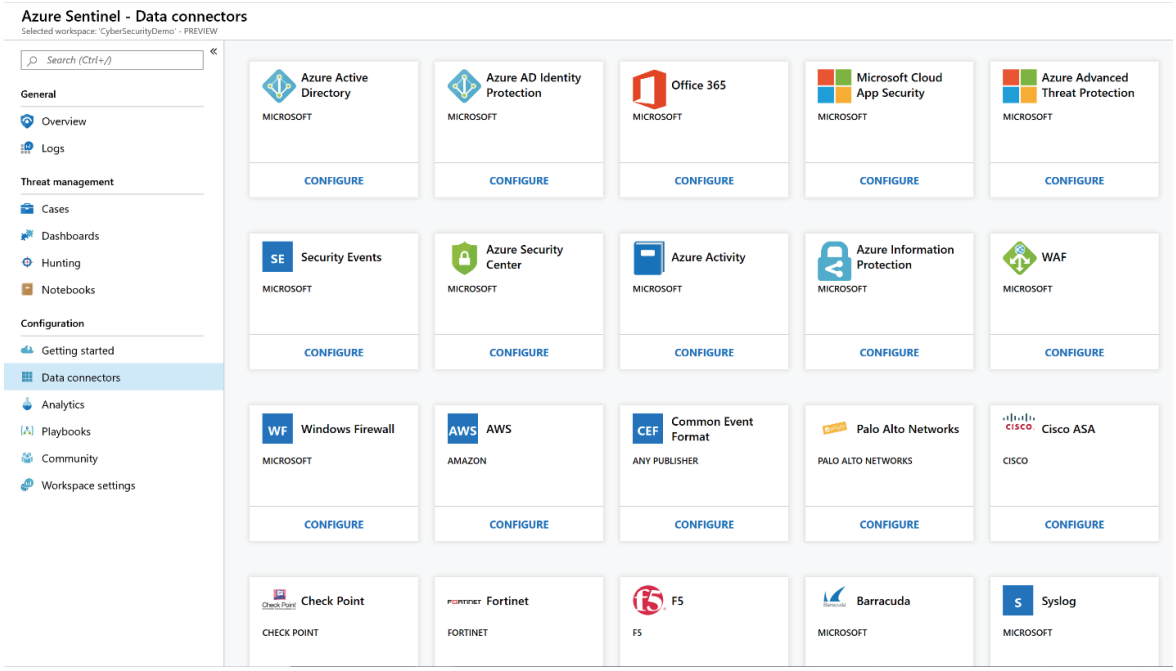
业中有限的安全资源，调整不同产品间的联动性，来提取事件，减少安全事件误报也已经变得不太可能。因为作为 IT，不仅需要对安全产品的认识的加强，还需要对所在行业中越来越细分领域的业务系统的了解，以及外部安全环境的都能同步保持更新。这对于企业的 IT 团队，是个巨大的挑战。因此，基于目前的需求，催生出了需要大数据平台才能提供的企业用户行为分析，威胁捕获等功能。

微软则结合其现有的云平台，将一方的安全部门的经验及发现应用于自研的安全平台，借助机器学习，打造了一款全新的云原生的 SIEM 平台，Azure Sentinel，为企业提供最前沿的安全防护建议的同时，为企业提供一个统一的，基于攻击逻辑的安全事件监控及管理。

接下来，我们就结合上述提到的一个完整的 SIEM 平台，从情报采集及过滤，威胁提取及勘探，事件调查，应对，及情景模拟及监控五个维度来看下 Azure Sentinel 这款纯云原生的 SIEM 平台，可以给企业带来何种保护。

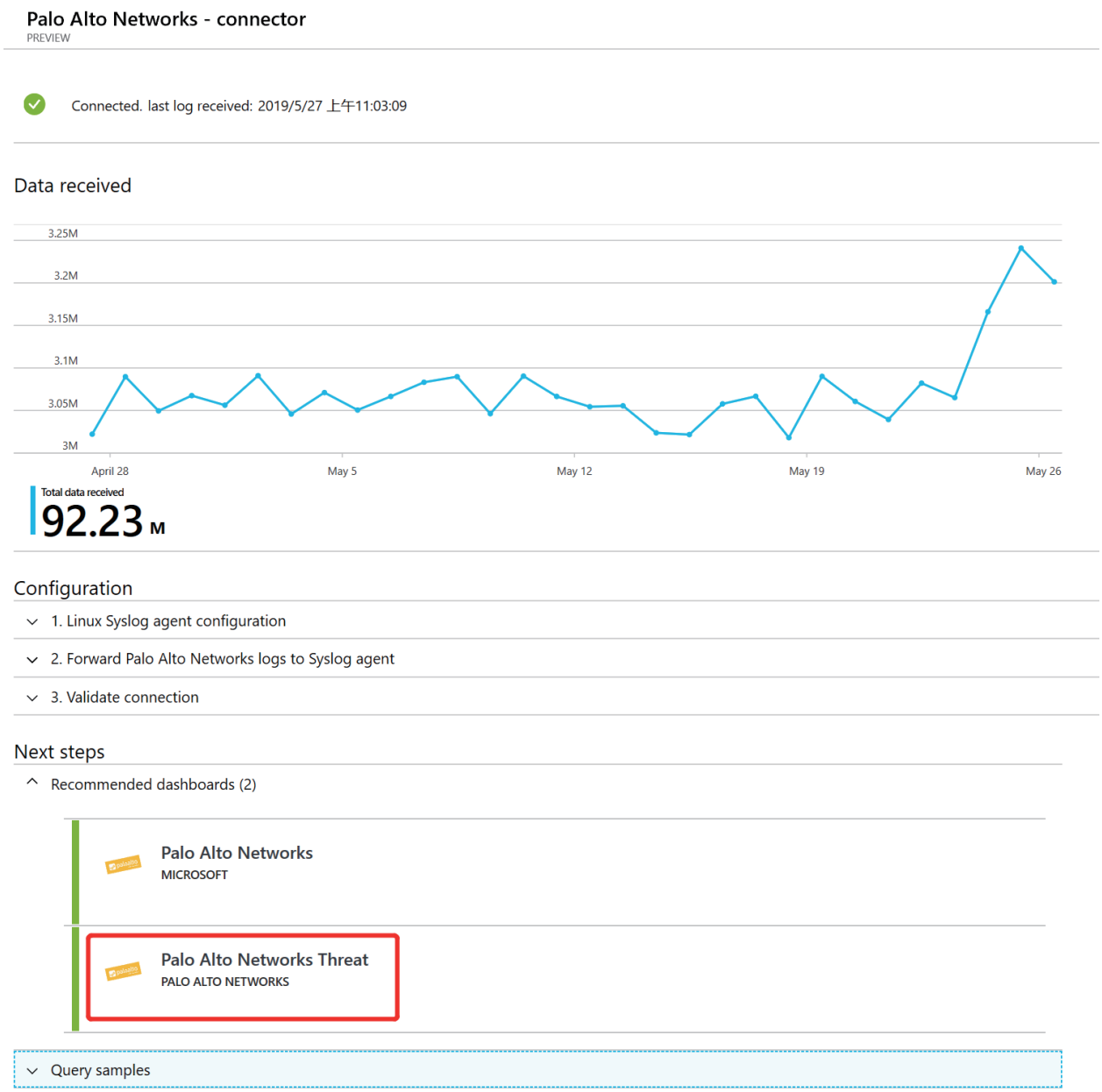
4.2 情报采集及过滤

为了能够赋能客户已有的安全产品及其他监控组件，覆盖到客户的整个生产环境，客户在使用 Azure Sentinel 的第一时间就建议来到 Data Connector 栏，将已有的微软的一方安全产品的日志信息，及三方的日志信息对接到平台上。从目前的支持列表中可以看到，我们不仅支持像 F5,Palo Alto，Check Point 等主流厂商的快速接入，您也可以通过 CEF（Common Event Format）或者 Syslog 这些常用的日志格式的文件，按配置步骤实现接入。

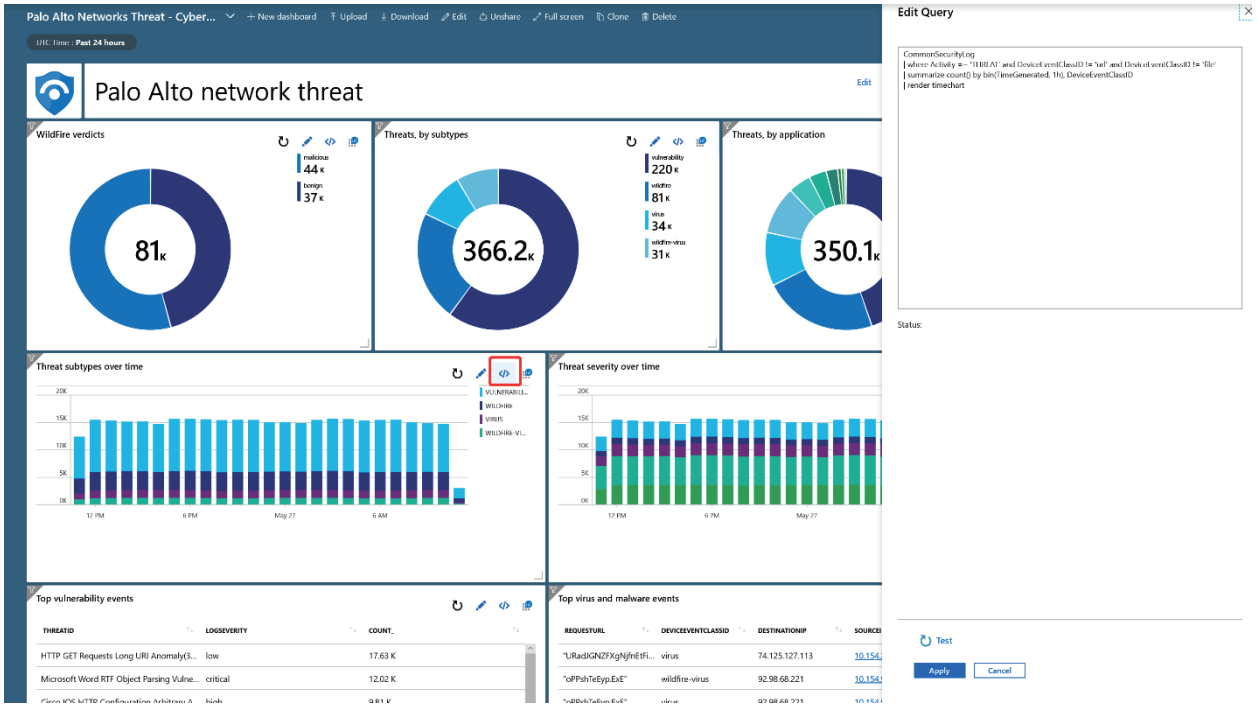


这边我们以上图中的 Palo Alto 为例进行配置，您只需按指引点击连接，之后就可以看到 Palo Alto 那边的流量信息已经展现在面板上，此外，Palo Alto 还与微软合作，将其搜集

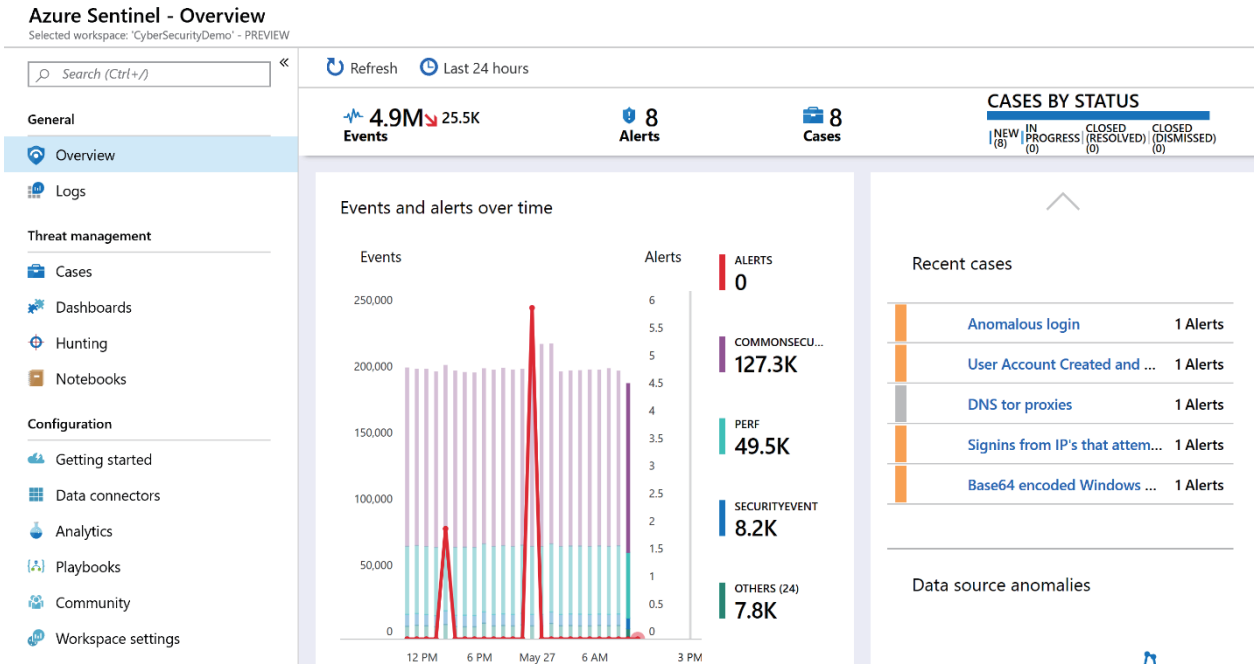
到的信息，分别由微软和 Palo Alto 两方各制作了一款完整的标准仪表板来展现客户所关心的日志信息的汇总。我们点击 Palo Alto 设计的仪表板。



进入仪表板后，可以看到威胁会按种类，来源的应用及时序的量值按重要性依次从上到下排列在仪表版上，如果您对于默认所展现的列别以及展示的时间段等信息想进行修改，都可以点击各块信息右上角的"Edit Query"来修改所要展示的信息。



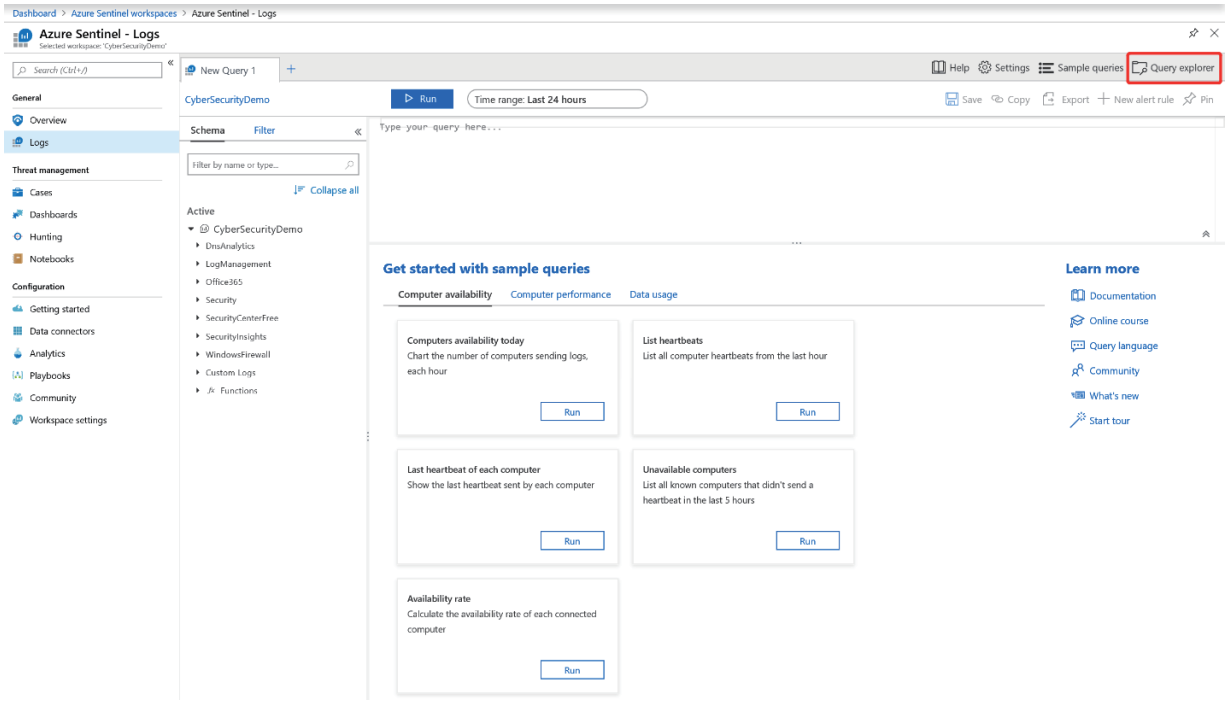
当你接入好所有一方和三方的日志后，你可以回到首页，从 Azure Sentinel 左侧的 Dashboard 中看到所有连接的 log 日志。并且你可以为不同的用户，设定他所可以查看的仪表版中所能看到的数据的权限，来符合所需要满足的合规要求。



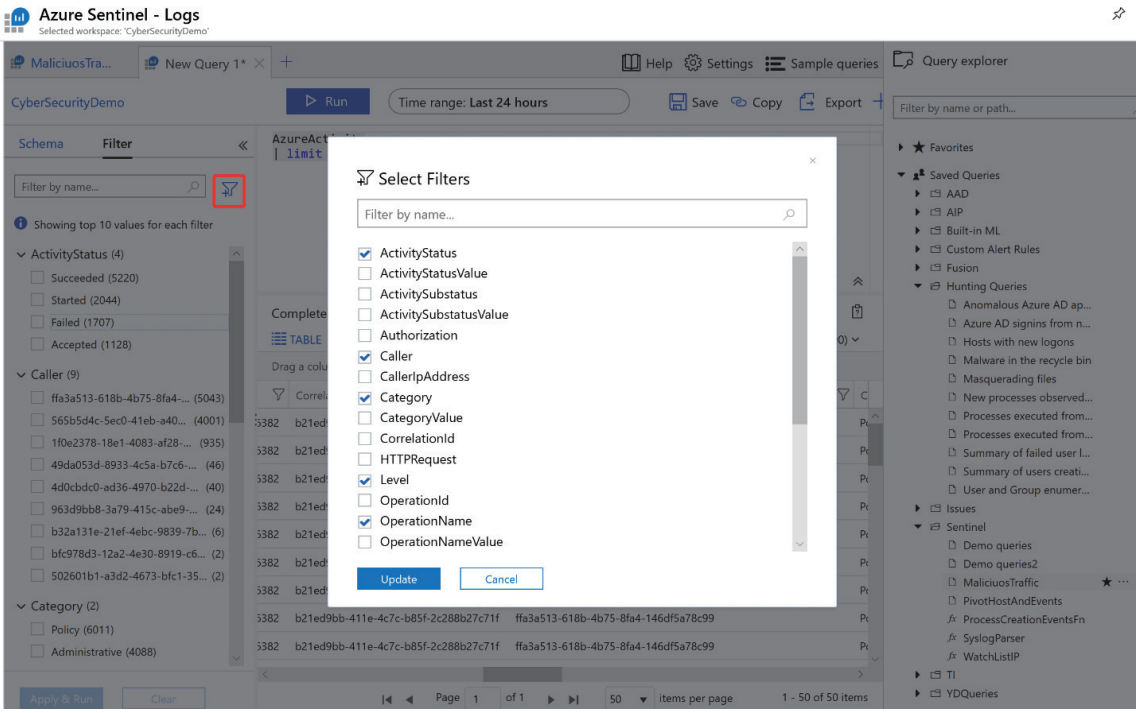
从 Azure Sentinel 首页上的默认仪表板首先会看到所监控到的所有日志中所产生的事件，网络峰值等信息按时序的展现给客户，并且把从事件所引申出来的威胁警报及案件，作为客

户最关心的重点展现在首页。

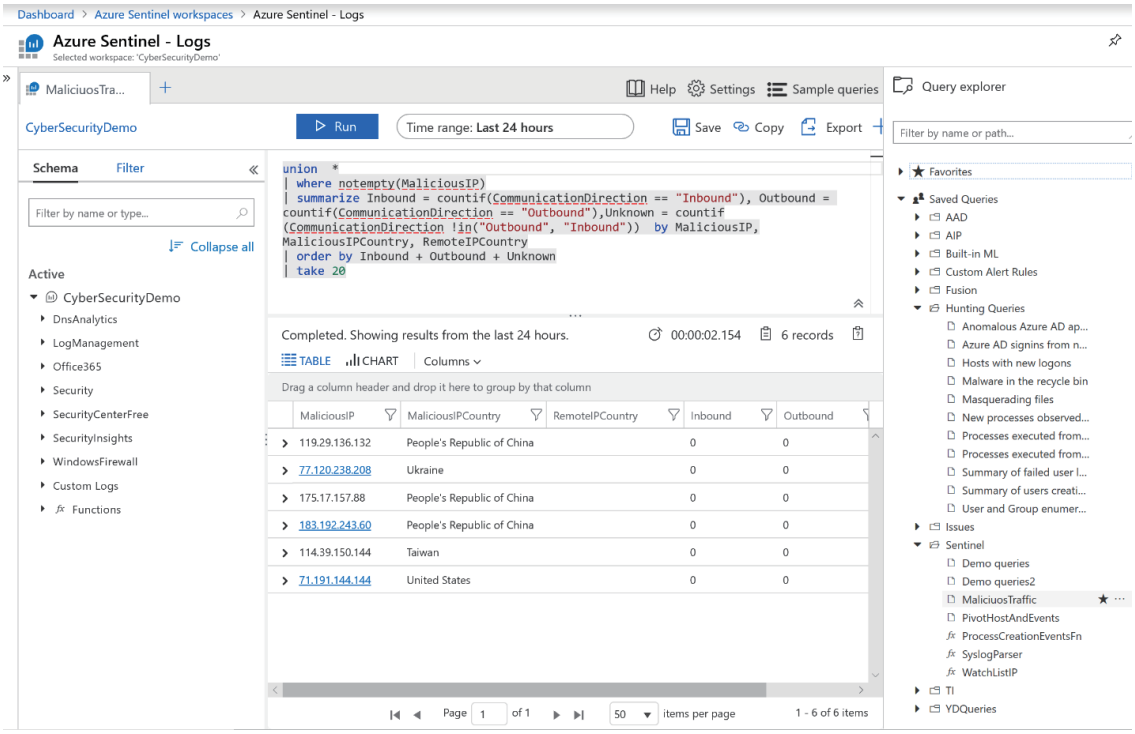
上述的仪表版只能对于日志呈现一些简单的，大局上的信息，如果需要对于特定的安全事件进行搜寻，则可以通过左侧栏中的” Logs “来对不同日志源中的数据进行统一的搜索和排查。整个 Log 平台依托于微软的 Log Analytics 以及 Azure Monitor 这两个组件，每天都会帮助客户处理 10 PB 以上的日志数据，客户只需通过短短的几行搜索命令就能够进行复杂的搜索逻辑，并且不需要考虑底层计算平台的算力，快速返回所查询到的结果。



当然，你也可以通过左侧的筛选器，对所收集的日志进行简单的分类，从而精准的执行所需要查找的日志数据。



另外，很多常用的搜索逻辑，比如查找异常登录信息，可疑 IP 地址段的提取等，你都可以直接在右侧的 Query Explorer 中利用微软安全团队已经生成的查询模板，就能够针对你接入的日志数据进行查询，查询的结果你可以根据需要，通过表单形式或者柱状图或者饼状图的形式展现在下方的结果显示栏中。



4.3 事件提取及调查

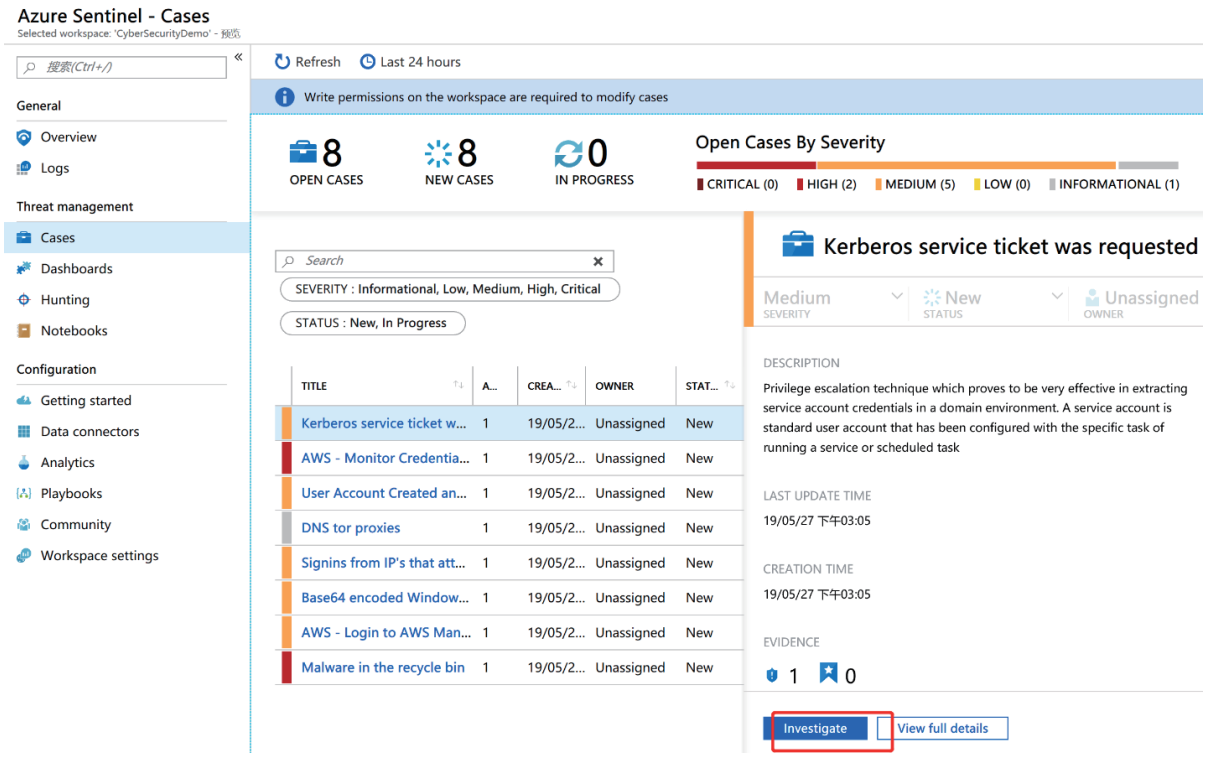
当客户将环境中的数据都悉数接入到 Azure Sentinel 平台以后，如此海量的日志信息，

平台又是如何来对真正的威胁进行提取的呢？接下来，我们来看下 Azure Sentinel 中最强大的部分之一，案件的生成，即如何从海量级的日志信息中提取出企业真正所关心的事件。

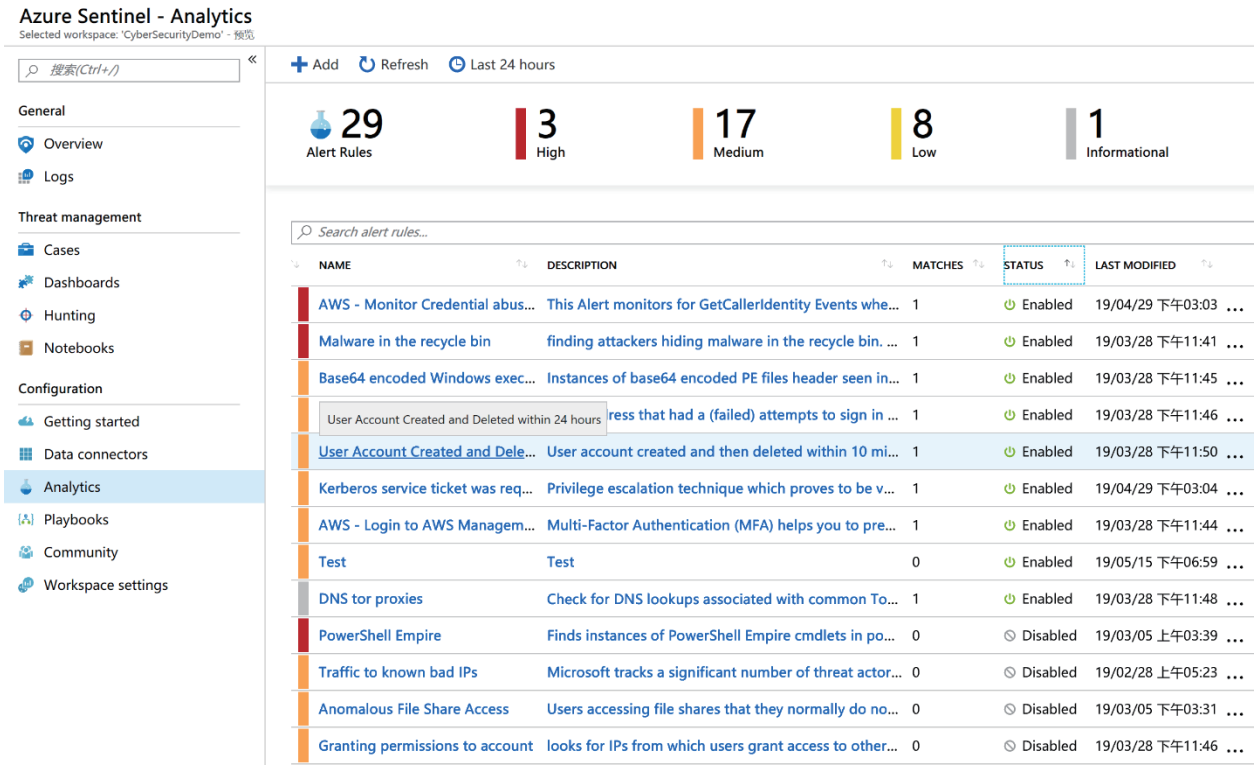
我曾经看到一份调查报告，它统计到，在 2017 年每个企业的安全团队每星期都需要面对近 1 万 7 千条的木马警告信息，以及数以十万计的各类事件，这样的一个工作面使得企业团队很难去精准的定位潜在的威胁。

同样的，微软的安全团队每天也需要面对是近四千万行的日志数据，但借助于微软的机器学习，深度学习等能力所赋能的分析工具以及团队的专业经验，他们每天能将这四千万行的日志数据筛选到只剩 100-200 个可疑事件。

微软也将这个能力，将专家对于各类事件 ID 中的洞察力，内置到 Azure Sentinel，从而让客户所需要直接面对的，变成呈几何数缩减的警报及案件，能够基于这个点，从点到面的对案件进行调查，找到真正的漏洞所在。



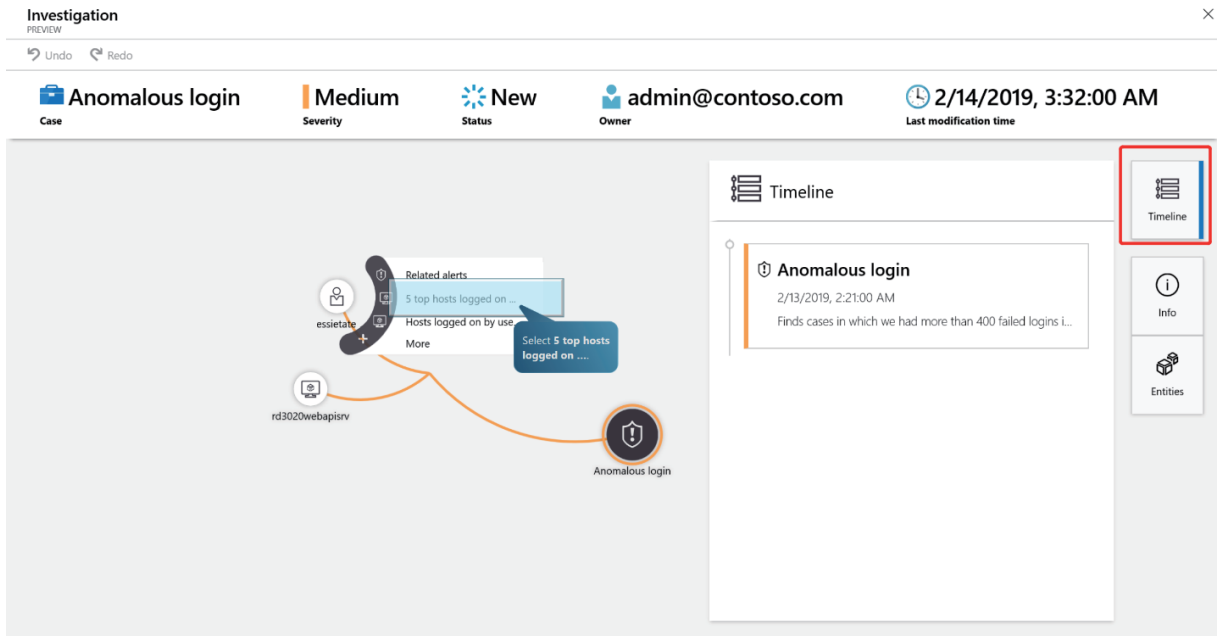
这里的 Case（案件）指的是一系列相关 Event 汇聚而成的一个案件，它可以包括多个不同的警报，这些警报来源于 Sentinel 内置的分析策略以及 Analytics 中客户自定义案件的形成方式，并且平台会按照案件的严重程度及状态反馈给客户。



案件之所以称之为案件，就因此客户的团队可以按标准流程来跟踪整个案件的进展，比如对案件的负责人进行指派，案件的进展汇报跟踪，结案等，都能通过 Azure Sentinel 平台以及借助其他工具来实现。

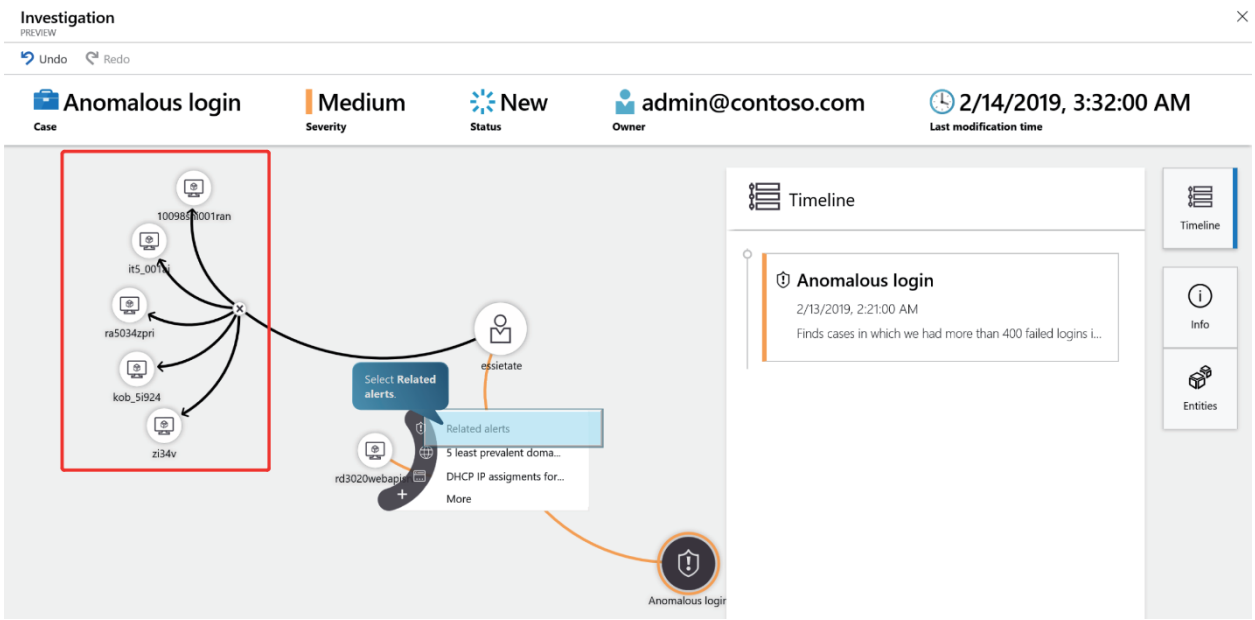
我们回到 Demo 中，大家可以看到，案件会根据发生的时间顺序，并用不同颜色标明严重程度，标识在界面上。

点击具体的一个案件，它会显示案件的描述，之后点击 Investigate 来通过发现的威胁做全面的勘探。

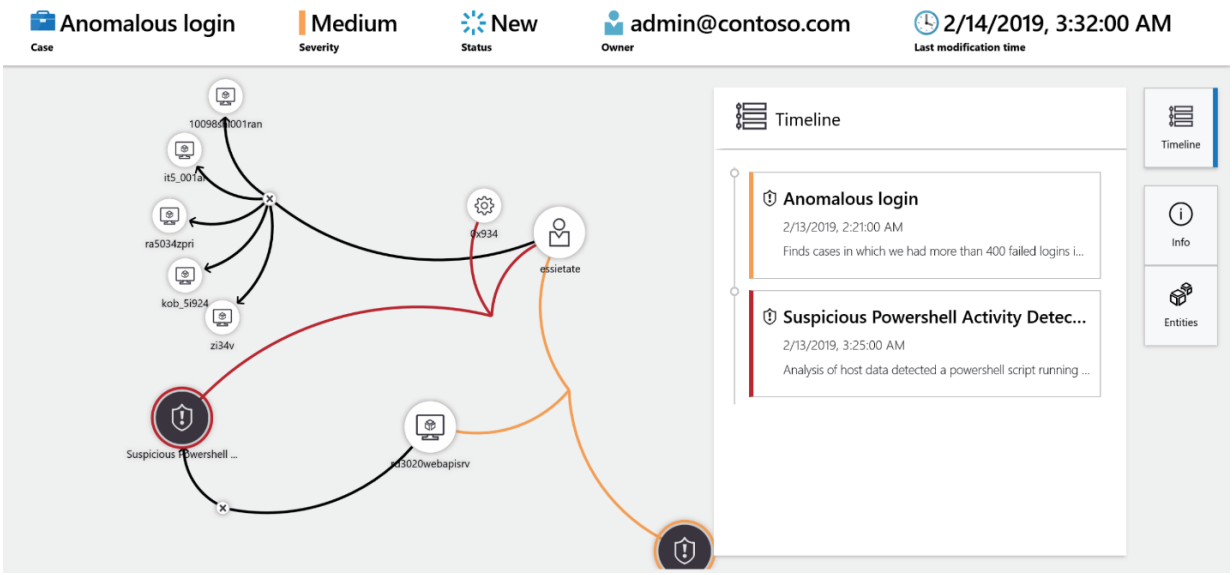


首先在 Investigate 中的右侧会把一个事件中相关的 Alerts，按时间顺序进行排列。在 Investigate 初期，Alerts 相互之间会处于独立状态。

这里我们已一次异常登录为案件发起点进行调查，点开案件后，针对异常登录自然会有异常登录的机器和异常登录的人员。我们点击人员，可以看到，你可以去查看与这个人员相关联的事件，比如这个人员所参与的其他的相关警告，或者他还在其他机器上的登录记录等。



之后点开登录的机器，我们拉出与这台机器相关的警报。



点开后发现，在 anomalous login 之后的一个事件点，还有另外一个 case，就是该机器上的 powershell 有异常的活动。这样就把这个可疑用户的行为衍生到它所造成的其他严重的事件。

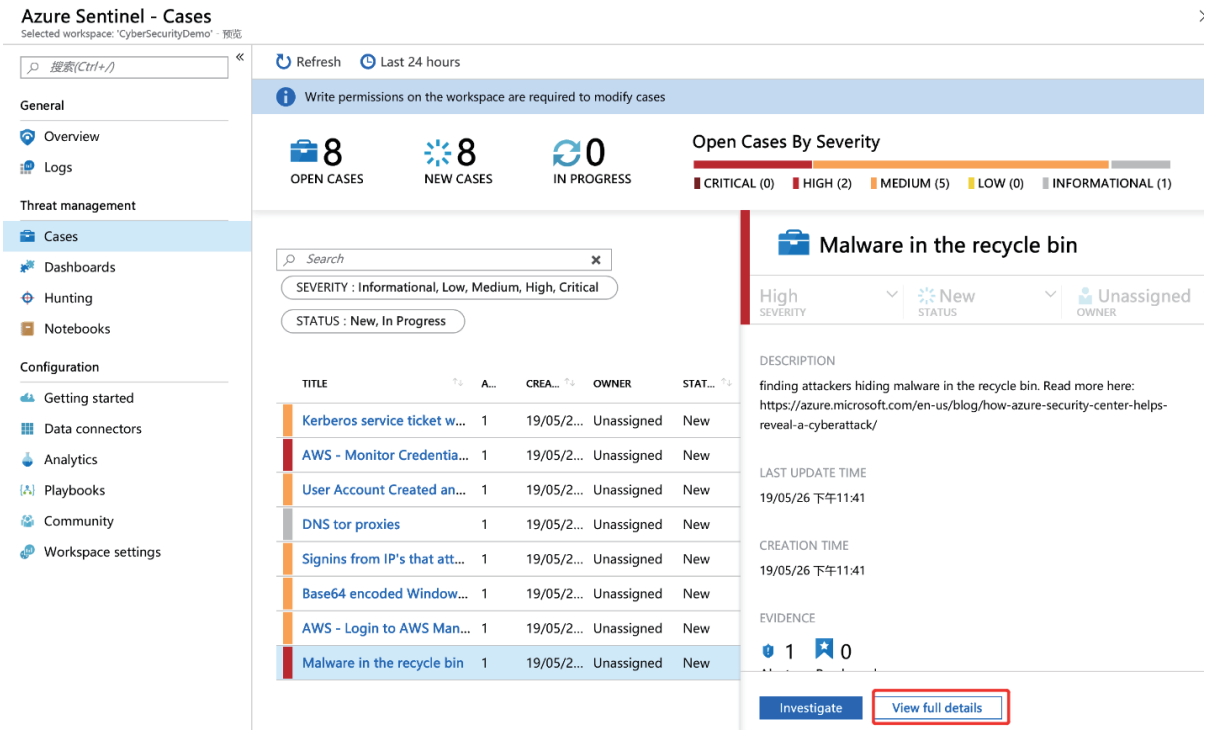
那一般的，公司的安全团队会从最严重的 case 开始调查，这样他们按照以上的逻辑倒

推回来，就会发现在以前的某个时间，是否存在该机器上的异常登录状态，追踪到具体产生异常登录的用户，并且横向移动看到该用户是否还登录了其他的机器，从而可以拦截该用户到其他几台机器上，甚至根据其产生的危害，禁止其登录所有机器等权限管控动作，快速的降低该事件在未来可能发生在其他虚机上的风险。

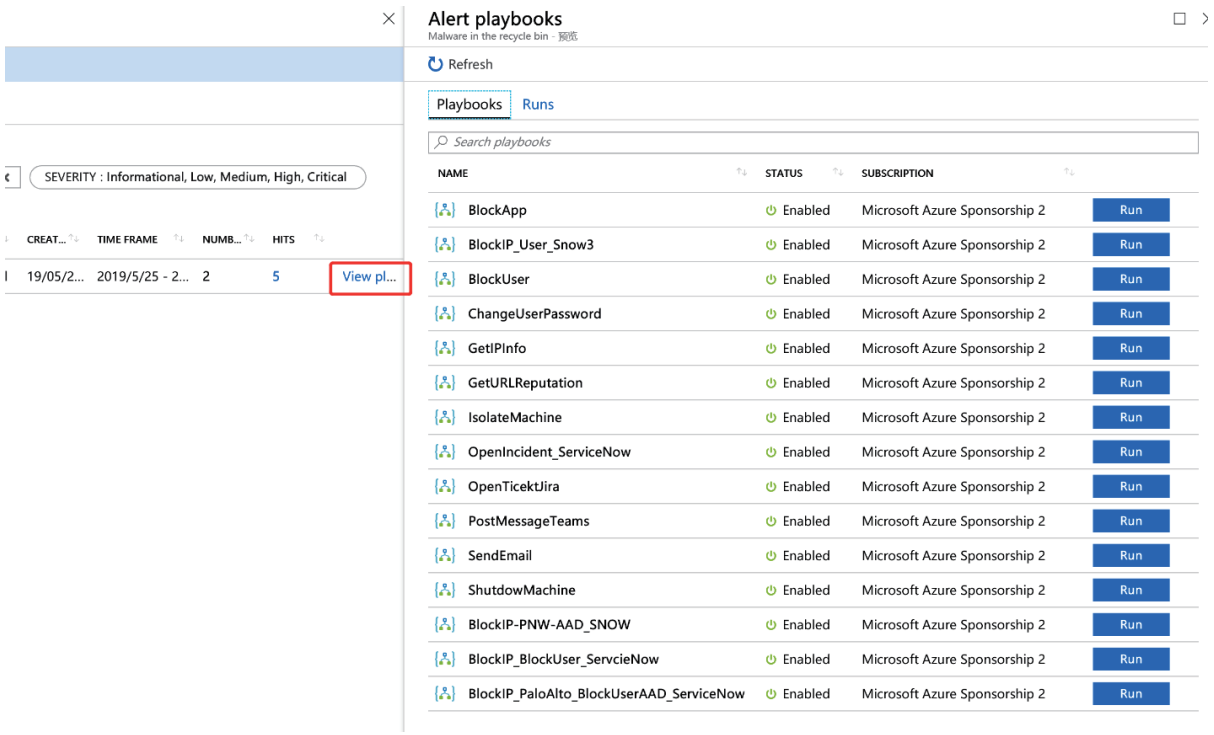
这样的一个调查过程，就能够及时从一个公司内部受危害的点，快速扩展了解到可能泄露的用户名，并看到其潜在的危害面，从而快速切断其对于公司环境内其他部分的影响，及时阻止其进入核心数据部分。

4.4 应对

查找到威胁的来源仅仅只是个开端，后续如何流程化的解决这个威胁，实现安全编排和自动相应。也是安全团队所需要去完成的工作，而这个过程，Azure Sentinel 作为 SOAR 平台，也能够帮助客户将整个 case 解决的流程给自动化。

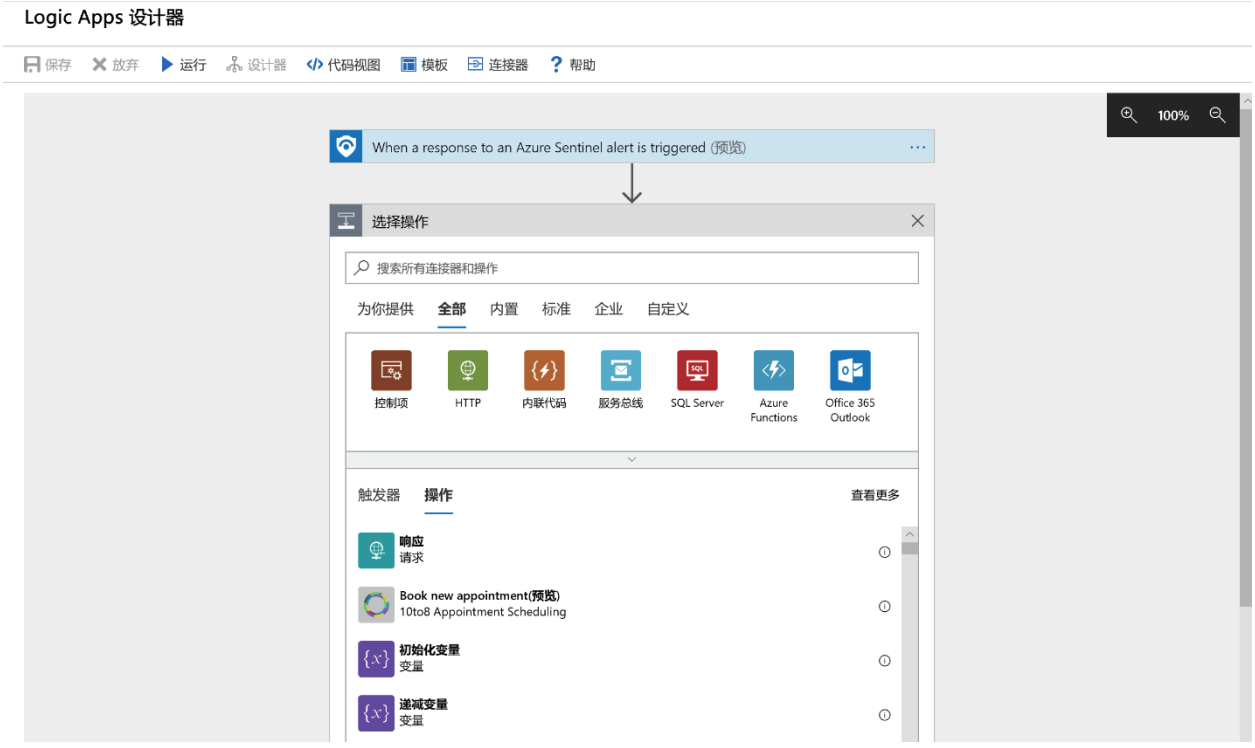


点击 View Full Details



点击 case 最右边的 view playbook，就会出现整片右边的菜单栏，这些是微软根据特定的 case 所预先生成和定义的自动化脚本，您只需一键 RUN 选择所需要执行的动作，就会触发对应的安全动作。

如果您对于所列的安全修复措施想做额外的修改和补充，您只需点击需要改进的 action，通过 Logic App 自己设计触发的逻辑及动作。



此外，在 Playbook 中，微软现在支持连接 ServiceNow, Jira 等 ticket system 来对接到客户的

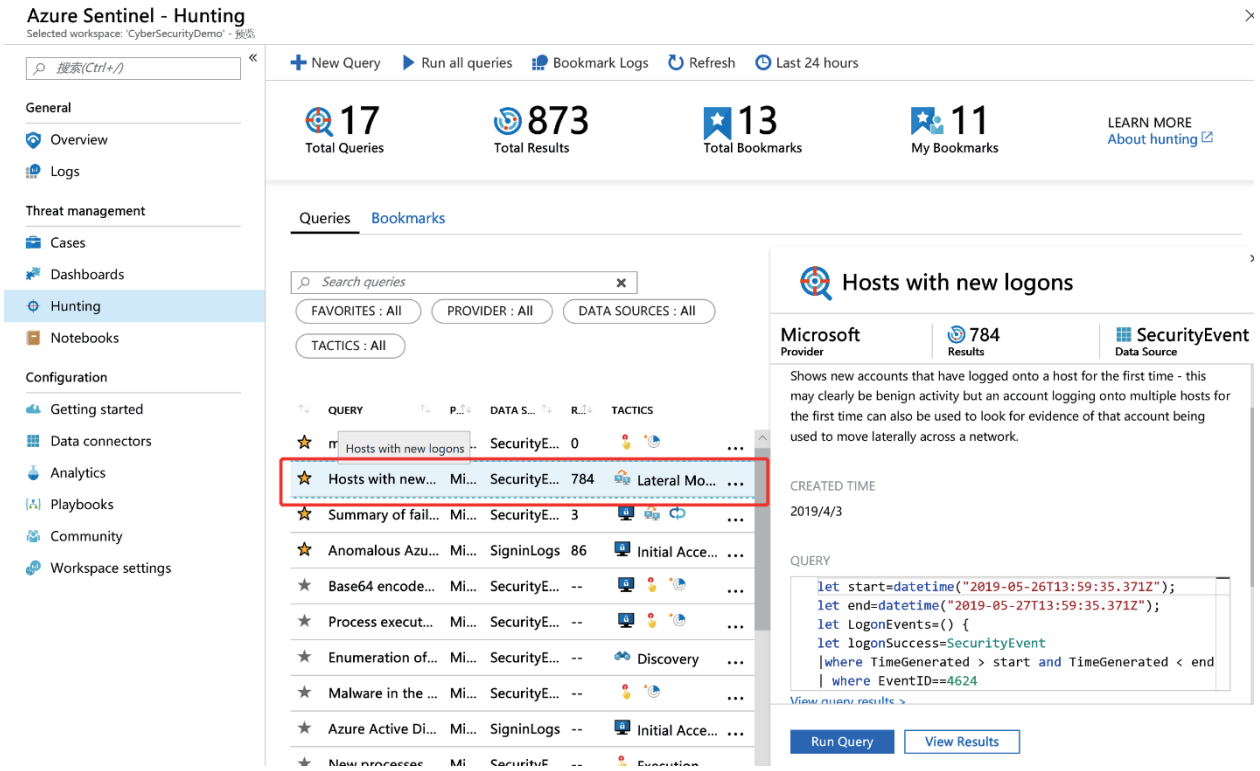
案件平台，对案件做有序的追踪，解决和记录。

4.5 情景模拟及主动搜查

除了以上一系列对于安全事件的快速响应机制，Azure Sentinel 还为客户提供了客制化安全防御的功能。

一段时间以来，公众对于安全可能一直存在一种固定认知，即安全与防御是紧密关联的，殊不知，一个成熟的安全团队，也会根据客户的行业属性，长时间对于公司内部应用，人员的使用情况的熟悉，进行主动的威胁追踪。借用 Azure Sentinel 中的 Hunting 模块，客户就可以为企业度身定做一款安全的矛，主动地去定位及清扫企业环境可能存在地风险。

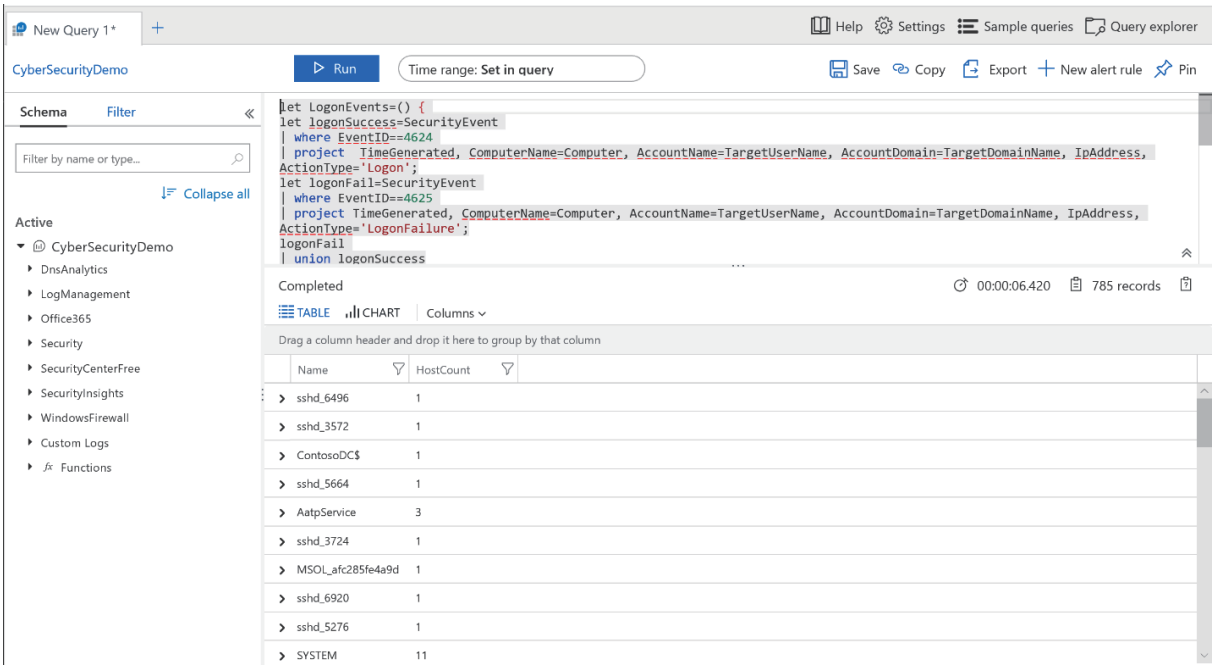
举个场景，某企业客户中，他们的安全团队清楚的了解，他们公司设计的应用所在的托管服务器常年都只由同一个用户名做登录，因此，即使公司内部存在其他账号，可能可以被赋予相应的权限，在公司内部受信任的 IP 登录这台 Host，但即使针对这个看似正常的行为，我也希望对这一个行为进行监控。因此他可以通过 Azure Sentinel 中的"Hunting"功能对所有这台托管机上新登录的这个操作进行监控及告警：



这里，我们就以针对一台服务器的登录情况，建立 Query，并定期触发这个搜索，返回相应的结果给到安全团队。

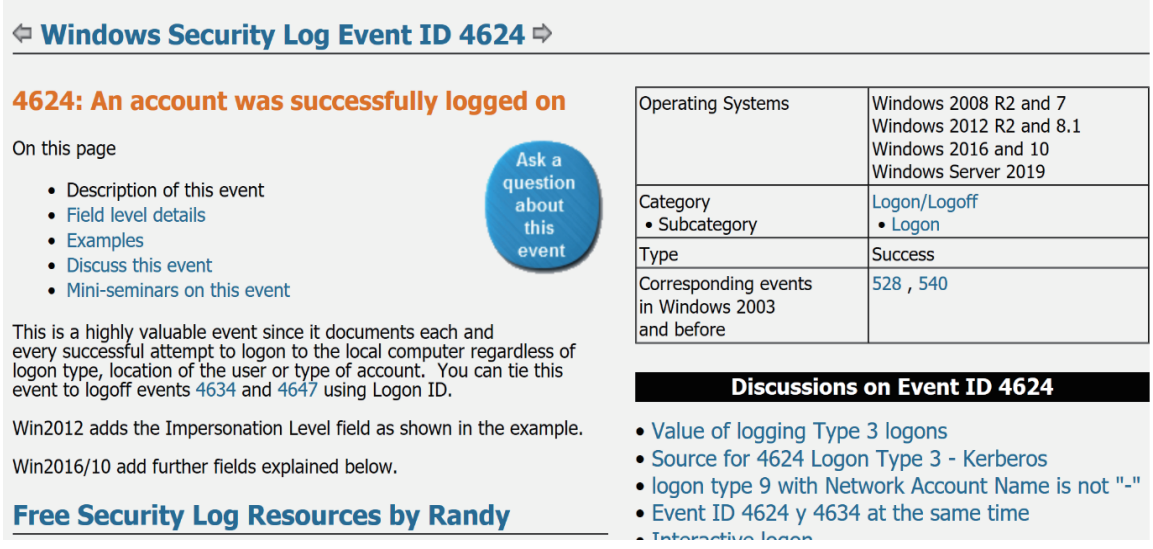
微软的安全专家团队已经为客户可能关心的几十种场景，针对不同的 log 来源，编写了对应的查询语句脚本，罗列给到客户进行选用。而在真实业务场景中，企业会出现对于公司特定成员及特定行为的主动监测，并且通过 Bookmark 来将此类结果进行标记，

从而方便安全团队在今后的事件中，提前做个标记，然后将相关联的事件能够做汇聚，可以把比如服务器上单个用户名的正常登录状态与两三个月前，该用户在其他某处的异常登录状态做关联，分析这个 ID 的行为状况。从而帮助安全团队对威胁进行预判。

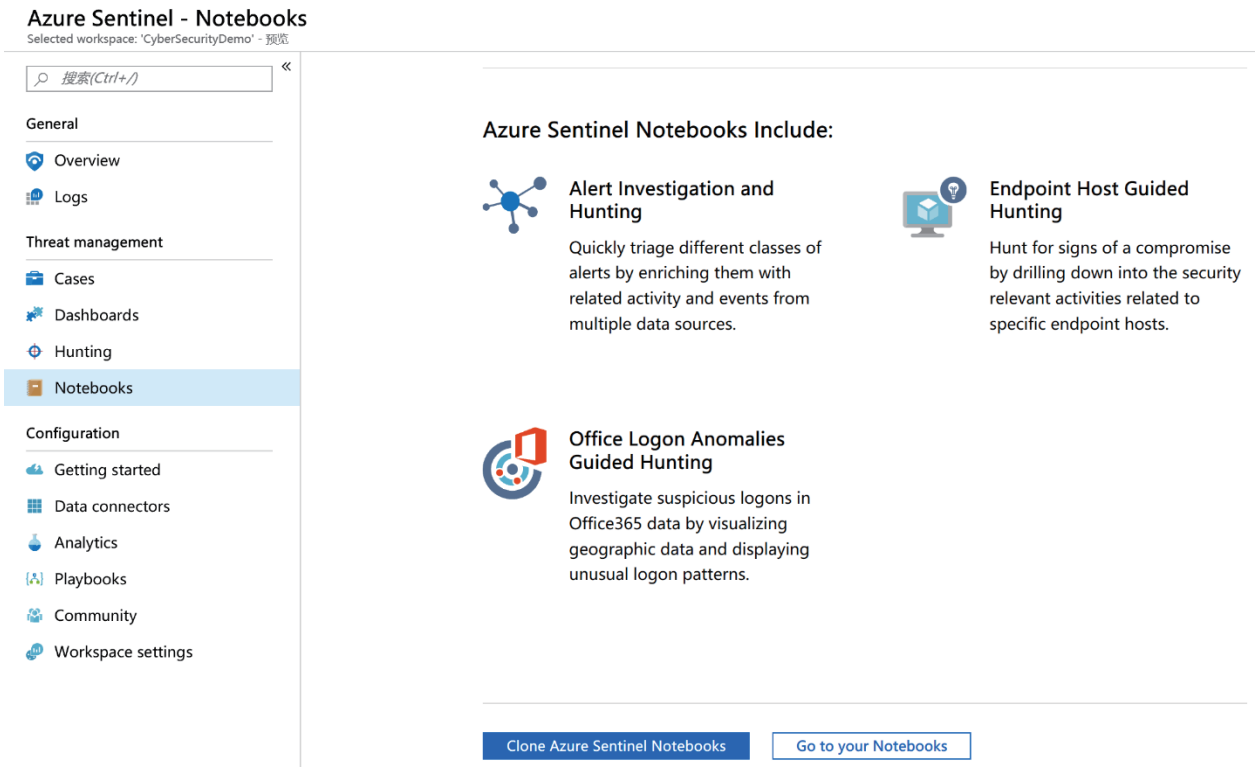


示例中，我们把所有新用户登录成功及登录失败的事件都做了一个计数。

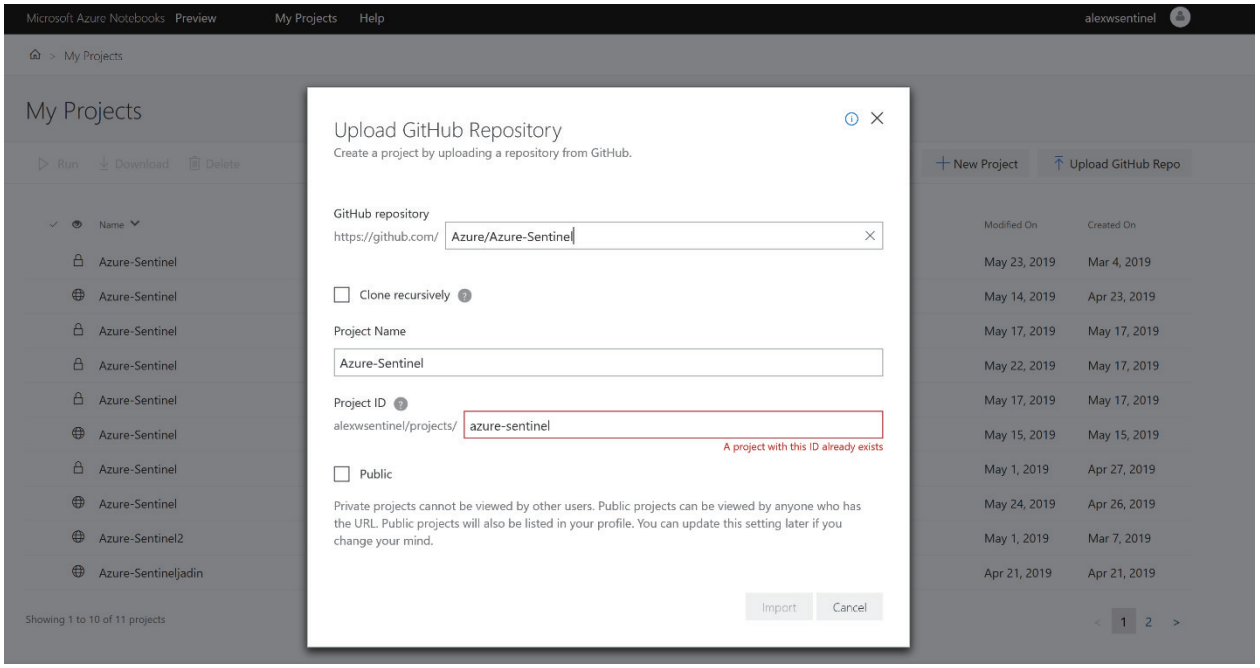
仔细来看搜索语句就可以看到，具体的搜索逻辑在这个查询中是通过 Event ID 来进行筛选。这里的 EventID 的 4624，4625 在 Windows Security Log 中都指的登录相关的事件。因此如果想了解对应到 Linux 机器中的登录情况，就可以去搜索在 Syslog 中对应登录状态的 EventID 或者 EventType 来放到查询语句中做查找。



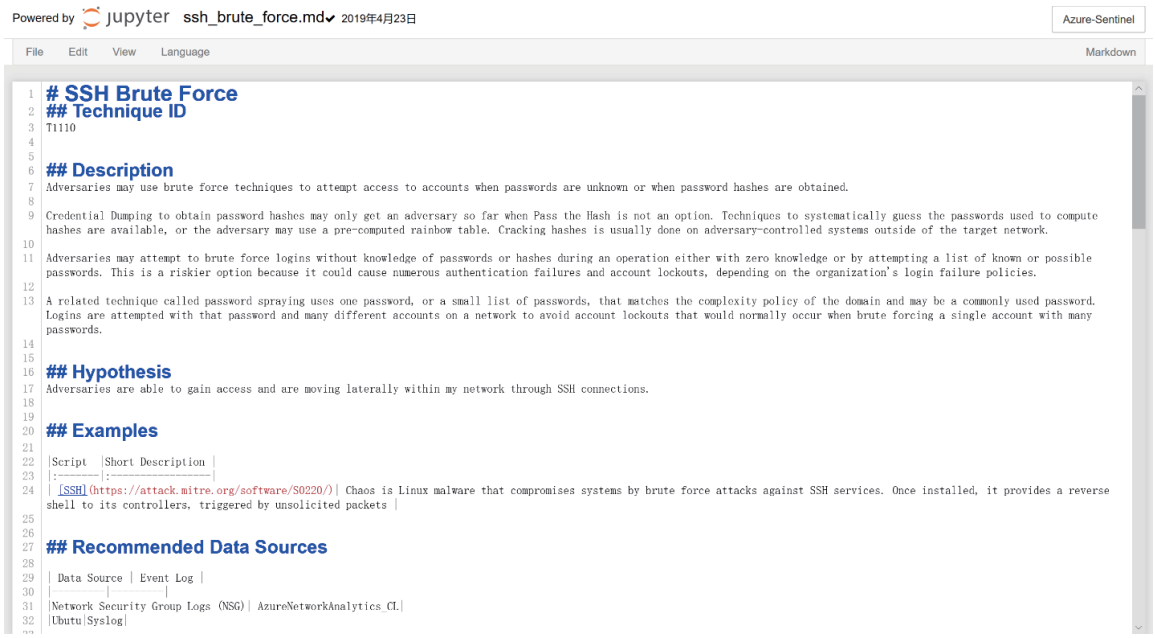
此外，Azure Sentinel 平台还为客户自定义的搜查场景提供运维平台 Jupyter Notebook，方便客户创建及运维主动调查的脚本及算力支撑。



而微软的安全团队，也会把自身的经验及所遇到的最新的调查逻辑，发布在 Github 对应的目录下面，客户也可以自行选取 Clone 到自己的目录下。



那下面我们一起来看下 Github 上的一个 hunting demo—通过 SSH 来暴力破解用户密码的这个威胁进行主动搜查的过程进行进一步的了解。



在这个 Notebook 的目录下，微软的安全工程师会按上图所示的逻辑把 Hunt 的脚本描述清楚，如 Description 中，会把暴力破解的几个场景罗列并解释清楚，并建议给客户推荐的数据收集来源。

Sample Hunting Script

```
// Start with the ML-Based SSH Alert detections
SecurityAlert
| where TimeGenerated >= ago(14d)
| where DisplayName == "Anomalous SSH login detected"

// *** Search for host across logs *** //
// Lets search over all of our data using that host name
// Replace HOST_NAME with the name of the host from the first above query
search "HOST_NAME"
| where TimeGenerated >= ago(14d)
| summarize count() by $table
| order by count_ desc

// *** Search for host across logs *** //
// Lets search over all of our data using that host name
// Replace HOST_NAME with the name of the host from the first above query
search in (AzureNetworkAnalytics_CL) "HOST_NAME"
| where TimeGenerated >= ago(1d)
| extend Host = replace(@'"]',@'',substring(toupper(tostring(split(VirtualMachine_s, "/",1))),2))
| where SubType_s == "Topology"
| where strlen(Host) > 0 and isnotnull(Host)
| project MACAddress_s, PrivateIPAddress=PrivateIPAddresses_s, PublicIPAddress=PublicIPAddresses_s, Host
| summarize by MACAddress_s, PrivateIPAddress, PublicIPAddress, Host

// ************************************************
// INVESTIGATE THE HOST
// Replace "IPs" with the IPs generated from the queries above
// name private and public ips from the first query
// ************************************************

// Lets return to the 2 ip address in the original alert
// One is a public Internet facing IP address and the other is private IP address
// Since there also could be some traffic going through a public facing lP, and
// it doesn't cost us much, lets use both ip addresses
search ("IPs" or "IPs")
| where TimeGenerated >= ago(14d)
| summarize count() by $table
| order by count_ desc
```

接下来我们来看下如何 Hunting 攻击者的暴力破解。

首先，当然需要从海量的日志数据中，把可疑的 SSH 登录的事件都筛选出来，借助 Azure 在各个组件中内置的检测机制，利用 ML 的分析能力，在事件发生的第一时间，就能够去判断事件自身是否异常。

那再经过 Azure 日志分析的大漏斗以后，就可以定位到发生可疑登录的服务器，找到这些服务器的 IP 地址等信息，经由其 IP 找到它与公司内部其他服务器间的流量往来，从而定位公司内部可能遭受公司的整个面。

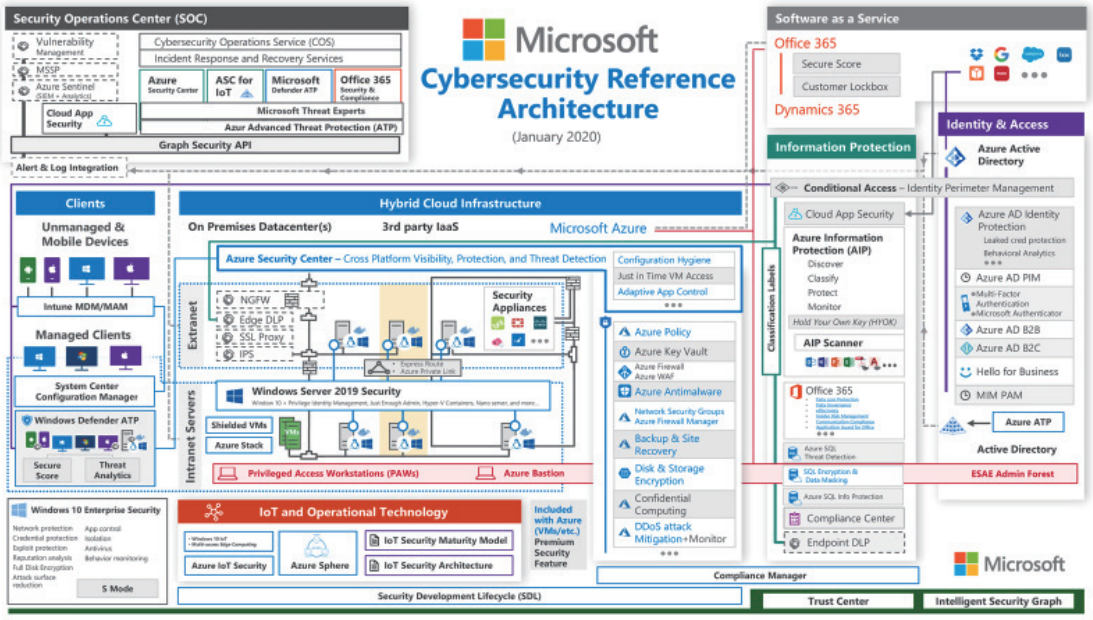
从 Sentinel 以上的功能点和分析的维度可以看到，Azure Sentinel 背靠微软强大的安全解决方案以及 ML 的分析能力，今后会在其与更多的微软一方的解决方案如 Office 365 ATP 相结合，依托于强大的 AAD 体系 (Azure B2B, Azure B2C)，将监测的颗粒度可以落到每个人员的 ID 上，帮助企业建立新型的企业安全边界应对当前开放的企业办公环境。保证企业中每个员工灵活高效的办公方式的同时，保护企业的数据及资产安全。

Chapter 5
微软安全功能总结

"Security is our top priority and we are committed to working with others across the industry to protect our customers."

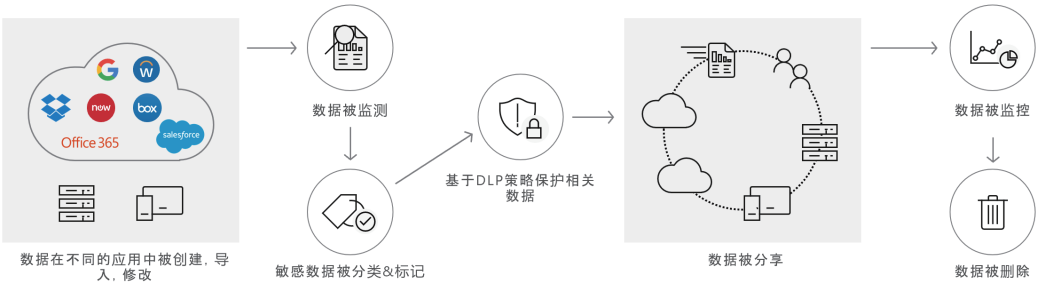
--Satya Nadella

一直以来，微软在开发每一项产品的同时，都会考虑其给到企业的安全性的保障，每年，微软都会投入超过十亿美元在安全方面，来保证已有的服务的安全性，以及开发更好的产品及服务，来帮助客户做到安全。下图将截止到目前为止，微软能够给到企业不同服务和领域的安全功能进行了总结。



可以看到从最右部分的身份及访问管理，基于 RBAC 以及 Zero Trust，结合 Azure B2B,B2C 或者本地 AD 作为企业中微软一方产品或者其他第三方的软件的身份，从而将所有的用户的日志都汇总到一个实体中，为后续建立企业身份的信用体系打下基础。

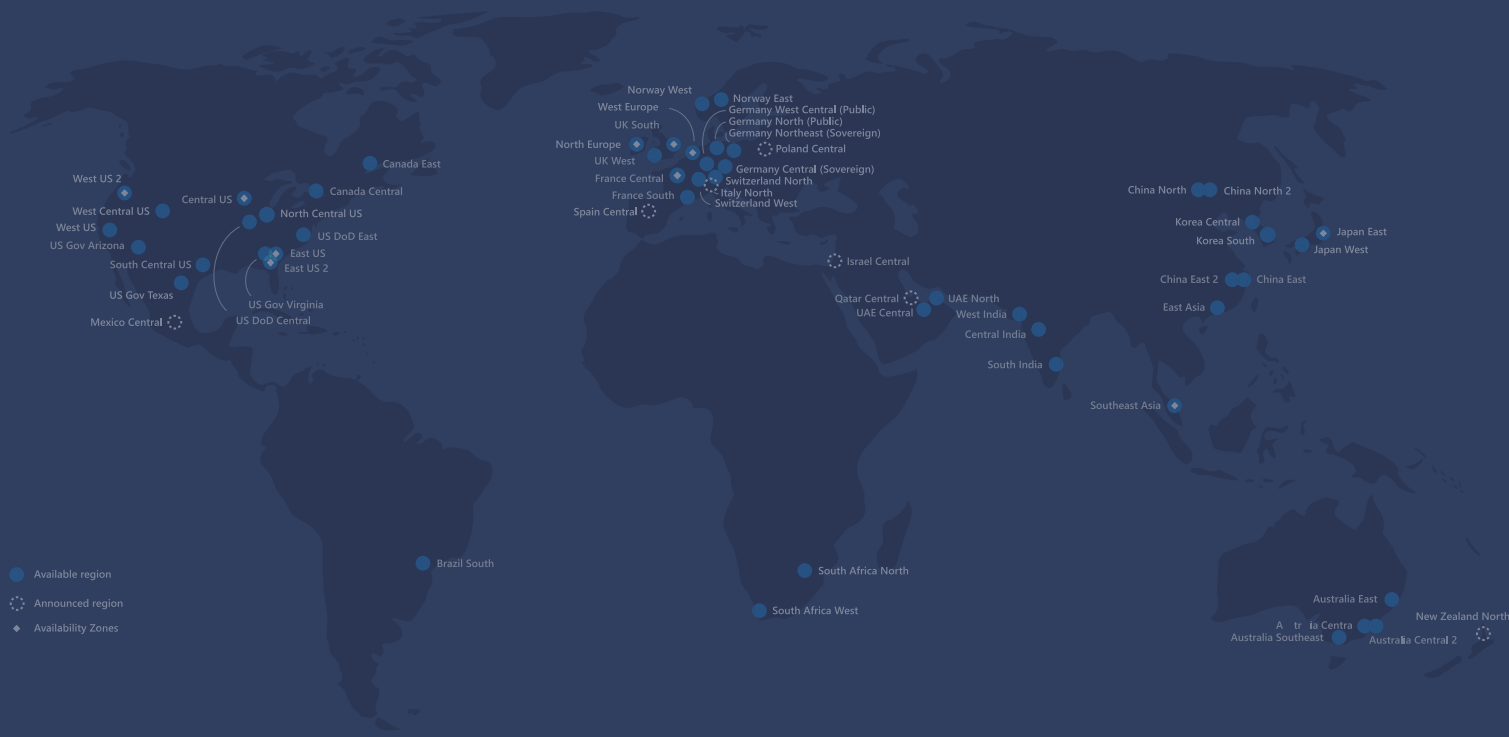
之后基于 Azure AD 的身份，将企业内部流转的信息，在不同的平台上，不管是本地服务器中，的还是邮箱或者企业信息管理平台，通过对于信息本身的敏感分级及保护，做到企业内部信息的全生命周期管理。



而传统领域对于服务器端的防护和监控，微软也在 Azure 端提供了各种功能，从虚拟机，到网络，到数据，以及从流程上，能够满足客户根据不同的合规及政策要求，完整地搭建整套安全框架。

如果客户对于企业安全环境有更高地要求，需要完整的一套安全监控及响应机制，Azure Sentinel 可以作为客户的依赖平台。只要通过 connector 将本地的，微软一方的，三方的应用及日志接入到平台，就能实现，对于企业中用户的，各类服务的，各种维度的监控及探测。

Microsoft


Norway West
Norway East
West Europe
Germany West Central (Public)
UK South
Germany North (Public)
Germany Northeast (Sovereign)
North Europe
Poland Central
UK West
Germany Central (Sovereign)
France Central
Switzerland North
Italy North
France South
Switzerland West
Spain Central
Canada East
West US 2
Canada Central
Central US
West Central US
North Central US
West US
US DoD East
US Gov Arizona
East US
South Central US
East US 2
US Gov Texas
US Gov Virginia
Mexico Central
US DoD Central
Israel Central
Qatar Central
UAE North
UAE Central
West India
Central India
South India
Southeast Asia
China North
China North 2
Korea Central
Japan East
Korea South
Japan West
China East 2
China East
East Asia
Brazil South
South Africa North
South Africa West
Australia East
New Zealand North
Australia Southeast
Australia Central 2
Available region
Announced region
Availability Zones