交互式网络安全场景电子书

真实场景。更明智的决策。更强大的防御。

戴尔对安全性的承诺是我们所做一切工作的核心。本电子书通过分享见解、最佳实践和创新技术，旨在为您提供所需的工具和知识，帮助您防范新兴网络风险。

选择攻击场景

网络安全威胁不断演变，组织需要有效响应以保护其数据。要让您的组织做好充分准备，不妨沉浸在真实的模拟练习中，助您制定网络安全战略以有效应对网络攻击。

了解各种攻击类型和行业特定挑战，场景涵盖联邦、州和地方政府以及金融服务和医疗保健等行业。在此过程中，您将了解戴尔的集成安全解决方案（从笔记本电脑和台式机到企业系统）可有效防范这些威胁。

- 备份渗透 →
- 勒索软件 →
- 分布式拒绝服务 (DDoS) →
- 供应链硬件 →
- 恶意内部人员 →
- 供应链软件 →
- 中间人攻击 (MITM) →
- 零日攻击 →
- 提示/SQL 注入攻击 →

攻击类型：备份渗透

作为云备份服务提供商的经理，一天晚上，您接到一位客户的电话，他们正在尝试还原丢失的一些数据。

他们多次尝试从云中恢复，但总是失败。

您去办公室发现所有电脑屏幕都显示全部数据已加密，要重新访问数据需要支付赎金。

检验掌握情况 →

攻击类型：备份渗透

1：减小受攻击面　2　3　4

您不确定哪些备份系统或客户受到了影响。您第一步应该做什么？

- [ ] 通知相关机构
- [ ] 关闭所有系统
- [ ] 尝试遏制并隔离威胁
- [ ] 确定您是否有干净备份可用于还原

查看正确答案 →

攻击类型：备份渗透

1：减小受攻击面 2 3 4

您不确定哪些备份系统或客户受到了影响。您第一步应该做什么？

- ✗ 通知相关机构
- ✗ 关闭所有系统
- ✓ 尝试遏制并隔离威胁
- ✗ 确定您是否有干净备份可用于还原

立即遏制并隔离威胁可防止威胁进一步传播或造成损害，并赢得时间来评估事件范围，从而尽可能减少各种网络攻击（包括涉及 AI 的网络攻击）的影响。

下一问题 →

攻击类型：备份渗透

1 — 2：检测和响应网络威胁 — 3 — 4

您的首要任务是快速恢复客户数据。如何实现？

- [ ] 支付赎金
- [ ] 识别勒索软件变种
- [ ] 通知相关机构
- [ ] 确定哪些数据已泄露

查看正确答案 →

攻击类型：备份渗透

1 — 2：检测和响应网络威胁 — 3 — 4

您的首要任务是快速恢复客户数据。如何实现？

- ✗ 支付赎金
- ✗ 识别勒索软件变种
- ✗ 通知相关机构
- ✓ 确定哪些数据已泄露

识别受损数据有助于将恢复工作集中在还原最关键的客户信息上，确保加快数据恢复，并避免在未受影响的系统上执行不必要的工作。

下一问题 →

攻击类型：备份渗透

1 — 2 — 3：从网络攻击中恢复 — 4

您确定有一个备份可用于恢复。恢复流程的第一步应该是什么？

- [ ] 首先还原关键系统
- [ ] 使用取证分析确认攻击已完全得到遏制
- [ ] 更改所有密码并撤销泄露的凭据
- [ ] 实施零信任原则

查看正确答案 →

攻击类型：备份渗透

1 — 2 — 3：从网络攻击中恢复 — 4

您确定有一个备份可用于恢复。恢复流程的第一步应该是什么？

- ✗ 首先还原关键系统
- ✓ 使用取证分析确认攻击已完全得到遏制
- ✗ 更改所有密码并撤销泄露的凭据
- ✗ 实施零信任原则

在还原系统之前，您需要确保已完全遏制攻击，以防止意外再次感染和进一步损坏，避免环境中的威胁持续存在或升级。

下一问题 →

攻击类型：备份渗透

1 2 3 4：整体最佳实践

可通过哪些方法减轻未来发生这种情况的风险？

- [ ] 奉行零信任原则
- [ ] 启用端点检测和响应 (EDR) 功能
- [ ] 实施不可变的安全隔离备份
- [ ] 以上都是

查看正确答案 →

攻击类型：备份渗透

1 2 3 4：整体最佳实践

可通过哪些方法减轻未来发生这种情况的风险？

- [x] 奉行零信任原则
- [x] 启用端点检测和响应 (EDR) 功能
- [x] 实施不可变的安全隔离备份
- [x] 以上都是

使用多层防御战略可以降低风险、充分减少损害并增强组织弹性，因为任何单一措施都不足以独立应对威胁。

查看解决方案 →

攻击类型：备份渗透

回顾

备份渗透是指网络犯罪分子利用备份系统中的漏洞破坏、删除或加密关键恢复数据。这些复杂攻击可能与勒索软件或恶意软件部署等其他事件同时发生或紧随其后，从而加剧运营和财务影响。

我们坚信，戴尔能够帮助组织在面临不断变化的网络威胁时保持弹性。依托我们的前沿解决方案、专业服务和可靠的合作伙伴关系，我们始终致力于协助您守护所珍视的一切。

详细了解我们的解决方案，以及我们如何应对当今严峻的网络挑战。

浏览备份渗透简述 →

⌂ 返回到场景

PowerProtect 产品组合 ›

我们不可变的安全隔离加密备份存储区以 AI 驱动的 CyberSense 分析为支持，确保快速检测和恢复，助您保持弹性。

PowerEdge 服务器 ›

凭借安全启动、硬件信任根和系统锁定功能，戴尔提供值得信赖的基础架构，可妥善保护您的备份。

可信任的工作区 ›

通过 SafeBIOS 和 SafeData 保护措施降低风险，确保您的备份系统在需要时保持未被篡改且随时可用。

安全性和弹性服务 ›

从安全部署到主动事件响应，我们的专家和合作伙伴可帮助您构建弹性并加快恢复速度。

网络解决方案 ›

通过网络分段、多因素身份验证 (MFA) 和最低权限配置，戴尔可帮助您锁定访问并保护关键数据。

攻击类型：分布式拒绝服务 (DDoS)

这是一个周二的下午，在州政府机构，这天预报会有一场大雪。

多名坐席人员打电话到交通部的 IT 团队，称无法登录任何系统来完成以下工作：

- 换发驾照
- 获得道路许可证
- 纳税
- 检查路况
- 接入应急响应系统，这会延误道路人员清理积雪/结冰的道路

一切都是系统超时所致。

检验掌握情况 →

攻击类型：分布式拒绝服务 (DDoS)

1：减小受攻击面　2　3　4

首先应排查哪里出了问题?

- [ ] 检查网络设备是否存在不明原因的入站流量突然激增
- [ ] 检查网络设备是否有来自单个或有限数量 IP 地址的异常流量
- [ ] 检查防火墙或网络可见性工具日志中是否有过多的连接失败或流量阻止事件
- [ ] 以上都是

查看正确答案 →

攻击类型：分布式拒绝服务 (DDoS)

1：减小受攻击面 — 2 — 3 — 4

首先应排查哪里出了问题？

- [x] 检查网络设备是否存在不明原因的入站流量突然激增
- [x] 检查网络设备是否有来自单个或有限数量 IP 地址的异常流量
- [x] 检查防火墙或网络可见性工具日志中是否有过多的连接失败或流量阻止事件
- [x] 以上都是

为了准确诊断大规模系统中断，您需要同时审查网络设备活动和防火墙或可见性工具日志，以快速发现异常模式或阻止事件。这样可以更快、更准确地响应事件，因为您可以区分网络事件和基础架构问题。

下一问题 →

攻击类型：分布式拒绝服务 (DDoS)

1 — 2：检测和响应网络威胁 — 3 — 4

您怀疑这可能是 DDoS 攻击。第一步是什么？

- [ ] 通过 DDoS 缓解服务重定向所有网络流量
- [ ] 激活 Web 应用程序防火墙 (WAF) 规则以筛选出恶意模式
- [ ] 检查流量激增是否由于合法来源所致
- [ ] 在内部和外部沟通当前情况

查看正确答案 →

攻击类型：分布式拒绝服务 (DDoS)

1 — 2：检测和响应网络威胁 — 3 — 4

您怀疑这可能是 DDoS 攻击。第一步是什么？

- ✗ 通过 DDoS 缓解服务重定向所有网络流量
- ✗ 激活 Web 应用程序防火墙 (WAF) 规则以筛选出恶意模式
- ✓ 检查流量激增是否由于合法来源所致
- ✗ 在内部和外部沟通当前情况

在激活 DDoS 对策之前，必须验证流量高峰的合法性。这样就能避免意外阻止真正用户，防止对关键利益相关者造成干扰，并确保任何进一步的保护措施适当合理并有的放矢，从而尽可能减少对公共运营和整体业务连续性的负面影响。

下一问题 →

攻击类型：分布式拒绝服务 (DDoS)

1 2 3：从网络攻击中恢复 4

您可以采取哪些步骤来避免将来发生 DDoS 攻击？

- [ ] 阻止有问题的 IP 地址
- [ ] 使用 DDoS 模拟执行定期渗透测试
- [ ] 将所有应用程序迁移到云，因为云提供商通常不会受到 DDoS 攻击
- [ ] 实施零信任原则

查看正确答案 →

攻击类型：分布式拒绝服务 (DDoS)

1 2 3：从网络攻击中恢复 4

您可以采取哪些步骤来避免将来发生 DDoS 攻击？

- ✗ 阻止有问题的 IP 地址
- ✓ 使用 DDoS 模拟执行定期渗透测试
- ✗ 将所有应用程序迁移到云，因为云提供商通常不会受到 DDoS 攻击
- ✓ 实施零信任原则

结合 DDoS 模拟的主动渗透测试可识别并强化防御漏洞，而零信任原则侧重于始终强制实施最小权限访问，从而尽可能降低风险。这有助于降低基本系统（例如应急响应协调或实时交通信号控制）中断的风险，即使在攻击期间，这些系统也必须保持正常工作。

下一问题 →

攻击类型：分布式拒绝服务 (DDoS)

1 2 3 4：整体最佳实践

作为整体事件响应和恢复计划 (IRR) 的一部分，您应该通知谁？

- [ ] 您的法律团队
- [ ] 您的网络保险供应商
- [ ] CISA（网络安全和基础架构安全局）、FBI、MS-ISAC（多国信息共享和分析中心）
- [ ] 以上都是

查看正确答案 →

攻击类型：分布式拒绝服务 (DDoS)

1 2 3 4：整体最佳实践

作为整体事件响应和恢复计划 (IRR) 的一部分，您应该通知谁？

- [x] 您的法律团队
- [x] 您的网络保险供应商
- [x] CISA（网络安全和基础架构安全局）、FBI、MS-ISAC（多国信息共享和分析中心）
- [x] 以上都是

在大规模网络事件中，考虑与法律、保险和政府机构就合规性、索赔和执法进行协调。满足所有法规要求后，您的组织就可以有效地遏制和解决风险事件并从中恢复。

查看解决方案 →

攻击类型：分布式拒绝服务 (DDOS)

回顾

DDoS 攻击旨在通过来自多个来源的大量流量来破坏网络、服务或服务器的正常运行。这些攻击通过利用僵尸网络实施，即由攻击者远程控制受感染设备组成的网络。

戴尔通过将高级检测和缓解技术与专家服务和零信任方法相结合，确保快速响应、尽可能减少中断并加强防御，从而帮助组织保持弹性，抵御 DDoS 攻击。

详细了解高级网络弹性战略，以及戴尔如何帮助您保护组织免受 DDoS 攻击。

浏览 DDoS 简述 →

返回到场景

网络解决方案 >

通过启用网络分段、微分段和最小权限强制实施，可以隔离关键资产、限制攻击传播，并确保快速遏制 DDoS 攻击。

PowerEdge 服务器 >

凭借硬件信任根、安全启动、系统锁定和实时篡改证据，戴尔可提供弹性十足且高性能的 DDoS 防护并加速恢复。

受信任的设备 >

集成的 SafeBIOS、SecureData 以及自动化检测和响应可将端点的受攻击面减少达 70%，从而防止 DDoS 干扰成为漏洞载体。

PowerProtect 产品组合 >

不可变的安全隔离加密备份环境以 AI 驱动的威胁分析为支持，可确保快速进行经验证的还原，并在 DDoS 中断期间保持业务连续性。

安全性和弹性服务 >

Managed Detection and Response (MDR)、事件响应和恢复 (IRR)、威胁搜寻和弹性体系结构指导可增强 DDoS 防范准备并提升防御能力。

攻击类型：恶意内部攻击

这是星期二早上 8 点。一家美国医疗公司的员工刚刚开始一天的工作。

一名处理高度敏感患者数据的高级员工在办公室工作至深夜后登录了系统。

她注意到自己在前一晚使用的文件夹发生了变化。与团队讨论后，她向 IT 部门提出疑问。

调查后，他们发现一名与犯罪集团有关联的初级 IT 员工欺骗一名高级员工将 USB Rubber Ducky 插入设备，导致基本输入/输出系统 (BIOS) 降级到易受攻击的版本，对系统造成风险。

检验掌握情况 →

攻击类型：恶意内部攻击

1：减小受攻击面　2　3　4　5

这名恶意内部人员使用两种方法发起了此次攻击，这两种方法均被 MITRE ATT&CK（MITRE 对抗策略、技术与常识）框架跟踪。它们是什么？

- [ ] 信任关系 + 通过可移动介质进行复制
- [ ] 社会工程 + 通过可移动介质进行复制
- [ ] 社会工程 + 外部远程服务
- [ ] 信任关系 + 硬件添加

查看正确答案 →

攻击类型：恶意内部攻击

1：减小受攻击面　2　3　4　5

这名恶意内部人员使用两种方法发起了此次攻击，这两种方法均被 MITRE ATT&CK（MITRE 对抗策略、技术与常识）框架跟踪。它们是什么？

- ✗ 信任关系 + 通过可移动介质进行复制
- ✓ 社会工程 + 通过可移动介质进行复制
- ✗ 社会工程 + 外部远程服务
- ✗ 信任关系 + 硬件添加

根据 MITRE ATT&CK 框架中通过便携式存储进行人工操纵和复制的技术，该攻击者利用社会工程欺骗高级员工连接 USB Rubber Ducky，通过可移动介质传输受损数据。

下一问题 →

攻击类型：恶意内部攻击

1 — 2：检测和响应网络威胁 — 3 — 4 — 5

攻击者为什么需要使用这两种方法？

- [ ] 以全局管理员身份进入网络以降级基本输入/输出系统 (BIOS)
- [ ] 对管理员进行网络钓鱼，以便能降级 BIOS
- [ ] 更改设备的域名系统 (DNS) 提供程序以获取一次性网络访问所需的凭据
- [ ] 在设备上安装恶意软件，以获取持续访问网络所需的凭据

查看正确答案 →

攻击类型：恶意内部攻击

1 — 2：检测和响应网络威胁 — 3 — 4 — 5

攻击者为什么需要使用这两种方法？

- ✗ 以全局管理员身份进入网络以降级基本输入/输出系统 (BIOS)
- ✗ 对管理员进行网络钓鱼，以便能降级 BIOS
- ✗ 更改设备的域名系统 (DNS) 提供程序以获取一次性网络访问所需的凭据
- ✓ 在设备上安装恶意软件，以获取持续访问网络所需的凭据

攻击者需要通过这两种方法（通过 USB Rubber Ducky 安装恶意软件来破坏设备和凭据以实现持续的网络访问），建立对目标环境的持久、未经授权的控制。

下一问题 →

攻击类型：恶意内部攻击

1 2 3：检测和响应网络威胁 4 5

检测不规则网络活动的一种方法是什么？

- [ ] 应用程序控制
- [ ] 扩展检测和响应 (XDR)
- [ ] 下一代防病毒软件 (NGAV)
- [ ] 端点地理围栏

查看正确答案 →

攻击类型：恶意内部攻击

1 2 3：检测和响应网络威胁 4 5

检测不规则网络活动的一种方法是什么？

- ✗ 应用程序控制
- ✓ 扩展检测和响应 (XDR)
- ✗ 下一代防病毒软件 (NGAV)
- ✗ 端点地理围栏

在提供广泛、关联的可见性以快速检测威胁方面，XDR 非常适合于检测可疑网络活动，因为它可以持续监控和分析端点、网络与云环境中的活动。

下一问题 →

攻击类型：恶意内部攻击

1 2 3 4：从网络攻击中恢复 5

哪些内置 PC 安全功能可以在杀伤链中及早检测到可疑活动？

- [ ] 安全信息和事件管理 (SIEM)
- [ ] 扩展检测和响应 (XDR)
- [ ] 攻击指标 (IOA)
- [ ] 基于角色的访问控制 (RBAC)

查看正确答案 →

攻击类型：恶意内部攻击

1 2 3 4：从网络攻击中恢复 5

哪些内置 PC 安全功能可以在杀伤链中及早检测到可疑活动？

- ✗ 安全信息和事件管理 (SIEM)
- ✗ 扩展检测和响应 (XDR)
- ✓ 攻击指标 (IOA)
- ✗ 基于角色的访问控制 (RBAC)

IOA 专注于检测正在发生的攻击者行为和可疑活动模式，使安全团队能够比签名方法更早地识别威胁，并在造成重大损失之前进行干预。

下一问题 →

攻击类型：恶意内部攻击

1 2 3 4 5：整体最佳实践

确定初始访问方法后，应采取什么措施从漏洞中恢复，并防止未来出现类似漏洞？

- [ ] 将 BIOS 更新至最新版本
- [ ] 禁用 BIOS 降级选项
- [ ] 禁用 USB 端口
- [ ] 实施精细控制，既保障 USB 设备的安全使用，又能防止恶意软件的传播
- [ ] 以上都是

查看正确答案 →

攻击类型：恶意内部攻击

1 2 3 4 5：整体最佳实践

确定初始访问方法后，应采取什么措施从漏洞中恢复，并防止未来出现类似漏洞？

- [x] 将 BIOS 更新至最新版本
- [x] 禁用 BIOS 降级选项
- [x] 禁用 USB 端口
- [x] 实施精细控制，既保障 USB 设备的安全使用，又能防止恶意软件的传播
- [x] 以上都是

通过解决不同的攻击载体以确保硬件安全并阻止降级，可以遏制基于 USB 的威胁，并在多个点上阻止恶意软件传播，从而帮助建立全面的分层防御体系，以恢复受影响的系统并防范未来漏洞。

查看解决方案 →

攻击类型：恶意内部攻击

回顾

恶意内部攻击指组织内部人员滥用访问权限，为达成个人、经济或竞争目的而破坏数据、干扰运营或窃取敏感信息的行为。该人员可以是员工、承包商、合作伙伴或任何有权合法访问公司系统和网络的人员。

戴尔将先进技术与严格的安全协议相结合，有效防范恶意内部网络攻击。

详细了解高级网络弹性战略，以及戴尔如何帮助您保护组织免遭恶意内部攻击。

浏览恶意内部攻击简述 →

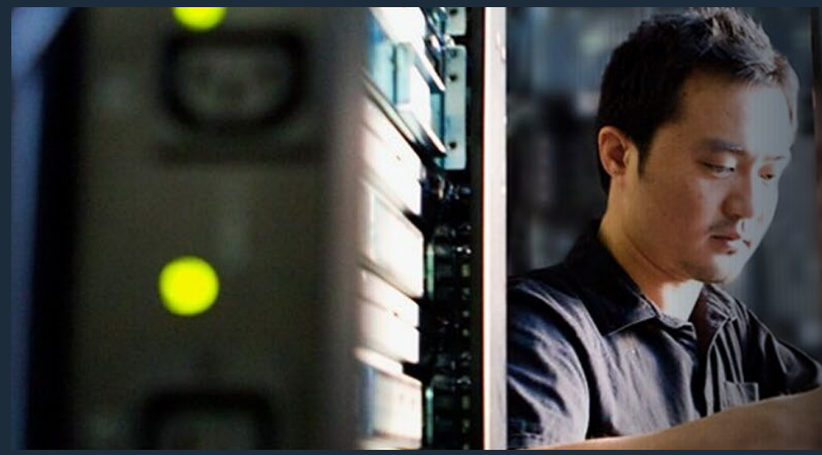
⌂ 返回到场景

受信任设备和基础架构 ›

内置最小权限、多因素身份验证 (MFA)、基于角色的访问控制 (RBAC)、双重身份验证和零信任保护可确保端点和基础架构的安全，降低内部威胁的风险。

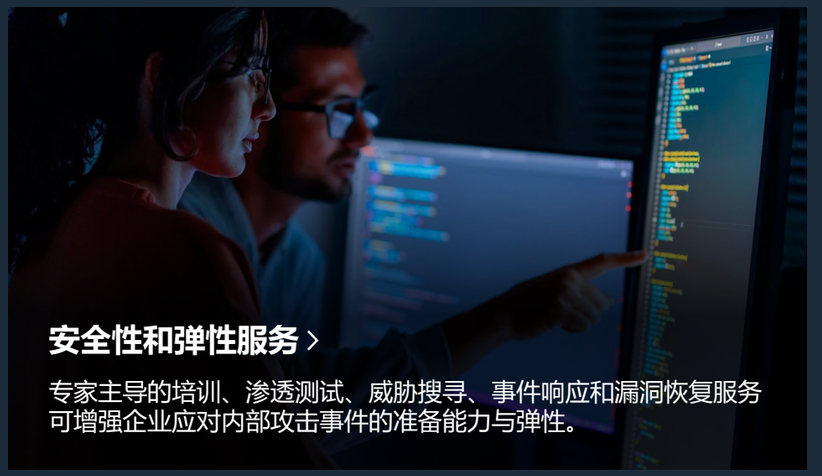
PowerEdge 服务器 ›

硬件信任根、安全启动、动态 USB 端口管理和系统锁定可防止篡改，并阻止物理或基于固件的内部攻击。



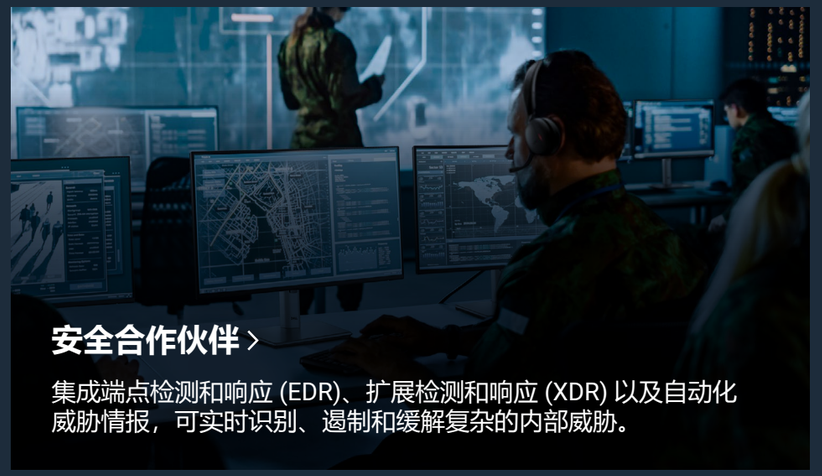
PowerProtect 产品组合 ›

不可修改的隔离备份可确保数据完整性、快速还原并及早检测数据操纵尝试，有助于从内部攻击事件中恢复。



安全性和弹性服务 ›

专家主导的培训、渗透测试、威胁搜寻、事件响应和漏洞恢复服务可增强企业应对内部攻击事件的准备能力与弹性。



安全合作伙伴 ›

集成端点检测和响应 (EDR)、扩展检测和响应 (XDR) 以及自动化威胁情报，可实时识别、遏制和缓解复杂的内部威胁。

攻击类型：中间人攻击 (MITM)

一位毫无戒备心的客户在咖啡店连接到不安全的免费 Wi-Fi，对共享团队文档进行最后的更新。

片刻之后，客户公司的 IT 部门就收到了通知，表明来自员工帐户的异常登录尝试，以及来自全球多个位置的未经授权的数据访问。

调查后，他们确认攻击者已截获并操纵无线连接，并访问了敏感信息。

检验掌握情况 →

攻击类型：中间人攻击 (MITM)

1：减小受攻击面　2　3　4

在检测到异常登录尝试后，IT 团队应首先调查哪里？

- [ ] 防火墙、入侵检测系统 (IDS)、入侵防御系统 (IPS) 日志和扩展检测响应 (XDR)
- [ ] 受影响员工的笔记本电脑
- [ ] 咖啡店不安全的 Wi-Fi 上的网络流量
- [ ] 公司系统中的身份验证日志

查看正确答案 →

攻击类型：中间人攻击 (MITM)

1：减小受攻击面 2 3 4

在检测到异常登录尝试后，IT 团队应首先调查哪里？

- ✓ 防火墙、入侵检测系统 (IDS)、入侵防御系统 (IPS) 日志和扩展检测响应 (XDR)
- ✗ 受影响员工的笔记本电脑
- ✗ 咖啡店不安全的 Wi-Fi 上的网络流量
- ✓ 公司系统中的身份验证日志

通过分析这些防火墙以及 IDS/IPS 和身份验证日志，IT 团队可以跟踪未经授权的访问尝试、评估被入侵的帐户，并更好地了解事件的范围。

下一问题 →

攻击类型：中间人攻击 (MITM)

1 — 2：检测和响应网络威胁 — 3 — 4

在确认 MITM 攻击后，IT 团队应立即采取什么行动？

- [ ] 立即断开受影响员工的设备与网络的连接，并将设备隔离以进行分析
- [ ] 更新防火墙规则和网络配置以阻止进一步未经授权的访问
- [ ] 重置所有员工帐户的密码
- [ ] 禁用受影响的系统以防止数据外泄

查看正确答案 →

攻击类型：中间人攻击 (MITM)

1 — 2：检测和响应网络威胁 — 3 — 4

在确认 MITM 攻击后，IT 团队应立即采取什么行动？

- ✓ 立即断开受影响员工的设备与网络的连接，并将设备隔离以进行分析
- ✓ 更新防火墙规则和网络配置以阻止进一步未经授权的访问
- ✗ 重置所有员工帐户的密码
- ✗ 禁用受影响的系统以防止数据外泄

立即断开并隔离受影响的设备可阻止攻击者访问，保留取证证据；而更新防火墙和网络规则可阻止进一步的恶意连接，保护更广泛的网络免受持续入侵。

下一问题 →

攻击类型：中间人攻击 (MITM)

1 2 3：从网络攻击中恢复 4

哪些预防措施可以降低易受 MITM 攻击的漏洞?

- [ ] 强制所有员工使用虚拟专用网 (VPN)
- [ ] 实施零信任安全原则，如多因素身份验证 (MFA)
- [ ] 避免连接公共 Wi-Fi
- [ ] 对通过电子邮件共享的敏感文件进行加密

查看正确答案 →

攻击类型：中间人攻击 (MITM)

1 — 2 — 3：从网络攻击中恢复 — 4

哪些预防措施可以降低易受 MITM 攻击的漏洞?

- ✓ 强制所有员工使用虚拟专用网 (VPN)
- ✓ 实施零信任安全原则，如多因素身份验证 (MFA)
- ✗ 避免连接公共 Wi-Fi
- ✗ 对通过电子邮件共享的敏感文件进行加密

在不安全的网络上强制使用 VPN 可加密员工互联网流量以防止被拦截；而实施零信任安全性和 MFA 可确保每个访问请求持续得到验证。

下一问题 →

攻击类型：中间人攻击 (MITM)

1 2 3 4：整体最佳实践

解决漏洞后，您的组织应该实施哪些长期战略？

- [ ] 定期审核和修补系统
- [ ] 通过增加网络分段，隔离敏感数据和系统
- [ ] 部署端点检测和响应 (EDR) 以及 Managed Detection and Response (MDR) 解决方案
- [ ] 对员工定期进行强效培训
- [ ] 以上都是

查看正确答案 →

攻击类型：中间人攻击 (MITM)

1 2 3 4：整体最佳实践

解决漏洞后，您的组织应该实施哪些长期战略？

- [x] 定期审核和修补系统
- [x] 通过增加网络分段，隔离敏感数据和系统
- [x] 部署端点检测和响应 (EDR) 以及 Managed Detection and Response (MDR) 解决方案
- [x] 对员工定期进行强效培训
- [x] 以上都是

为了防范不同威胁，这些长期战略相互结合，共同构建全面、弹性的安全态势，阻止攻击者利用漏洞，并确保快速有效地应对漏洞。

查看解决方案 →

攻击类型：中间人攻击 (MITM)

回顾

MITM 攻击是指网络犯罪分子秘密拦截两方通信的行为，例如截获员工与公司服务器之间或客户与企业网站之间的数据传输。攻击者的目标可能有所不同，但结果相同：破坏信任和安全性。

戴尔提供创新、可扩展的安全解决方案，助力组织通过所需的工具和专业知识检测和响应风险并充满信心地恢复，从而抵御 MITM 威胁、保护资产并保持业务完整性。

详细了解高级网络弹性战略，以及戴尔如何帮助您保护组织免受 MITM 攻击。

阅读 MITM 攻击简述 →

返回到场景

受信任的设备 ›

凭借硬件身份验证、SafeBIOS 和 SafeID 等固件保护、强大的加密功能和零信任框架，戴尔可妥善保护端点和传输中的数据。

PowerEdge 服务器 ›

安全启动、芯片级信任根、动态 USB 端口管理和系统锁定可确保硬件完整性，并保护关键工作负载免受网络威胁。

存储解决方案 ›

静态和传输中的加密数据与隔离快照和快速恢复功能相结合，可确保文件保持安全，并可在遭受 MITM 攻击后快速还原。

PowerProtect 产品组合 ›

不可修改的隔离备份和 AI 驱动的 CyberSense 分析可在发生 MITM 攻击时实现快速恢复和可信数据还原。

安全性和弹性服务 ›

从漏洞评估和用户培训到渗透测试和事件响应，戴尔专家与合作伙伴可全面支持您增强防御能力。

攻击类型：提示/SQL 注入攻击

您在一家航空公司的客服部门工作，该公司主要通过聊天机器人提供服务。

您开始注意到，您和您的同事接到大量客户来电，表示他们无法进入其常飞旅客帐户，而当他们进入帐户时，发现所有常飞旅客里程不翼而飞。

检验掌握情况 →

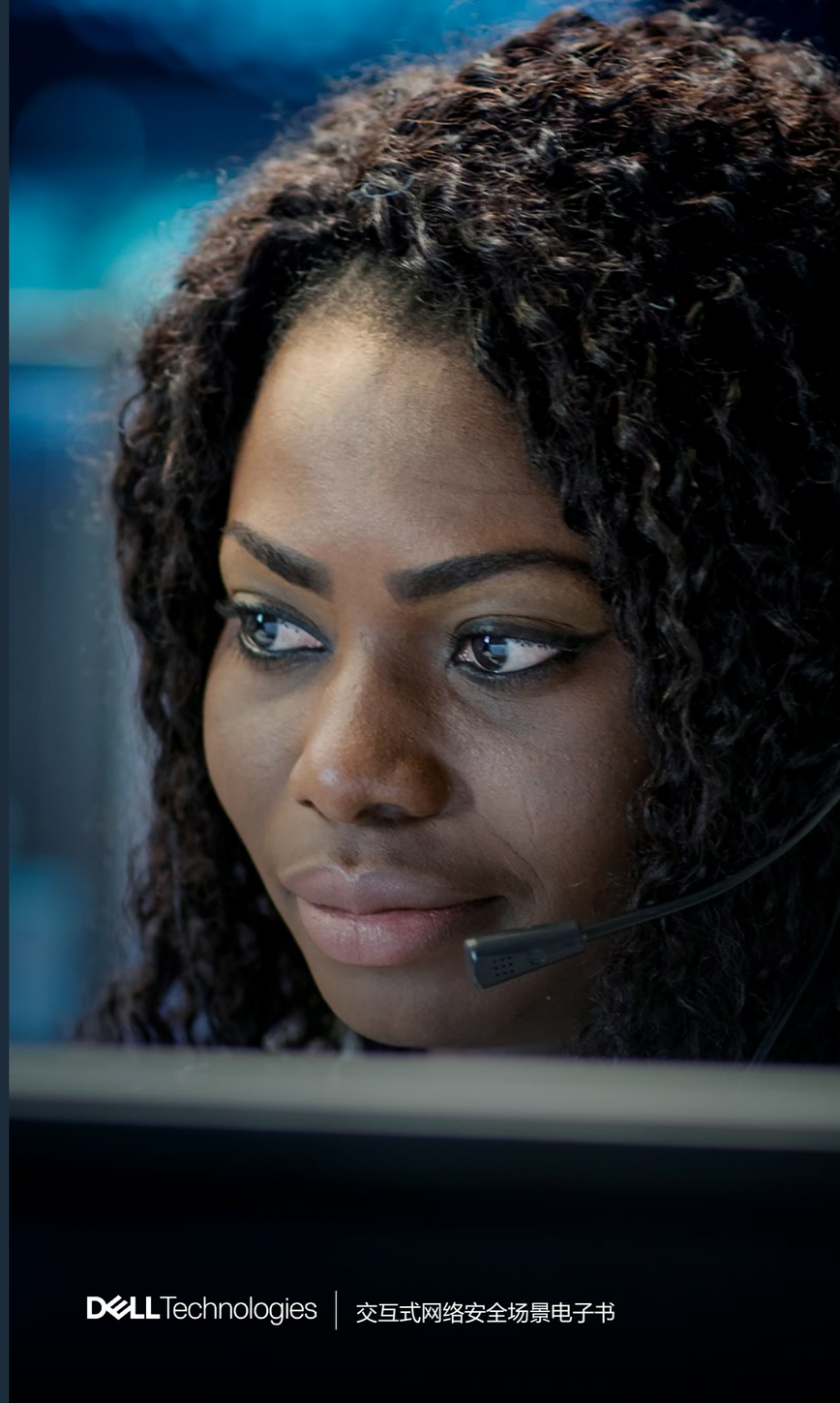
攻击类型：提示/SQL 注入攻击

1：减小受攻击面　2　3　4

在调查后，您在日志中看到一些错误，包括*结构化查询语言 (SQL) 语句中的语法错误或无效列名 “admin”*。这是哪种类型的网络事件？

- [ ] 凭据被盗
- [ ] 提示或 SQL 注入攻击
- [ ] 中间人攻击
- [ ] 网络钓鱼

查看正确答案 →



攻击类型：提示/SQL 注入攻击

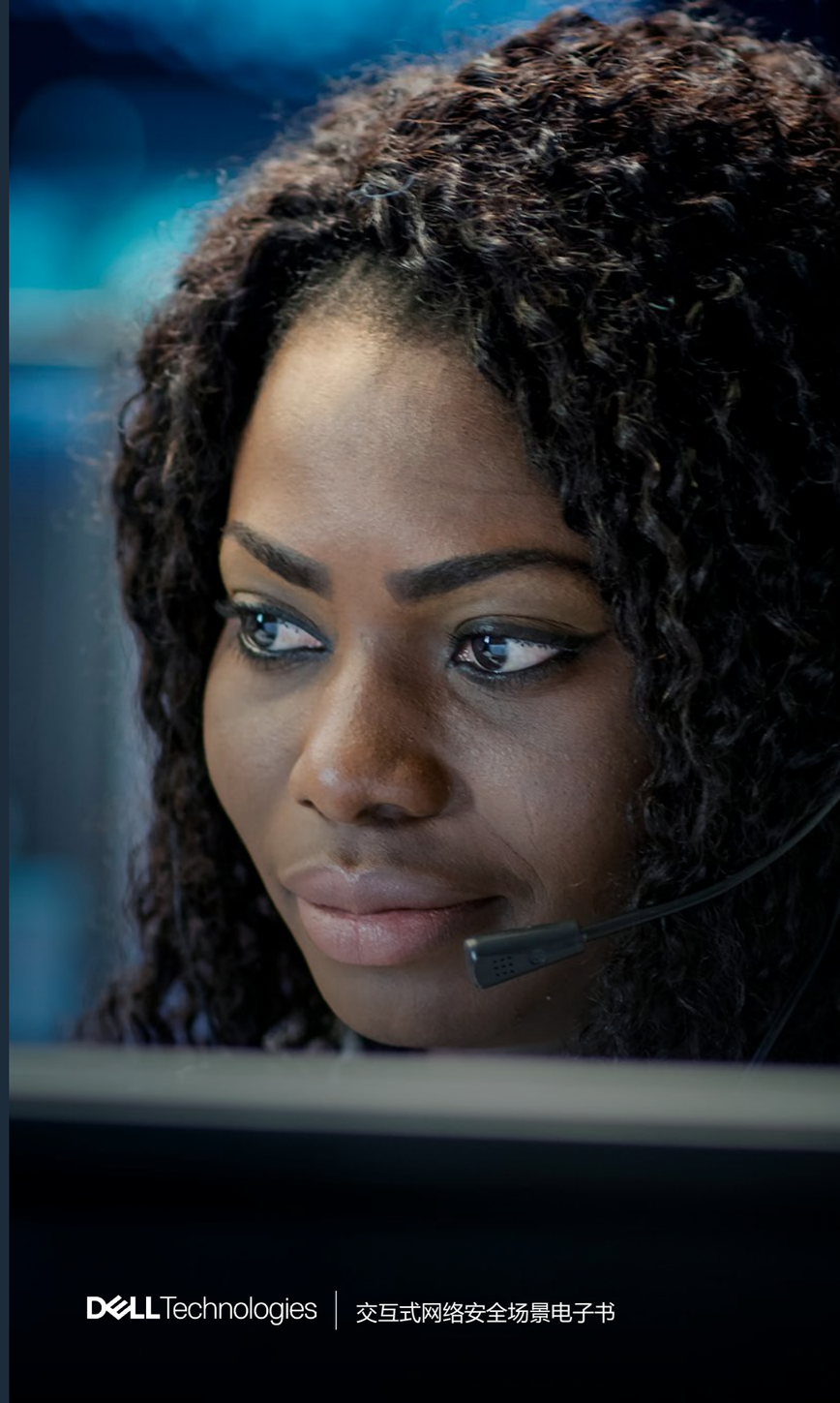
1：减小受攻击面 2 3 4

在调查后，您在日志中看到一些错误，包括*结构化查询语言 (SQL) 语句中的语法错误*或*无效列名 "admin"*。这是哪种类型的网络事件？

- ✗ 凭据被盗
- ✓ 提示或 SQL 注入攻击
- ✗ 中间人攻击
- ✗ 网络钓鱼

"提示或 SQL 注入攻击"正确，因为"SQL 语句中的语法错误"或"无效列名'admin'"等日志错误表明，攻击者使用恶意 SQL 代码利用聊天机器人的输入字段访问或更改客户帐户数据，这是 SQL 注入攻击的明显技术指标，与所述可疑活动相符。

下一问题 →



攻击类型：提示/SQL 注入攻击

1 — 2：检测和响应网络威胁 — 3 — 4

您意识到您的客服聊天机器人遭受到提示/SQL 注入攻击。您应该怎么做？

- [ ] 使机器人离线
- [ ] 调查数据库日志中是否有未经授权的访问以及被盗、修改或删除的数据
- [ ] 遵守所有数据泄露披露法
- [ ] 以上都是

查看正确答案 →

攻击类型：提示/SQL 注入攻击

1 — 2：检测和响应网络威胁 — 3 — 4

您意识到您的客服聊天机器人遭受到提示/SQL 注入攻击。您应该怎么做？

- [x] 使机器人离线
- [x] 调查数据库日志中是否有未经授权的访问以及被盗、修改或删除的数据
- [x] 遵守所有数据泄露披露法
- [x] 以上都是

要应对提示/SQL 注入攻击，需要使聊天机器人离线、调查数据库日志中是否存在未经授权的访问，并确保遵守信息披露法。这些步骤对于停止漏洞利用、评估损害以及履行监管和道德义务至关重要。

下一问题 →

攻击类型：提示/SQL 注入攻击

1 2 3：从网络攻击中恢复 4

您应该设置哪些功能来帮助停止提示/SQL 注入攻击？

- [ ] 指导开发团队使用准备好的语句和参数化查询作为编码实践
- [ ] Managed Detection and Response (MDR) 工具
- [ ] 实施最小权限访问，例如多因素身份验证 (MFA)、基于角色的访问控制 (RBAC)、Web 应用程序防火墙 (WAF) 等
- [ ] 细分后端数据库/知识库

查看正确答案 →

攻击类型：提示/SQL 注入攻击

1 — 2 — 3：从网络攻击中恢复 — 4

您应该设置哪些功能来帮助停止提示/SQL 注入攻击？

- ✓ 指导开发团队使用准备好的语句和参数化查询作为编码实践
- ✗ Managed Detection and Response (MDR) 工具
- ✓ 实施最小权限访问，例如多因素身份验证 (MFA)、基于角色的访问控制 (RBAC)、Web 应用程序防火墙 (WAF) 等
- ✗ 细分后端数据库/知识库

培训开发团队使用准备好的语句和参数化查询，这可在源头阻止 SQL 注入攻击，而强制实施最小权限访问控制（如 MFA、RBAC 和 WAF）可防止攻击者升级权限或横向移动，从而限制任何注入尝试的影响。

下一问题 →

攻击类型：提示/SQL 注入攻击

1 2 3 4：整体最佳实践

您会采取哪些步骤来恢复航空公司的客户数据？

- [ ] 跟踪被盗数据
- [ ] 请客户重建其配置文件
- [ ] 向网络攻击者赎回
- [ ] 通过未受影响的最新备份还原常飞旅客里程，通知客户更改密码并检查信用卡

查看正确答案 →

攻击类型：提示/SQL 注入攻击

1 2 3 4：整体最佳实践

您会采取哪些步骤来恢复航空公司的客户数据？

- ✗ 跟踪被盗数据
- ✗ 请客户重建其配置文件
- ✗ 向网络攻击者赎回
- ✓ 通过未受影响的最新备份还原常飞旅客里程，通知客户更改密码并检查信用卡

从未受损的最新备份恢复丢失的帐户数据有助于维护数据完整性并减少停机时间。在发生破坏性注入攻击后，及时通知客户重置密码并监控信用卡活动，进一步满足监管合规要求。

查看解决方案 →

攻击类型：提示/SQL 注入攻击

回顾

提示注入和 SQL 注入攻击已被反复证明是网络犯罪分子使用的极具破坏性和普遍性的网络攻击手段。这些攻击利用了用户查询或数据库系统中的漏洞，使恶意攻击者能够操纵服务器、窃取数据或中断工作流。

戴尔持续致力于网络安全，从中聚焦于保护您的组织免受不断变化的提示/SQL 注入威胁和攻击，我们提供检测、响应和恢复所需的工具和专业知识。

了解高级网络弹性战略，以及戴尔如何帮助您的组织抵御提示和 SQL 注入攻击。

浏览提示/SQL 注入攻击简述 →

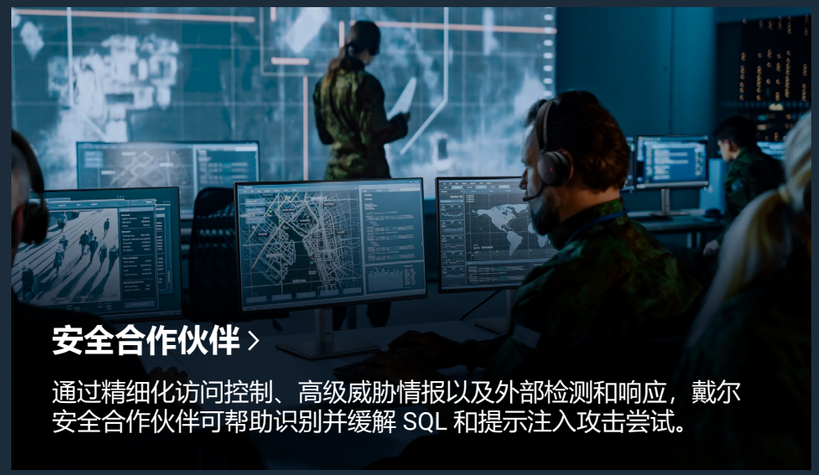
返回到场景

可信工作区和可信基础架构 ›

保护端点，并降低泄露凭据被注入攻击利用的风险。

PowerEdge 服务器 ›

凭借硬件信任根、安全启动、基于芯片的安全性和实时配置验证，Dell PowerEdge 服务器可确保基础架构防篡改，仅运行可信代码。



安全合作伙伴 ›

通过精细化访问控制、高级威胁情报以及外部检测和响应，戴尔安全合作伙伴可帮助识别并缓解 SQL 和提示注入攻击尝试。

PowerProtect 产品组合 ›

戴尔不可修改的安全隔离备份和高级网络恢复分析提供可信任的还原点，能够从数据损坏或外泄情况下快速恢复。

安全性和弹性服务 ›

从安全开发培训和渗透测试到威胁搜寻和事件响应，戴尔专家与合作伙伴可帮助验证保护措施并快速修复注入攻击。

攻击类型：勒索软件

您是一家地区医院的 IT 专业人员，该医院以互联医疗系统闻名，包括电子健康档案 (EHR)、智能输液泵和放射影像系统，所有这些都连接到一个集中式网络。

昨晚，多个系统同时开始崩溃。到了早上，临床工作人员报告称无法访问患者记录。

多个终端上出现了以下勒索信息：

“你的文件已被加密。在 72 小时内支付 20 枚比特币，否则患者数据将被公开。”

检验掌握情况 →

攻击类型：勒索软件

1：减小受攻击面　2　3　4

咨询台收到 100 多份关于文件加密和应用程序错误的报告。安全日志显示来自内部域账户的异常文件重命名活动。第一步是什么？

- [ ] 立即支付赎金以还原关键服务
- [ ] 通知执法人员和法律顾问
- [ ] 开始重新映像所有受影响的端点
- [ ] 断开受感染系统与网络的连接

查看正确答案 →

攻击类型：勒索软件

1：减小受攻击面 2 3 4

咨询台收到 100 多份关于文件加密和应用程序错误的报告。安全日志显示来自内部域账户的异常文件重命名活动。第一步是什么？

- ✗ 立即支付赎金以还原关键服务
- ✗ 通知执法人员和法律顾问
- ✗ 开始重新映像所有受影响的端点
- ✓ 断开受感染系统与网络的连接

立即断开和隔离受感染的医院系统可阻止勒索软件蔓延、保护关键医疗设备和敏感患者数据、保留证据以供调查，并为协调响应和恢复争取重要时间。

下一问题 →

攻击类型：勒索软件

1 — 2：检测和响应网络威胁 — 3 — 4

事件响应团队发现，攻击很可能始于一个被入侵的帐户，该帐户曾被用来访问一台未启用多因素身份验证 (MFA) 的服务器。以下哪一项最直接导致了此次攻击？

- [ ] 过时的防病毒定义
- [ ] 电子健康记录 (EHR) 数据库泄露
- [ ] 远程访问缺少 MFA
- [ ] 薄弱的电子邮件筛选功能

查看正确答案 →

攻击类型：勒索软件

1 — 2：检测和响应网络威胁 — 3 — 4

事件响应团队发现，攻击很可能始于一个被入侵的帐户，该帐户曾被用来访问一台未启用多因素身份验证 (MFA) 的服务器。以下哪一项最直接导致了此次攻击？

- ✗ 过时的防病毒定义
- ✗ 电子健康记录 (EHR) 数据库泄露
- ✓ 远程访问缺少 MFA
- ✗ 薄弱的电子邮件筛选功能

远程访问缺少 MFA 导致服务器被入侵，攻击者能够使用被盗或猜测的凭据登录，而无需经过额外的验证步骤。使用 MFA 时，即使是被入侵的帐户也需要第二道验证因素，从而显著降低未经授权访问的风险。

下一问题 →

攻击类型：勒索软件

1 2 3：从网络攻击中恢复 4

医务人员现在依赖纸质工作流。今天安排手术的患者无法在系统中得到验证。支持医院运营的最佳短期行动是什么？

- [ ] 重新启动核心数据库服务器以尝试重新初始化
- [ ] 启用所有旧备份，即使它们是 6 个月前的数据
- [ ] 启动医院的手动停机程序并上报给应急响应团队
- [ ] 让员工根据具体情况自行决定如何处理

查看正确答案 →

攻击类型：勒索软件

1 2 3：从网络攻击中恢复 4

医务人员现在依赖纸质工作流。今天安排手术的患者无法在系统中得到验证。支持医院运营的最佳短期行动是什么？

- ✗ 重新启动核心数据库服务器以尝试重新初始化
- ✗ 启用所有旧备份，即使它们是 6 个月前的数据
- ✓ 启动医院的手动停机程序并上报给应急响应团队
- ✗ 让员工根据具体情况自行决定如何处理

激活手动停机程序并上报给紧急响应团队，以确保关键临床工作流的即时连续性、保障患者安全，并建立用于验证和记录护理的标准化流程。这种方法可充分减少错误、高效管理风险和资源，并支持专业人员安全地还原数字系统。

下一问题 →

攻击类型：勒索软件

1 2 3 4：整体最佳实践

当地媒体已经报道了此事。领导层想知道是否应该发布公开声明，而法律部门则在询问《健康保险流通与责任法案》(HIPAA) 中规定了哪些义务。最合适的下一步是什么？

- [ ] 在获得更多信息之前，公开否认该事件
- [ ] 发布新闻稿，指责第三方 IT 供应商
- [ ] 通知监管机构并启动内部数据泄露通知程序
- [ ] 立即支付赎金并避免公众关注

查看正确答案 →

攻击类型：勒索软件

1 2 3 4：整体最佳实践

当地媒体已经报道了此事。领导层想知道是否应该发布公开声明，而法律部门则在询问《健康保险流通与责任法案》(HIPAA) 中规定了哪些义务。最合适的下一步是什么？

- ✗ 在获得更多信息之前，公开否认该事件
- ✗ 发布新闻稿，指责第三方 IT 供应商
- ✓ 通知监管机构并启动内部数据泄露通知程序
- ✗ 立即支付赎金并避免公众关注

根据 HIPAA 和州法律的要求，及时向当局和受影响的个人报告违反受保护健康信息的行为，以确保监管合规性、法律保护和最佳实践透明度，从而防止法律和声誉损害、履行强制性披露义务，并与患者、员工和利益相关者建立适当的沟通。

查看解决方案 →

攻击类型：勒索软件

回顾

勒索软件是一种恶意软件，它阻止用户访问计算机系统或数据，并要求支付赎金后才能恢复。它是最具破坏性的网络攻击类型之一。全球有 50% 的企业在过去一年中至少遭受过一次勒索软件攻击，勒索软件攻击后的平均停机时间为三周，这会导致严重的运营中断。

戴尔优先考虑采用零信任框架、端点保护和网络分段阻止勒索软件入侵并限制其传播，为您的组织保驾护航。通过专家主导的事件响应计划，我们可帮助您保持弹性并快速从攻击中恢复。

详细了解高级网络弹性战略，以及戴尔如何帮助您保护组织免遭勒索软件攻击。

浏览勒索软件攻击简述 →

⌂ 返回到场景

可信任的基础架构 ›

通过硬件身份验证、多因素身份验证 (MFA)、基于角色的访问控制 (RBAC) 和零信任框架，在基础架构级别阻止勒索软件。

网络和 PowerEdge 服务器 ›

限制勒索软件的移动。具有网络分段、安全启动、芯片级信任根、动态 USB 端口管理和系统锁定功能。

可信任的工作区 ›

集成 SafeBIOS、SafeID、SafeData 以及端点检测和响应 (EDR) 工具，可在设备级别提供主动式威胁情报、实时检测和自动化恶意软件遏制。

PowerProtect 产品组合 ›

通过不可修改的安全隔离备份、智能网络恢复分析和快速还原功能来保护关键数据，以防止勒索并实现弹性。

安全性和弹性服务 ›

与 CrowdStrike 等公司的专家合作，提供评估、漏洞管理、安全意识培训、渗透测试和事件响应等服务。

攻击类型：供应链硬件

您的公司要在全球的办事处部署 500 台新的笔记本电脑。为了加快进程，您将映像和硬件准备工作外包给了第三方 IT 物流供应商。他们将预配置的计算机直接运送给员工。

短短几天内，您就接到了来自现场的多个电话，内容如下：

- 多因素身份验证 (MFA) 请求被绕过，无法正常工作。
- 安全团队发现在非工作时段多次出现未经授权的管理员登录事件。
- 他们还看到本应处于离线状态的用户产生了虚拟专用网络 (VPN) 流量。

检验掌握情况 →

攻击类型：供应链硬件

1：减小受攻击面　2　3　4

一名员工报告在未尝试登录时收到多因素身份验证 (MFA) 推送通知。组织的安全控制面板显示，登录来自于具有公司资产编号的设备。安全运营中心 (SOC) 团队最合乎逻辑的第一步是什么？

- [ ] 禁用用户帐户，并远程清除其笔记本电脑
- [ ] 将登录 IP 和设备指纹与其他已知被入侵的用户进行比较
- [ ] 上报给人力资源部（认为用户有错）
- [ ] 在整个公司范围内发出警报，要求立即更改密码

查看正确答案 →

攻击类型：供应链硬件

1：减小受攻击面 2 3 4

一名员工报告在未尝试登录时收到多因素身份验证 (MFA) 推送通知。组织的安全控制面板显示，登录来自于具有公司资产编号的设备。安全运营中心 (SOC) 团队最合乎逻辑的第一步是什么？

- ✗ 禁用用户帐户，并远程清除其笔记本电脑
- ✓ 将登录 IP 和设备指纹与其他已知被入侵的用户进行比较
- ✗ 上报给人力资源部（认为用户有错）
- ✗ 在整个公司范围内发出警报，要求立即更改密码

在 SOC 团队确定可疑活动属于更广泛的攻击还是独立攻击以实现快速模式识别时，有针对性的事件响应和进一步风险控制在逻辑上是发现供应链硬件攻击时合乎逻辑的第一步。

下一问题 →

攻击类型：供应链硬件

1 — 2：检测和响应网络威胁 — 3 — 4

您的事件响应团队发现，多台受影响的笔记本电脑运行的 SSD 固件版本与供应商官方发行说明不符。端点检测响应 (EDR) 未显示恶意进程。这很可能意味着什么？

- [ ] IT 供应商配置错误
- [ ] 一种会自我删除的新型勒索软件
- [ ] 固件级供应链入侵
- [ ] 映像期间的正常行为

查看正确答案 →

攻击类型：供应链硬件

1 — 2：检测和响应网络威胁 — 3 — 4

您的事件响应团队发现，多台受影响的笔记本电脑运行的 SSD 固件版本与供应商官方发行说明不符。端点检测响应 (EDR) 未显示恶意进程。这很可能意味着什么？

- ✗ IT 供应商配置错误
- ✗ 一种会自我删除的新型勒索软件
- ✓ 固件级供应链入侵
- ✗ 映像期间的正常行为

多台笔记本电脑上具有未经授权的 SSD 固件，这些固件未被 EDR 检测到且与官方版本不符，表明存在蓄意的硬件或固件篡改行为，这正是固件级供应链漏洞的特征。

下一问题 →

攻击类型：供应链硬件

1 2 3：从网络攻击中恢复 4

您已隔离 100 个包含恶意 SSD 固件的可疑设备。您需要决定下一步行动，而不惊动可能具有远程访问权限的攻击者。您认为最佳的后续措施是什么？

- [ ] 关闭所有设备并送交取证
- [ ] 在系统运行时进行实时内存转储并进行调查
- [ ] 通知第三方供应商，他们的系统已被入侵
- [ ] 擦除所有设备并向全球所有用户重新发放新笔记本电脑

查看正确答案 →

攻击类型：供应链硬件

1 — 2 — 3：从网络攻击中恢复 — 4

您已隔离 100 个包含恶意 SSD 固件的可疑设备。您需要决定下一步行动，而不惊动可能具有远程访问权限的攻击者。您认为最佳的后续措施是什么？

- ✗ 关闭所有设备并送交取证
- ✓ 在系统运行时进行实时内存转储并进行调查
- ✗ 通知第三方供应商，他们的系统已被入侵
- ✗ 擦除所有设备并向全球所有用户重新发放新笔记本电脑

实时内存转储对于保留活动恶意软件和 Rootkit 等易失性证据至关重要，它能够在证据丢失或攻击者察觉之前，发现隐藏的威胁和接入点，从而实现有针对性的事件响应。

下一问题 →

攻击类型：供应链硬件

1 2 3 4：整体最佳实践

首席信息安全官要求您总结说明此次攻击是如何进入环境的。您需要向高管团队简要说明。您应该如何解释此次攻击？

- [ ] 从网络钓鱼链接意外下载了病毒
- [ ] 存在网络配置错误，允许外部访问
- [ ] 在笔记本电脑资源调配期间，恶意固件通过一家被入侵的硬件供应商进入我们的环境
- [ ] 我们的一位开发人员将不安全的代码推送到生产环境

查看正确答案 →

攻击类型：供应链硬件

1 2 3 4：整体最佳实践

首席信息安全官要求您总结说明此次攻击是如何进入环境的。您需要向高管团队简要说明。您应该如何解释此次攻击？

- ✗ 从网络钓鱼链接意外下载了病毒
- ✗ 存在网络配置错误，允许外部访问
- ✓ 在笔记本电脑资源调配期间，恶意固件通过一家被入侵的硬件供应商进入我们的环境
- ✗ 我们的一位开发人员将不安全的代码推送到生产环境

固件版本不匹配并且不存在活动恶意软件，这表明这是源自供应商的固件级攻击，而不是用户错误或配置错误。

查看解决方案 →

攻击类型：供应链硬件

回顾

供应链攻击近年来大幅增加。通过在生产、运输或部署期间篡改物理设备，或者发现软件提供商的弱点，攻击者就可以获得注入恶意组件或代码、损坏系统或泄露敏感数据的手段。受害者涵盖从小型企业到跨国企业的各类组织，导致的后果包括：重大财务损失、客户信任崩塌以及法律追责风险。

通过集成严格的供应商风险评估、嵌入零信任原则并结合持续的设备验证和独立的完整性检查，戴尔能够有效缓解供应链硬件攻击。我们在硬件的整个生命周期加强硬件完整性。

详细了解高级网络弹性战略，以及戴尔如何帮助您保护组织免遭供应链硬件攻击。

浏览供应链硬件攻击简述 →

⌂ 返回到场景

供应链保障 ›

凭借先进溯源、防篡改物流和透明采购，戴尔供应链能够在产品到达您的组织之前，对硬件、固件和供应商进行严格验证。

安全组件验证 (SCV) ›

在工厂和安装期间对 PC 组件进行加密验证，可确保真实性、检测隐藏的更改并降低供应链篡改风险。

可信工作区和可信基础架构 ›

基于硬件的身份验证和持续固件完整性检查可保护端点，提醒您注意未经授权的更改或恶意植入，做到未雨绸缪。

资产跟踪和具有 SupportAssist 的 ProSupport Suite ›

全面的资产跟踪、设备来源的实时监控和主动完整性验证，确保快速检测异常和全机群的安全性。

安全合作伙伴：AI 驱动的检测和响应 ›

AI 驱动的安全工具可实现持续监控、取证调查和自动遏制篡改或异常设备行为，确保快速应对供应链威胁。

攻击类型：供应链软件

您的公司提供医院使用的云分析软件。您的后端服务依赖于由 GitHub 上的可信第三方开发人员维护并且广泛使用的开源日志库。

在开发团队毫无察觉之际，攻击者入侵了 GitHub 帐户并植入了恶意更新，其中的隐藏代码旨在：

- 筛选环境变量，包括应用程序编程接口 (API) 密钥和 JavaScript Object Notation Web 令牌 (JWT) 密钥
- 在特定 IP 发出请求时创建反向 shell
- 保持休眠状态，除非远程触发

检验掌握情况 →

攻击类型：供应链软件

1：减小受攻击面　2　3　4

您的 API 突然开始向关键客户端返回 500 个错误。云监控检测到，在您的容器化服务与一个未知域之间存在出站连接。您首先会如何响应？

- [ ] 禁用所有来自容器的出站网络流量
- [ ] 重新启动受影响的服务以清除任何内存问题
- [ ] 在 GitHub 存储库中检查最近提交的代码
- [ ] 联系域的托管提供商

查看正确答案 →

攻击类型：供应链软件

1：减小受攻击面 2 3 4

您的 API 突然开始向关键客户端返回 500 个错误。云监控检测到，在您的容器化服务与一个未知域之间存在出站连接。您首先会如何响应？

- [x] 禁用所有来自容器的出站网络流量
- [ ] 重新启动受影响的服务以清除任何内存问题
- [ ] 在 GitHub 存储库中检查最近提交的代码
- [ ] 联系域的托管提供商

禁用容器的所有出站网络流量能够立即阻止攻击者泄露敏感数据或通过受损的日志记录库建立远程访问，从而实时隔离您的环境，并赢得关键时间来进行调查、保护 API 密钥和机密，防止休眠攻击机制被激活。

下一问题 →

攻击类型：供应链软件

1 — 2：检测和响应网络威胁 — 3 — 4

您的工程主管在问题开始前三天确认了从 GitHub 自动提取代码的应用程序。在任何公共数据库中，该版本尚未标记为恶意。负责任的即时行动是什么？

- [ ] 通过 GitHub 直接联系库维护者
- [ ] 删除所有本地项目依赖项并重建
- [ ] 等待公共漏洞和暴露 (CVE)，然后再采取进一步措施
- [ ] 回滚到上一个已知安全的代码版本

查看正确答案 →

攻击类型：供应链软件

1 — 2：检测和响应网络威胁 — 3 — 4

您的工程主管在问题开始前三天确认了从 GitHub 自动提取代码的应用程序。在任何公共数据库中，该版本尚未标记为恶意。负责任的即时行动是什么？

- ✗ 通过 GitHub 直接联系库维护者
- ✗ 删除所有本地项目依赖项并重建
- ✗ 等待公共漏洞和暴露 (CVE)，然后再采取进一步措施
- ✓ 回滚到上一个已知安全的代码版本

回滚到上一个已知的安全代码版本可立即删除受影响更新、消除攻击者的立足点，并恢复运营完整性，从而主动遏制风险并保护敏感数据。

下一问题 →

攻击类型：供应链软件

1 2 3：从网络攻击中恢复 4

经分析确认，库泄露了 API 密钥和云凭据。您发现有多个容器使用受影响版本构建。在您的遏制战略中，哪一步最关键？

- [ ] 在受影响的环境中撤销和轮换所有凭据
- [ ] 使用更新的操作系统 (OS) 映像重新映像容器
- [ ] 擦除开发团队的笔记本电脑
- [ ] 提交 GitHub 存储库的删除通知

查看正确答案 →

攻击类型：供应链软件

1 2 3：从网络攻击中恢复 4

经分析确认，库泄露了 API 密钥和云凭据。您发现有多个容器使用受影响版本构建。在您的遏制战略中，哪一步最关键？

- ✓ 在受影响的环境中撤销和轮换所有凭据
- ✗ 使用更新的操作系统 (OS) 映像重新映像容器
- ✗ 擦除开发团队的笔记本电脑
- ✗ 提交 GitHub 存储库的删除通知

云遭受入侵后，撤销并轮换凭据是第一个关键步骤，可阻止攻击者访问服务、中断数据盗窃并保护系统（无论漏洞范围如何）。

下一问题 →

攻击类型：供应链软件

1 2 3 4：整体最佳实践

您需要向首席技术官和法律/合规团队说明情况。最准确清晰的解释是什么？您如何总结此事件？

- [ ] 我们的内部持续集成和持续部署/交付 (CI/CD) 工具失败，导致部署了有问题的代码
- [ ] 第三方软件依赖性受到影响，而我们的自动化将该软件引入生产环境
- [ ] 开发人员在仓促发布的版本中引入了未经测试的代码
- [ ] 攻击者暴力入侵了 GitHub 存储库

查看正确答案 →

攻击类型：供应链软件

1 2 3 4：整体最佳实践

您需要向首席技术官和法律/合规团队说明情况。最准确清晰的解释是什么？您如何总结此事件？

- ✗ 我们的内部持续集成和持续部署/交付 (CI/CD) 工具失败，导致部署了有问题的代码
- ✓ 第三方软件依赖性受到影响，而我们的自动化将该软件引入生产环境
- ✗ 开发人员在仓促发布的版本中引入了未经测试的代码
- ✗ 攻击者暴力入侵了 GitHub 存储库

根本原因是供应链攻击：第三方软件依赖项被攻击者破坏，自动化构建进程直接将恶意更新引入生产环境，影响了应用程序完整性和敏感环境，暴露出可信外部依赖项中恶意更新的风险。

查看解决方案 →

攻击类型：供应链软件

回顾

供应链软件网络攻击利用软件更新、第三方集成和开发环境中的漏洞，嵌入跨网络传播的恶意代码。这些攻击可能会导致广泛的数据泄露和运营中断，并危及整个生态系统，从而影响各个规模的企业。

戴尔致力于提升网络弹性，注重透明度、安全开发和持续监控，同时维护强大的事件响应计划，从而确保快速恢复并与利益相关者保持沟通。

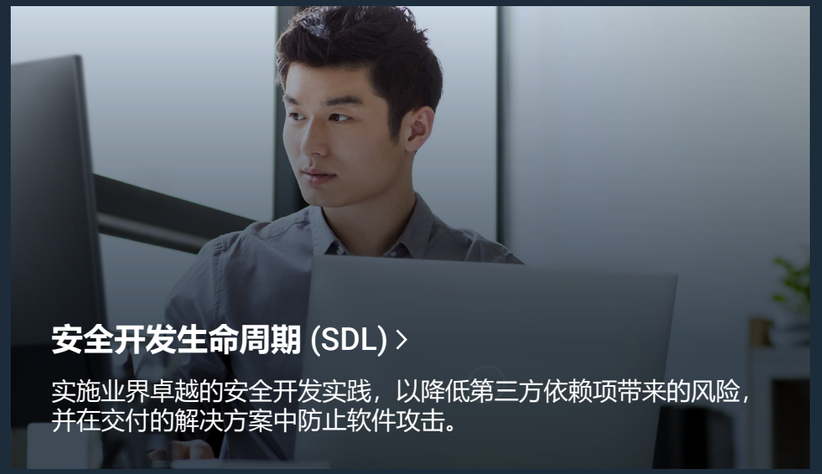
详细了解高级网络弹性战略，以及戴尔如何帮助您保护组织免遭供应链软件攻击。

浏览供应链软件攻击简述 →

返回到场景

供应链保障 ›

凭借先进溯源、防篡改物流和透明采购，戴尔供应链能够在产品到达您的组织之前，对硬件、固件和供应商进行严格验证。



安全开发生命周期 (SDL) ›

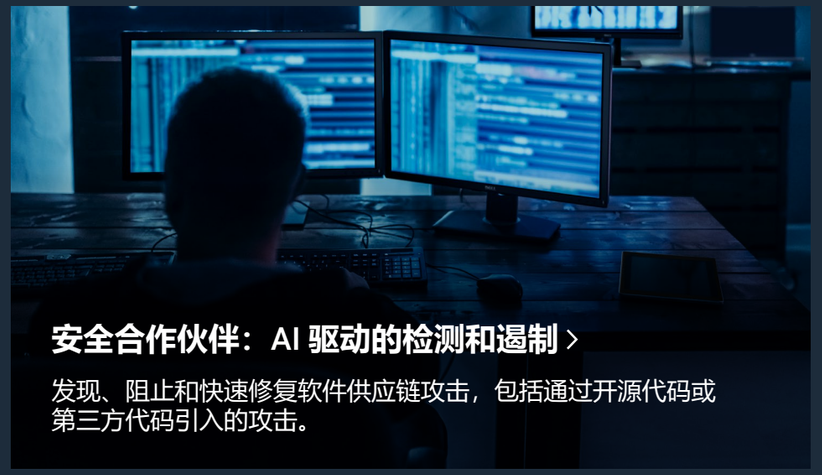
实施业界卓越的安全开发实践，以降低第三方依赖项带来的风险，并在交付的解决方案中防止软件攻击。

可信工作区和可信基础架构 ›

SafeBIOS、SafeID 和 SafeDataDelivers 硬件身份验证有助于确保端点仅运行可信代码，并快速检测未经授权或恶意的软件修改。

资产跟踪和具有 SupportAssist 的 ProSupport Suite ›

实时监控设备和软件可快速检测和响应供应链中出现的异常情况。



安全合作伙伴：AI 驱动的检测和遏制 ›

发现、阻止和快速修复软件供应链攻击，包括通过开源代码或第三方代码引入的攻击。

攻击类型：零日攻击

您是负责监控公司身份验证日志的安全分析师。近期，用户反映其帐户遭到未经授权的访问，但他们并未共享任何凭据。

调查日志后，您发现存在以下活动：

```
[INFO] 2025-04-02 14:05:12 - User Login - UserID: 1023 - IP: 192.168.1.15 - JWT Token Issued
[INFO] 2025-04-02 14:07:35 - User Login - UserID: 1023 - IP: 5.62.60.12 - JWT Token Reused
[INFO] 2025-04-02 14:08:00 - User Login - UserID: 1023 - IP: 203.0.113.45 - JWT Token Reused
```

与此同时，一位安全研究人员发现应用程序编程接口 (API) 存在漏洞：

- JavaScript Object Notation Web 令牌 (JWT) 永不过期。
- 令牌存储在本地存储中，而非 HTTP-only Cookie。
- 不强制实施多因素身份验证 (MFA)。

检验掌握情况 →

攻击类型：零日攻击

1：减小受攻击面　2　3　4

您是一名安全团队成员，由于攻击未触发警告，您怀疑这是零日攻击，如何确认这一点？

- [ ] 将所有用户从其系统中注销
- [ ] 识别日志中的关键异常身份验证行为
- [ ] 致电其他公司的朋友，看看他们是否遇到相同的问题
- [ ] 尝试与其他安全异常活动进行关联

查看正确答案 →

攻击类型：零日攻击

1：减小受攻击面 2 3 4

您是一名安全团队成员，由于攻击未触发警告，您怀疑这是零日攻击，如何确认这一点？

- ✗ 将所有用户从其系统中注销
- ✓ 识别日志中的关键异常身份验证行为
- ✗ 致电其他公司的朋友，看看他们是否遇到相同的问题
- ✓ 尝试与其他安全异常活动进行关联

确定异常身份验证行为（如异常登录次数、凭据重复使用或来自非典型设备的访问），并将其与其他异常安全活动（如数据访问异常或权限升级）相关联，可确认发生协同零日攻击。

下一问题 →

攻击类型：零日攻击

1 — 2：检测和响应网络威胁 — 3 — 4

漏洞未知，因此安全团队必须在调查时限制损害程度。您会怎么做？

- [ ] 使系统范围内的所有身份验证会话无效
- [ ] 将所有资源集中在攻击的进入点
- [ ] 仅强制执行多因素身份验证 (MFA) 登录
- [ ] 依靠当前静态防火墙或 Web 应用程序防火墙 (WAF) 规则

查看正确答案 →

攻击类型：零日攻击

1 — 2：检测和响应网络威胁 — 3 — 4

漏洞未知，因此安全团队必须在调查时限制损害程度。您会怎么做？

- ✓ 使系统范围内的所有身份验证会话无效
- ✗ 将所有资源集中在攻击的进入点
- ✓ 仅强制执行多因素身份验证 (MFA) 登录
- ✗ 依靠当前静态防火墙或 Web 应用程序防火墙 (WAF) 规则

这些措施可共同增强安全性并尽可能降低风险，同时切断攻击者的访问，以便安全团队可以调查和解决底层漏洞。

下一问题 →

攻击类型：零日攻击

1 2 3：从网络攻击中恢复 4

戴尔 PC 具有安全启动、可信平台模块 (TPM)、基本输入/输出系统 (BIOS) 密码保护和 SafeBIOS 等技术。在零日攻击中，这些技术有何帮助？

- [ ] 防止窃取应用程序编程接口 (API) 令牌的凭据转储攻击
- [ ] 防止具有物理访问权限的攻击者绕过操作系统 (OS) 安全性，安装窃取身份验证令牌的恶意软件
- [ ] 确保攻击者无法操纵 BIOS 设置来削弱操作系统安全性，导致 API 会话劫持
- [ ] 以上都是

查看正确答案 →

攻击类型：零日攻击

1 — 2 — 3：从网络攻击中恢复 — 4

戴尔 PC 具有安全启动、可信平台模块 (TPM)、基本输入/输出系统 (BIOS) 密码保护和 SafeBIOS 等技术。在零日攻击中，这些技术有何帮助？

- [x] 防止窃取应用程序编程接口 (API) 令牌的凭据转储攻击
- [x] 防止具有物理访问权限的攻击者绕过操作系统 (OS) 安全性，安装窃取身份验证令牌的恶意软件
- [x] 确保攻击者无法操纵 BIOS 设置来削弱操作系统安全性，导致 API 会话劫持
- [x] 以上都是

这种分层方法可提供全面防护，避免受到以 BIOS、固件、凭据和系统配置为目标的零日攻击。通过防止篡改、未经授权的访问和凭证盗窃，即使攻击者发现新的漏洞，这些技术同样能保持有效。

下一问题 →

攻击类型：零日攻击

1 2 3 4：整体最佳实践

防止零日攻击发生的最佳方法是什么？

- [ ] 不使用开源软件
- [ ] 利用零信任原则
- [ ] 进行全面修补，包括操作系统 (OS)、固件、应用程序编程接口 (API)、库和容器
- [ ] 在公司周围安装一道通电的大门，将威胁者挡在外面

查看正确答案 →

攻击类型：零日攻击

1 2 3 4：整体最佳实践

防止零日攻击发生的最佳方法是什么？

- ✗ 不使用开源软件
- ✓ 利用零信任原则
- ✗ 进行全面修补，包括操作系统 (OS)、固件、应用程序编程接口 (API)、库和容器
- ✗ 在公司周围安装一道通电的大门，将威胁者挡在外面

若存在未知漏洞或未修补的系统，零信任原则通过以下方式防止零日攻击：消除来自用户和设备的隐性信任、强制执行持续身份验证、仅允许访问必要信息，并遏制攻击者移动来显著降低因未发现的威胁而带来的组织风险。

查看解决方案 →

攻击类型：零日攻击

回顾

零日攻击是指攻击者在修补程序或补丁程序推出之前，攻击软件或硬件中未公开的安全漏洞。攻击者通常会利用这个窗口期趁虚而入，在企业发现并解决漏洞之前造成大规模的业务中断。

戴尔通过零信任控制、网络分段、快速遏制和用户培训应对零日攻击，可进一步增强对新兴威胁的防御能力。

详细了解高级网络弹性战略，以及戴尔如何帮助您保护组织免遭零日攻击。

浏览零日攻击简述 →

返回到场景

可信工作区和可信基础架构 >

保护端点和基础架构。利用 SafeBIOS、SafeID、SafeData 保护并结合多因素身份验证 (MFA) 和基于角色的访问控制 (RBAC) 等零信任框架，戴尔提供多层防御体系，可限制攻击路径并确保硬件身份验证。

POWEREDGE 服务器 >

安全启动、芯片级信任根和 SmartFabric 网络分段可限制横向移动，确保仅在基础架构上运行可信代码。

安全合作伙伴 >

高级威胁情报、Managed Detection and Response (MDR)、扩展检测和响应 (XDR) 以及精细化访问控制有助于在零日攻击传播之前检测、搜寻和遏制这些攻击。

PowerProtect 产品组合 >

不可变备份、隔离的网络恢复存储区和 AI 驱动的 CyberSense 分析可确保在零日泄露后快速恢复并保持弹性。

安全性和弹性服务 >

从修补程序管理到事件响应，戴尔专家提供快速遏制、取证调查和弹性计划，有效应对零日威胁。


DELL Technologies