白皮书

缓解风险，阻止并切断杀伤链

借助 Akamai Guardicore Segmentation 尽可能降低勒索软件的影响

概述

勒索软件一度只是令人烦恼，因为网络犯罪分子会用它来加密文件和数据，造成这些内容无法正常访问，但时至今日，它已演变成更加糟糕的攻击方法。数据永久损失的威胁本身就足以令人不安，更何况网络犯罪分子和国家民族主义支持的黑客的技术已经足够娴熟，能够利用勒索软件渗透大型企业、政府机构、全球基础架构和医疗保健公司，从而造成严重破坏。

2017 年，WannaCry 加密蠕虫病毒利用 Microsoft Windows 系统的一个漏洞入侵了全球 23 万台电脑，成为勒索软件引发广泛关注的一个重大节点。自那之后，攻击者的手段愈加狡诈，攻击日渐普遍。这其中包括勒索软件即服务 (RaaS) 问世，这为黑客打开了出售其服务的大门。《2022 年上半年 Akamai 勒索软件威胁报告》评估了 Conti 的攻击模式，这个恶名卓著的 RaaS 团伙最初曝光于 2020 年，其大本营似乎位于俄罗斯。分析表明，针对横向移动的有力保护必不可少，在抵御勒索软件方面，这类保护可以发挥关键作用。除此之外，调查还发现，绝大多数 Conti 受害者都是收入在 1,000 万美元到 2.5 亿美元之间的企业。

> 微分段技术仅允许建立已在策略中明确定义的连接，从而减少网络中的隐含信任，为机器间流量的应用场景实施最小特权访问权限。
>
> - Forrester，《Zero Trust 微分段最佳实践》(Best Practices For Zero Trust Microsegmentation)，2022 年 6 月 27 日

这清晰地表明，陈旧过时的技术、仅关注安全边界和端点的那种所谓“够用就行”的防御策略、培训不足和不良的安全习惯，再加上没有已知的“万能型”解决方案，这些不利因素相互交织，造成各种规模的企业都面临风险。事实上，Cybersecurity Ventures 的《2023 年勒索软件对手方分析报告》(Who's Who In Ransomware: 2023 Report) 预测，到 2031 年，勒索软件平均每两秒就会向企业、消费者或设备发起一次攻击。

勒索软件有赖于横向移动

勒索软件攻击最初始于入侵，其手段通常是网络钓鱼电子邮件、利用网络安全边界中的漏洞或暴力破解攻击，目的是找到突破口并使防御偏离攻击者的真实意图。一旦恶意软件侵入某个设备或应用程序，就会在网络和多个端点内继续进行权限升级和横向移动，从而最大限度地扩大感染范围并增加加密点数量。攻击者通常会获得域控制器的控制权，接着盗取凭据，然后找到并加密数据备份，以防止操作人员恢复被冻结的服务。

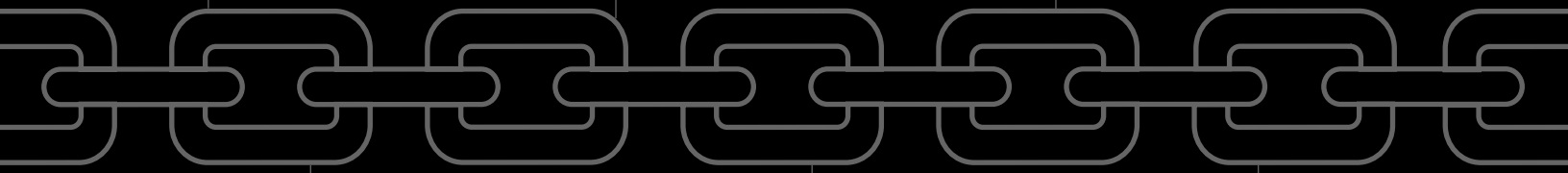
横向移动是攻击成功的关键。如果恶意软件无法传播到着陆点之外，它就毫无用处；因此，关键在于阻止横向移动。Akamai Guardicore Segmentation 这样的解决方案包含监测和分段功能，可以帮您迅速制定相应策略，以防范和控制最初的入侵。此外，您还会收到关于横向移动和其他可疑行为的警报，使您可以尽早检测到恶意软件，从而迅速作出反应。

第 1 部分：切断勒索软件杀伤链：风险缓解和防范

勒索软件并不是通过入侵单台机器或设备来实现传播。网络犯罪分子利用勒索软件来尽可能多地加密网络中的系统，从而迫使受害者支付赎金。

由于勒索软件是一种多层面攻击，因此实施多层防御有助于防止出现广泛的损害、数据丢失和停机。第一层防御是尝试防止勒索软件的初始感染。

勒索软件杀伤链



1. **初始立足点**
   （鱼叉式）网络钓鱼或易受攻击的服务
2. **横向移动**
   在整个网络中传播，尽可能扩大影响
3. **渗漏式攻击**
   寻找并窃取有价值的数据
4. **加密**
   使用 PKI 实施加密，以防止破解
5. **赎金通知**
   壁纸、电子邮件、勒索 txt 文件等
6. **影响**
   数据、财务、品牌等

防止初始感染

对任何网络来说，与互联网的接触点都是最容易出现漏洞的地方。尽管许多勒索软件攻击依靠的都是鱼叉式网络钓鱼，但没有什么能够阻止它们破坏您在互联网上公开提供的服务。

利用 Akamai Guardicore Segmentation 的监测功能，您可以监控自己在互联网上公开的服务，并针对以下各项制定相应策略来限制其暴露范围：

- 远程访问服务（RDP、SSH、TeamViewer、AnyDesk、VPN）
- 可能存在漏洞的服务（Apache、IIS、Nginx）
- 可能存在漏洞的机器（使用其他 Insight 功能来检测操作系统未经修补的机器）
- 意外暴露的服务（数据库、域控制器、内部 Web 服务器或文件服务器）

利用分段来切断杀伤链

网络上的某些点难免会遭到入侵。其原因可能是鱼叉式网络钓鱼、人为错误，也可能是某台服务器上运行着一项未加以合理缓解的漏洞服务。正因为如此，制定合适的风险缓解策略至关重要。

一旦机器遭到入侵，您就需要限制病毒在网络内的传播。您可以通过三种方法达到此目的：

1. 通过应用程序安全围栏实现分段

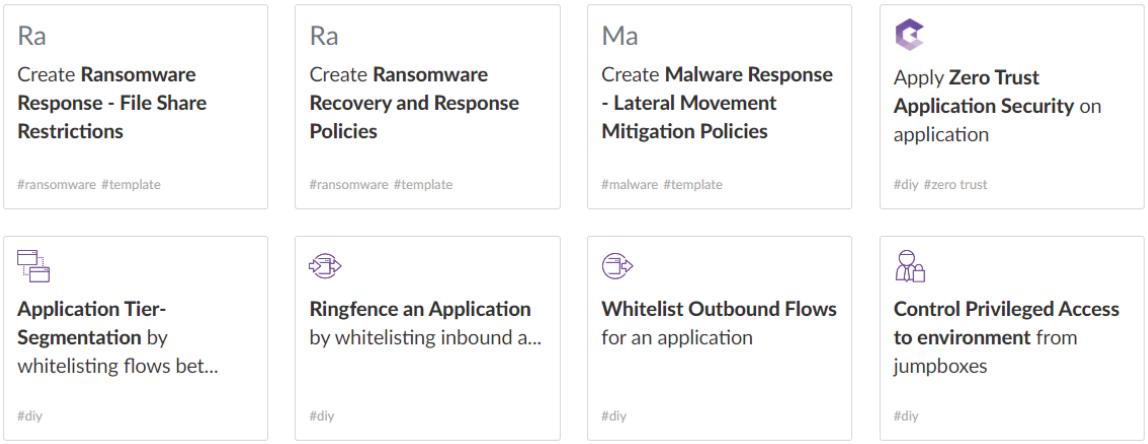
您需要将网络划分为多个可操作的段（按应用程序、用途或环境进行划分），并且不允许在这些段之间及之内建立不必要的连接。

您可以考虑采用以下四个分段准则：

- 阻止笔记本电脑/工作站之间的任何通信。
- 阻止使用“强力”域用户权限（例如域管理员）运行的进程所发出的通信。
- 对可以在服务器上执行进程的用户进行限制。
- 限制笔记本电脑/工作站对数据中心服务器和云实例的访问。

Akamai Guardicore Segmentation 使您能够轻松抵御勒索软件，保护您的网络。您可以利用预构建的模板，通过简单三步完成策略设置，开始抵御攻击：

1. **选择目标**，例如为关键应用程序设置安全围栏、创建勒索软件抵御策略或保护某个活动目录。
2. **确定需要保护的相关资产**，例如需要设置安全围栏的电商应用程序资产、数据中心内的所有活动目录工作负载，或需要保护以防止勒索软件威胁扩散的端点。在许多情况下，这一步都通过 Akamai 的 AI 标记功能自动完成。
3. **通过创建策略来保护资产**。Akamai Guardicore Segmentation 的 AI 功能可以根据环境中的真实流量自动推荐策略，并总结出数百个网络内的应用程序通信模式。

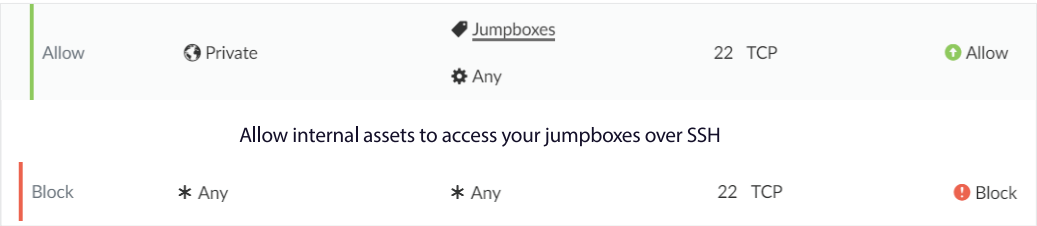


示例：Akamai Guardicore Segmentation 模板

2. 利用协议限制规则来防止横向移动

针对特定的协议和行为，存在一些通用准则。某些协议在正常的每日运营情况下发挥着固有用途，因此应对其加以谨慎限制。Akamai Guardicore Segmentation 能够直观呈现所有流量，从而针对 WinRM、SMB、RPC、RDP 和 SSH 等高风险协议，为您的环境创建高度精准的规则。

例如，SSH 有助于实现远程管理，还可用于提高其他协议的安全性（例如 sFTP），但攻击者也可能将其用作一种入侵机器并在网络内传播的手段。您需要为授权用户创建跳箱，以尽可能地限制在全网范围内使用 SSH。



在 Akamai Guardicore Segmentation 中创建的规则

3. 保护备份和关键数据服务

为了最大程度增加破坏力度，勒索软件攻击通常是以企业的备份服务器为目标，对其中存储的数据进行加密。同样，数据服务和文件服务器也是勒索软件的目标。

使用 Akamai Guardicore Segmentation 限制对备份服务器、数据库和文件服务器的访问，同时限制来自您网络之外和您网络内不需要访问的区域的访问。为尽量减少与关键备份服务器的往来通信，您可以使用 Akamai Guardicore Segmentation 为应用程序创建安全围栏，并将与应用程序的往来通信锁定到进程和用户级别。通过将数据服务限制为仅开放至运营所需最低限度，可以降低此类服务的风险系数，同时阻断勒索软件的入侵和传播途径。

第 2 部分：勒索软件检测与响应

在应对勒索软件这样的网络威胁时，预先规划和提高警惕性至关重要。只要在发生入侵时快速作出反应，就能将对网络的破坏降至最低。Akamai Guardicore Segmentation 的功能在威胁检测与响应这两方面都能为您提供极大的帮助。

利用 Akamai Guardicore Segmentation 进行威胁检测

事件可能包括：

- **欺骗**——检测和拦截可疑的横向移动企图，并将其重定向到动态蜜罐，以使其操作能得到监控和分析。欺骗事件具有高保真度，可提供关于恶意活动及网络犯罪分子下一阶段攻击的详细数据。
- **网络扫描**——网络犯罪分子一旦侵入到网络，就会开始收集情报。他们使用网络扫描作为侦察手段，以检测其他服务器正在侦听的开放端口或服务。Akamai Guardicore Segmentation 可以自动检测网络扫描，并立即向用户发出警报。
- **基于策略的检测**——网络和进程级别的安全策略可以即时识别未经授权的通信以及不符合标准的流量。

Akamai Guardicore Segmentation 提供 Insight 功能

Akamai Guardicore Segmentation 借助基于 osquery 的附加功能，提供对各个资产的监测。它所提供的查询框架可快速检测异常活动，例如卷影复制，这是勒索软件最常采用的预加密操作。它还能检测用于传送勒索软件的木马病毒，方法是搜索常用的挖空技术，该技术可以将恶意软件隐藏在 svchost.exe 之下，而后者则是一个合法的 Windows 进程。

托管式威胁搜寻

Akamai Hunt 托管式威胁搜寻服务可以针对用户网络内部的任何异常行为向用户发出警报。此功能通过各种技术实现，例如分析传入和传出的互联网连接及其关联的 GeoIP、寻找网络覆盖率正在扩大（可能表示正在传播）的新可执行文件，以及分析资产连接，从而通过相邻接口数量异常来查找横向移动的征兆。

即时响应

一旦检测到网络内部存在勒索软件等威胁，您就可以快速部署抵御措施，采用进程和用户级别的策略来主动拒绝和隔离恶意活动。

更有力的感染监测

在发现入侵线索或入侵征兆 (IOC) 后，您可以开始寻找其他征兆，例如通信模式、进程、使用的端口、感染的资产等等。Akamai Guardicore Segmentation 可帮您查找出现此类征兆的所有资产（与 C2 进行通信的所有资产、与某个唯一端口进行通信的所有资产，或是运行某个恶意进程的所有资产）。通过您的工作环境的直观映射图，您可以寻找受感染机器之间的其他相似性或传播轨迹。

第 3 部分：消除感染和恢复

获得所有受感染机器和 IOC 的列表后，即可启动消除感染的工作。将机器分为三个标签组：**已隔离**、**受监控**和**未感染**。

已隔离

- 受恶意软件**感染**的资产
- 将这些资产保持**已隔离**状态，直至恶意软件被清除

受监控

- **感染**情况不明的资产
- 持续**监控**，直至确定恶意软件已被**清除**

未感染

- 确认**未感染**且可以**正常运行**的资产

关于恢复的分段准则

设定三个标签组之后，即可开始添加策略，通过创建四个通信层来对网络进行分段：

- **阻止**所有来自**已隔离**机器的传入和传出通信。
- **阻止**传至或传自**受监控**机器的远程管理协议通信。
- 针对任何远程管理协议通信向**未感染**机器发出**警报**。
- **阻止**各个标签组之间的所有通信。

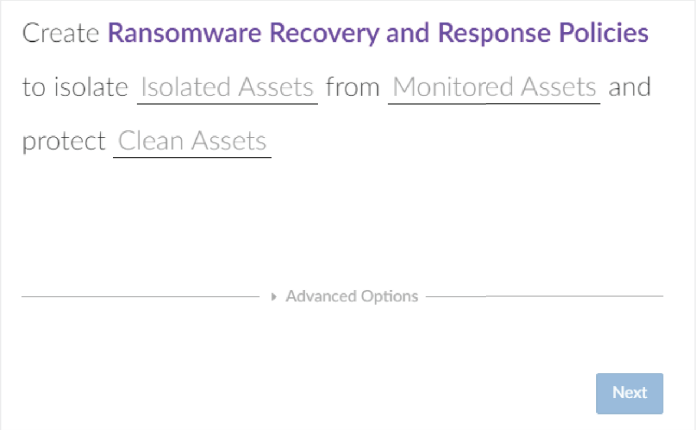
	Override Alert	* Any	Clean Any	5985, 5986 ... TCP | UDP
	Override Block	Monitored Any	Clean Any	Any TCP | UDP
	Override Block	Clean Any	Monitored Any	Any TCP | UDP
	Override Block	Monitored Any	* Any	5985, 5986 ... TCP | UDP
	Override Block	* Any	Isolated Any	Any TCP | UDP Any ICMP
	Override Block	Isolated Any	* Any	Any TCP | UDP Any ICMP

Akamai Guardicore Segmentation 中的阻止和警报规则

勒索软件恢复和响应模板

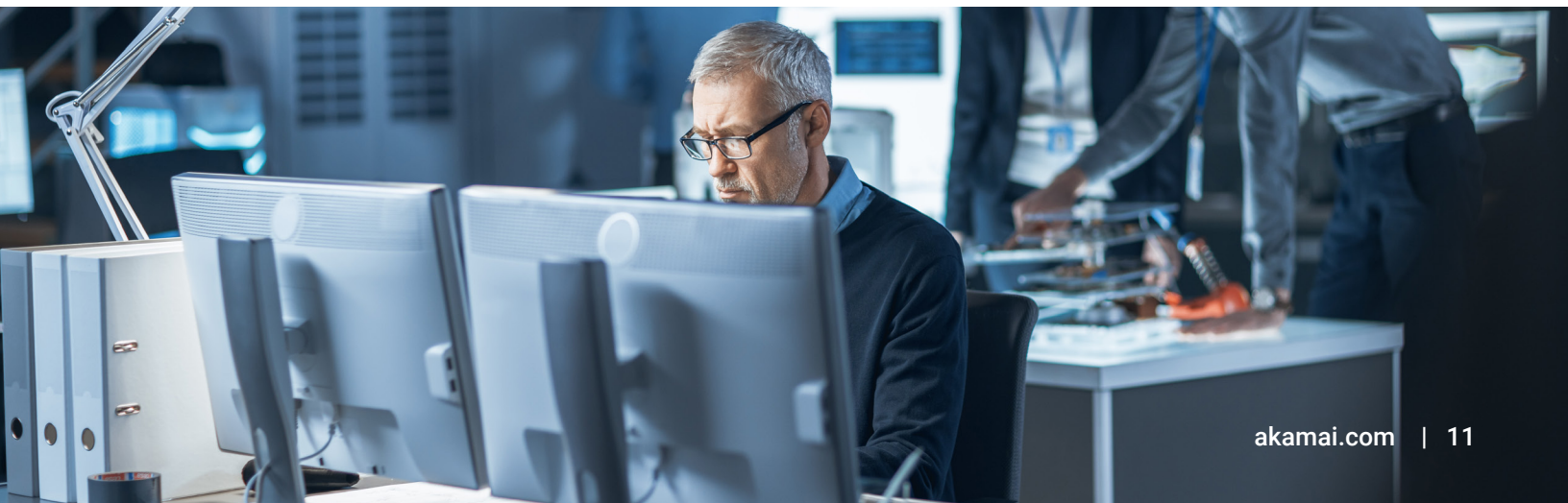
Akamai Guardicore Segmentation 中包含的勒索软件恢复和响应策略模板为您提供了一种使用简便的预构建策略，用于限制**已隔离**、**受监控**和**未感染**标签组的访问权限。

借助此模板，您可以轻松地让**未感染**机器保持持续运行，同时不必担心来自**已隔离**机器引发的感染或重新感染风险。



结论

如果您仍然依靠传统防火墙或仅保护安全边界的防御措施，则无法阻止勒索软件在您的网络中传播并锁定关键应用程序及基础架构。现实情况是：数据泄露不可避免，您必须为此做好准备。Akamai Guardicore Segmentation 可帮助您检测东西向数据中心流量中的威胁，并阻止横向移动，让勒索软件无法借助此类移动加密您最关键的资产并向您发起勒索。



利用 Akamai Guardicore Segmentation 缓解勒索软件攻击影响的五个步骤

做好准备：识别您的 IT 环境中运行的每个应用程序和资产。

预防：创建规则，以阻止常见的勒索软件传播技术。

检测：接收警报，以掌握是否有人访问分段应用程序与备份的情况。

补救：启动威胁控制和隔离措施，在检测到攻击时立即采取行动。

恢复：借助可视化功能，获得对分阶段恢复策略的支持。

阻断勒索软件在您网络内的横向移动。
仍有疑惑？何不眼见为实。akamai.com/guardicore

无论您在何处创建何种内容和体验，也无论您将其分发到何处，Akamai 都可在其中融入安全性，从而保护您的客户体验、员工、系统和数据。我们的平台具备监测全球威胁的能力，这让我们得以帮您调整并增强安全状况，从而实现 Zero Trust、阻止勒索软件、保护应用程序和 API 或抵御 DDoS 攻击，让您信心十足地不断创新、发展和转型。如需详细了解 Akamai 的安全、计算及交付解决方案，请访问 akamai.com 和 akamai.com/blog，或者扫描下方二维码，关注我们的微信公众号。发布时间：23 年 05 月。

扫码关注，获取最新CDN前沿资讯