端点安全性是零信任之旅的重要组成要素

关于做好零信任准备的三点建议

1 下一页

执行摘要

构建零信任环境是一段漫长的旅程。它并不是由组织实施的产品或解决方案，而是长久以来建立的安全管理战略框架。本电子书为 IT 决策者顺利推进零信任转型提供了切实可行的指导，其中着重介绍了在当今随时随地办公的大环境下，端点设备安全性对于构筑真正安全的现代化基础所发挥的作用。

目录

网络现状 3
随时随地办公环境带来的影响 4
安全战略需要改变 5
了解零信任的基础 6
启用零信任原则 7
关于做好零信任准备的三点建议 8
要点 11
采取下一步行动 11

网络现状

在不断普及的远程/混合和云办公环境下，安全威胁与日俱增。

在过去几年里，保护组织数据资产的复杂性急剧增长。随着越来越多的企业采用远程/混合办公模式，云已经对企业生产力产生颠覆性影响，但它并非不计成本。从只管理本地基础架构转向兼容并包的云环境，为不法分子创造了更大的攻击面，同时带来了愈发严重的后果。例如，一旦攻击者得逞，那么影响的不仅仅是一位客户，很可能是该云服务的每位客户以及整个供应链上的客户。威胁行为体（上至民族国家，下至普通罪犯）所获得的回报可能异常巨大，因此他们会继续寻找新漏洞加以利用。

到 2025 年，全球网络犯罪造成的损失预计将攀升至 **10.5 万亿美元**[i]

在 2022 年的一项研究中，Verizon 报告了 **5,200 起**已经证实的数据泄露事件，**相比上一年增加了 1.3 倍**[ii]

随时随地办公环境带来的影响

组织必须找到方法，提前布局应对不断变化的威胁环境。

那么，不断增加的远程办公环境带来了哪些影响？两个方面：

所有组织都不堪一击...

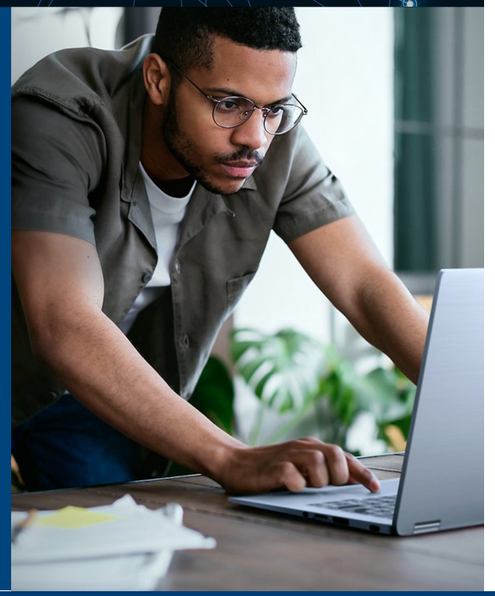
> “如果一个处心积虑的实体真的想进入您的系统，那么他们成功的可能性相当大。”
>
> *— 美国国家安全局前局长、美国网络司令部前司令 Michael Rogers 上将*[iii]

...而错误的代价可能是致命的。

> “2024 年，一次数据泄露造成的平均损失达到历史最高水平 488 万美元。”[iv]

攻击载体不断增加，攻击面不断扩大，没有公司完全安全。组织必须假设最坏情况，并针对不可避免的攻击加强防御。

69% 的组织有过由于面向互联网的资产管理不善而遭受某种网络攻击的经历。[v]



安全战略需要不断演变

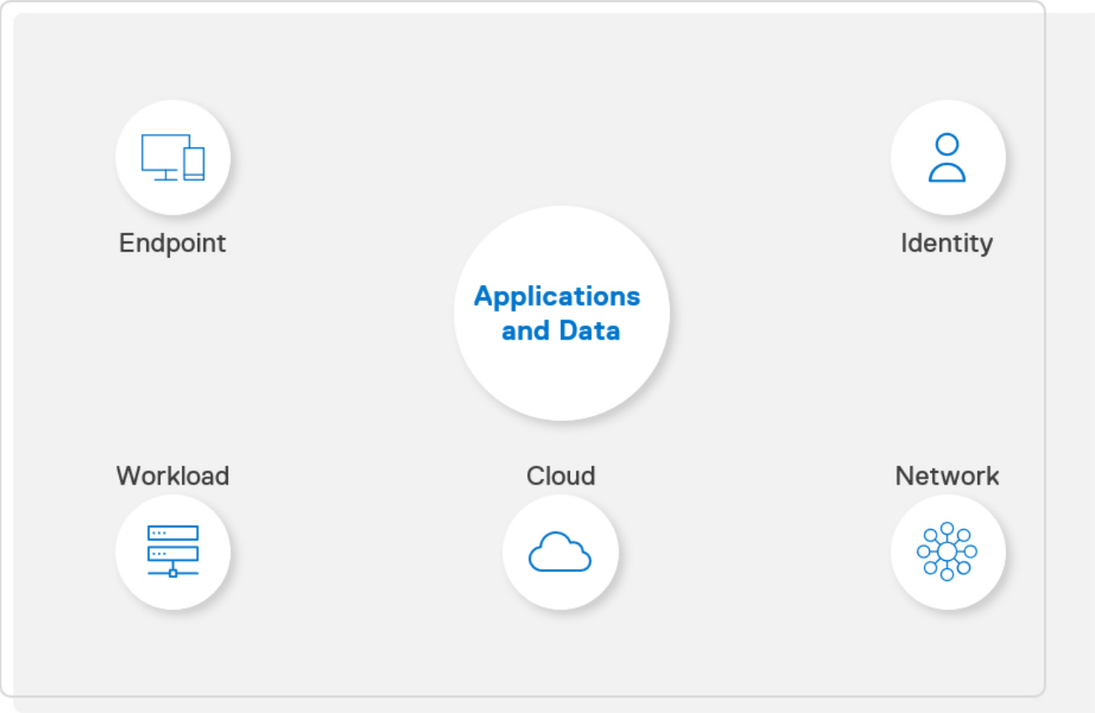
我们必须接纳云环境，由此零信任应运而生。

传统安全模式失去作用。原因如下。

任何组织想要拥有强健的安全态势，就必须考虑五个控制点：端点、工作负载、身份、网络和云。目标是保护应用程序和数据。

传统方法通常是相互孤立的，这使得采用这些方法的组织更容易受到攻击。

接下来...

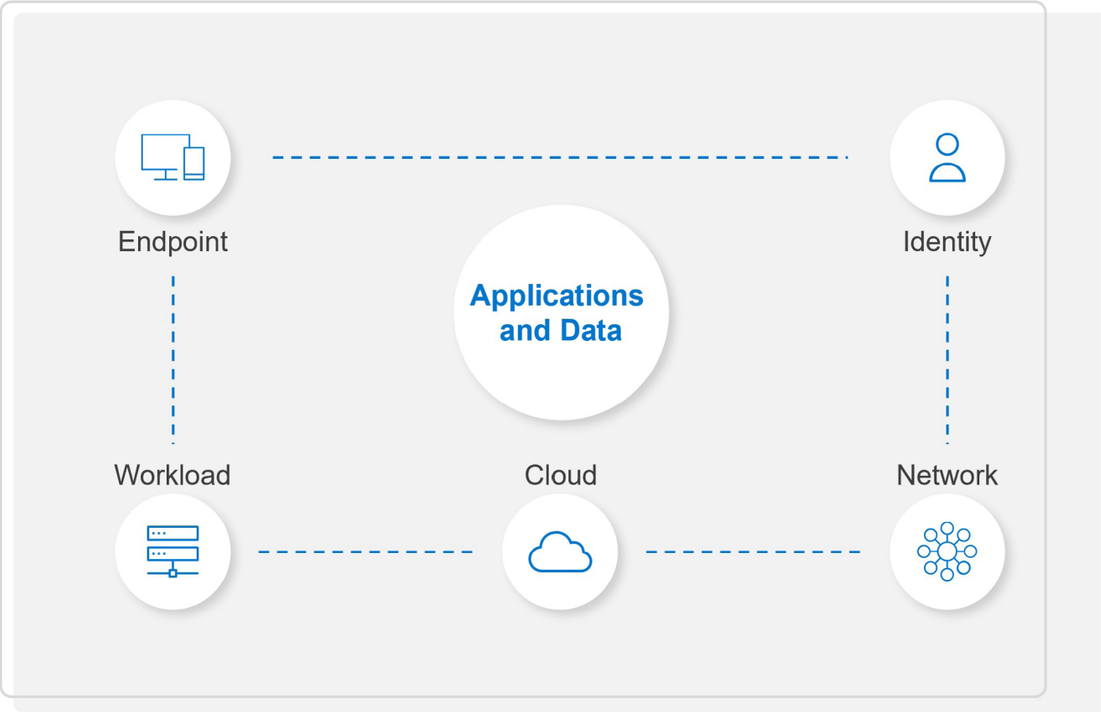


安全战略需要不断演变

我们必须接纳云环境，由此零信任应运而生。

现代方法趋向于实施更多管控，并在控制点之间实现更好的通信。但是，随着我们越来越多地采用远程/混合办公环境，我们需要进一步加强外围安全。

接下来...

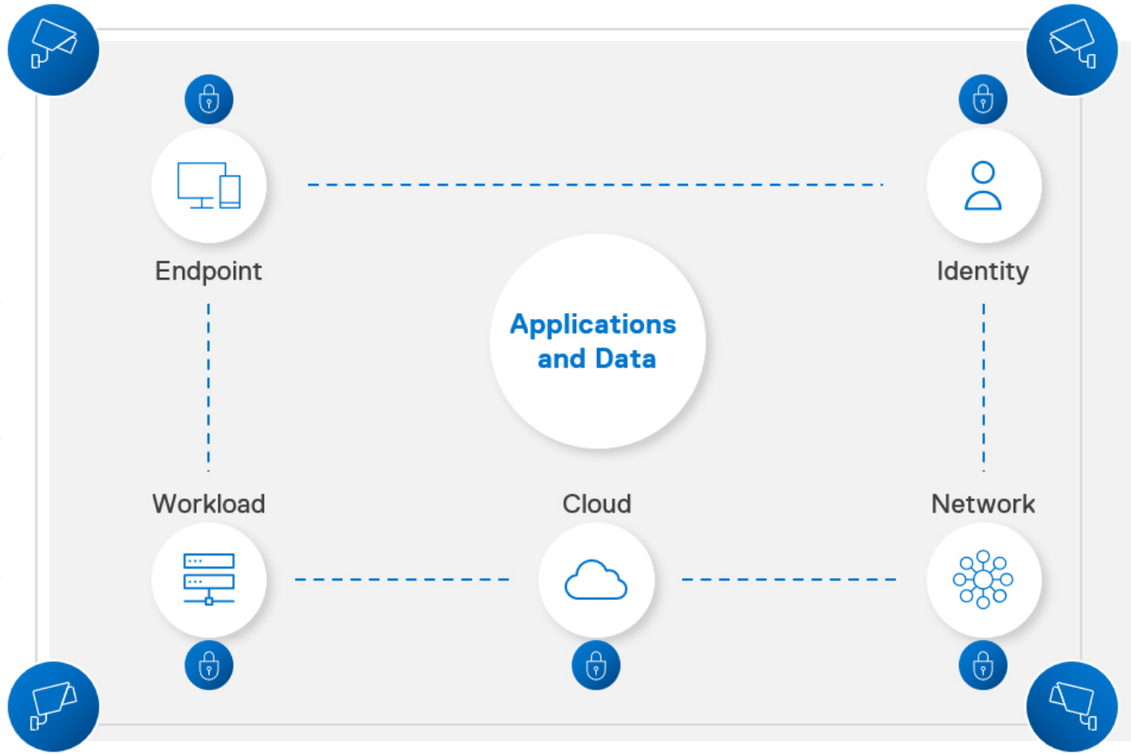


安全战略需要不断演变

我们必须接纳云环境，由此零信任应运而生。

如今，员工可以在家、咖啡馆、酒店随时随地办公，经常使用不安全的 Wi-Fi，甚至无法连接到防火墙保护的办公室和数据中心。默认情况可能是从他们的设备直接连接到互联网，然后连接到云文件服务器和“软件即服务”(SaaS) 应用程序，并使用企业数据。

随着攻击变得日益诡诈以及攻击载体的数量不断增加，建立在隐式信任基础上的传统安全战略不再有效。由此零信任应运而生。



了解零信任的基础

零信任是思考安全性的一种全新方式。它取代了隐式 信任，即一旦通过身份验证，用户就可以在网络上畅通无阻。零信任颠覆了这种范式，为组织提供了一种显式控制 IT 环境的手段。

我们可以借助一个众所周知的概念来解释零信任，即构建安全协议。

您在一家公司的办公室工作。当您被聘用时，您收到了一个工牌并学习了安全协议。每天您都会走进办公大楼。摄像头遍布四周。您可以在多个地方使用工牌进入。坐在办公桌前，您通过输入密码来解锁计算机。

An employee arrives at their office building and gets their badge out to gain entry.

接下来...

了解零信任的基础

零信任是思考安全性的一种全新方式。它取代了隐式 信任，即一旦通过身份验证，用户就可以在网络上畅通无阻。零信任颠覆了这种范式，为组织提供了一种显式控制 IT 环境的手段。

我们可以借助一个众所周知的概念来解释零信任，即构建安全协议。

您在一家公司的办公室工作。当您被聘用时，您收到了一个工牌并学习了安全协议。每天您都会走进办公大楼。摄像头遍布四周。您可以在多个地方使用工牌进入。坐在办公桌前，您通过输入密码来解锁计算机。

An employee arrives at their office building and gets their badge out to gain entry.

They use their badge to gain access to the elevator assigned to their floor.

接下来...

了解零信任的基础

零信任是思考安全性的一种全新方式。它取代了隐式 信任，即一旦通过身份验证，用户就可以在网络上畅通无阻。零信任颠覆了这种范式，为组织提供了一种显式控制 IT 环境的手段。

我们可以借助一个众所周知的概念来解释零信任，即构建安全协议。

您在一家公司的办公室工作。当您被聘用时，您收到了一个工牌并学习了安全协议。每天您都会走进办公大楼。摄像头遍布四周。您可以在多个地方使用工牌进入。坐在办公桌前，您通过输入密码来解锁计算机。

An employee arrives at their office building and gets their badge out to gain entry.

They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.

接下来...

了解零信任的基础

零信任是思考安全性的一种全新方式。它取代了隐式 信任，即一旦通过身份验证，用户就可以在网络上畅通无阻。零信任颠覆了这种范式，为组织提供了一种显式控制 IT 环境的手段。

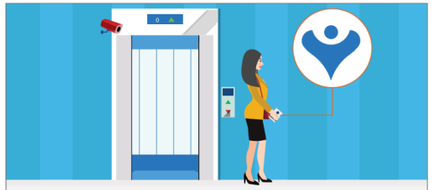
我们可以借助一个众所周知的概念来解释零信任，即构建安全协议。

您在一家公司的办公室工作。当您被聘用时，您收到了一个工牌并学习了安全协议。每天您都会走进办公大楼。摄像头遍布四周。您可以在多个地方使用工牌进入。坐在办公桌前，您通过输入密码来解锁计算机。

An employee arrives at their office building and gets their badge out to gain entry.

They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

接下来...

了解零信任的基础

零信任是思考安全性的一种全新方式。它取代了隐式 信任，即一旦通过身份验证，用户就可以在网络上畅通无阻。零信任颠覆了这种范式，为组织提供了一种显式控制 IT 环境的手段。

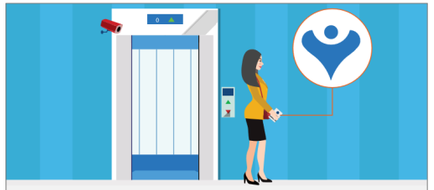
我们可以借助一个众所周知的概念来解释零信任，即构建安全协议。

您在一家公司的办公室工作。当您被聘用时，您收到了一个工牌并学习了安全协议。每天您都会走进办公大楼。摄像头遍布四周。您可以在多个地方使用工牌进入。坐在办公桌前，您通过输入密码来解锁计算机。

An employee arrives at their office building and gets their badge out to gain entry.

They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

They swipe their ID card to gain entry to their suite.

接下来...

了解零信任的基础

零信任是思考安全性的一种全新方式。它取代了隐式 信任，即一旦通过身份验证，用户就可以在网络上畅通无阻。零信任颠覆了这种范式，为组织提供了一种显式控制 IT 环境的手段。

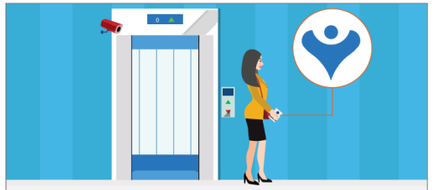
我们可以借助一个众所周知的概念来解释零信任，即构建安全协议。

您在一家公司的办公室工作。当您被聘用时，您收到了一个工牌并学习了安全协议。每天您都会走进办公大楼。摄像头遍布四周。您可以在多个地方使用工牌进入。坐在办公桌前，您通过输入密码来解锁计算机。

An employee arrives at their office building and gets their badge out to gain entry.

They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

They swipe their ID card to gain entry to their suite.

The employee arrives at their desk and unlocks their computer using a password.

接下来...

了解零信任的基础

这就是零信任的工作原理。

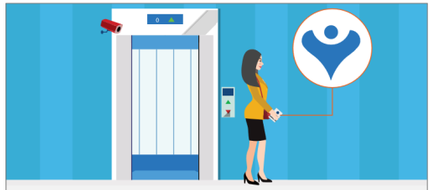
您的雇主在第一天就标识了您的身份。从那时起，您请求的每次访问都会经过验证，以保护组织的资产（用户、数据等）。为了增加一层安全保障，保安人员会在监视器前关注大楼内的所有活动。任何试图进入“禁区”的可疑行为都会受到调查。

如今，无论是用户、设备、应用程序还是数据，它们都比以往都更频繁地出现在公司网络之外。这就导致了用户身份成为盲点，身份盗用成为造成绝大多数数据泄露事件的关键因素。零信任将彻底改变这种局面。

An employee arrives at their office building and gets their badge out to gain entry.

They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

They swipe their ID card to gain entry to their suite.

The employee arrives at their desk and unlocks their computer using a password.

启用零信任原则

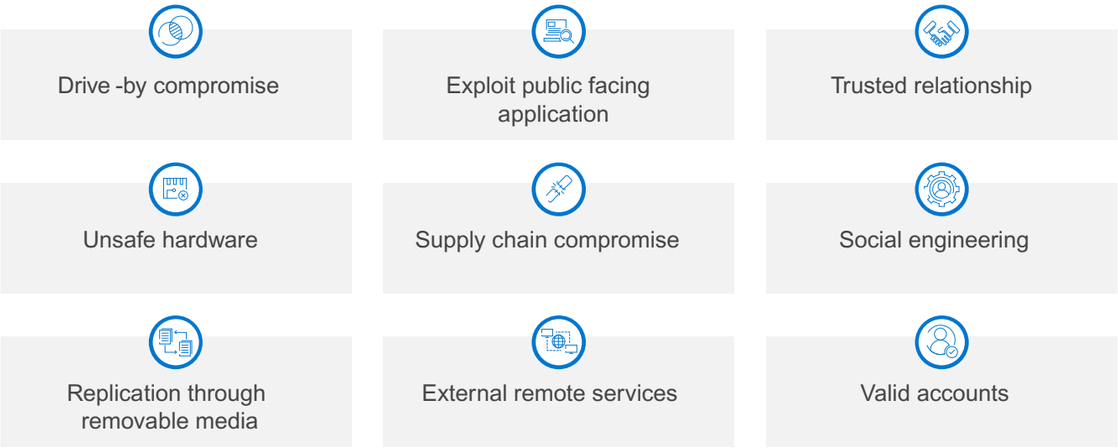
端点安全性是零信任转型的重要组成要素。

为了确保零信任策略的可靠性，您必须加强端点保护。

MITRE ATT&CK® 框架表明，当前，不法分子通常使用九种“初始访问技术”获取网络访问权限（*参见下图*）。[vi] 研究表明，在基于云的环境中，传统的防御措施无法保证端点的安全。攻击者只需要一个进入点。通过端点，威胁行为体可以在设备的整个生命周期内利用许多漏洞。

随着网络中设备数量的增加，端点变成了越来越大的攻击载体。

零信任模式中的安全策略详尽地定义了“已知良好的行为”，除这些行为之外，其他任何行为都会被阻止。之后，威胁管理功能密切监视偏离已知良好行为情况的发生，标记反常行为，并触发相应修正操作来防范潜在威胁。



第 1 幅图，共 3 幅

启用零信任原则

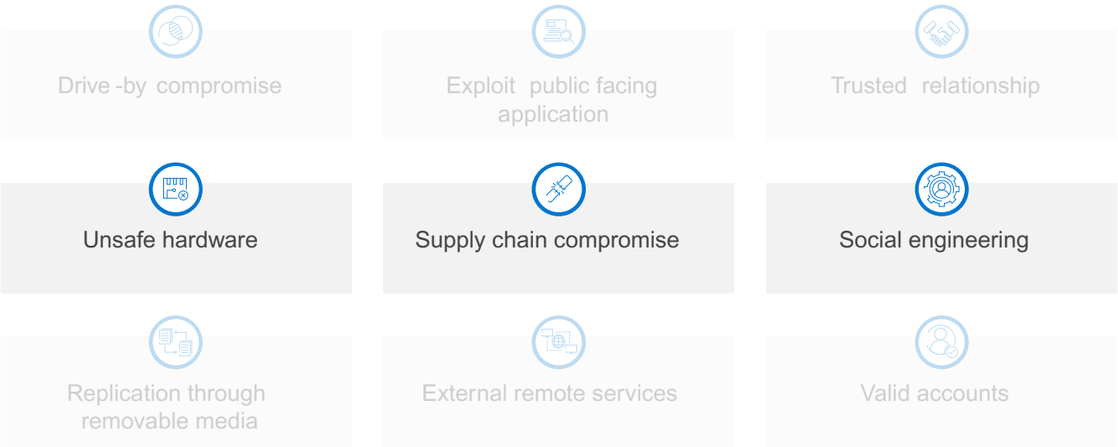
端点安全性是零信任转型的重要组成要素。

为了确保零信任策略的可靠性，您必须加强端点保护。

MITRE ATT&CK® 框架表明，当前，不法分子通常使用九种“初始访问技术”获取网络访问权限（*参见下图*）。[vi] 研究表明，在基于云的环境中，传统的防御措施无法保证端点的安全。攻击者只需要一个进入点。通过端点，威胁行为体可以在设备的整个生命周期内利用许多漏洞。

随着网络中设备数量的增加，端点变成了越来越大的攻击载体。

零信任模式中的安全策略详尽地定义了“已知良好的行为”，除这些行为之外，其他任何行为都会被阻止。之后，威胁管理功能密切监视偏离已知良好行为情况的发生，标记反常行为，并触发相应修正操作来防范潜在威胁。



启用零信任原则

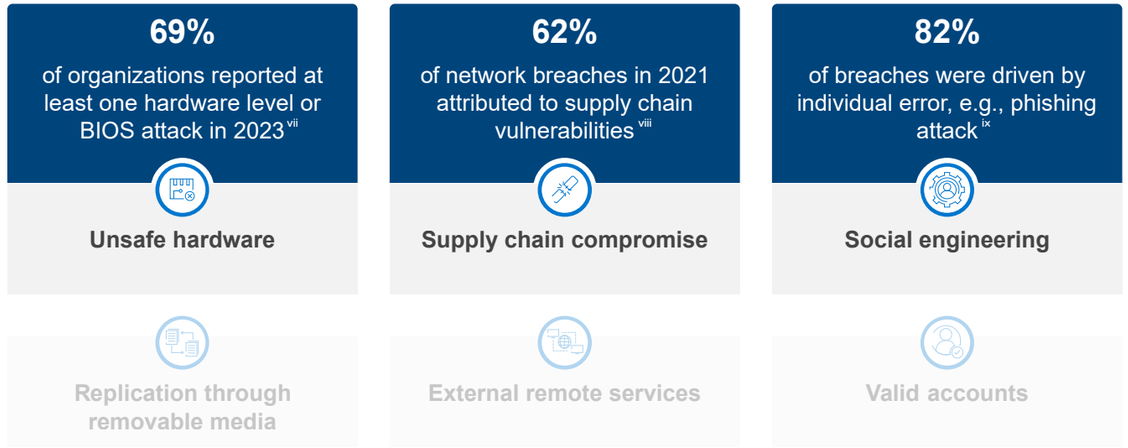
端点安全性是零信任转型的重要组成要素。

为了确保零信任策略的可靠性，您必须加强端点保护。

MITRE ATT&CK® 框架表明，当前，不法分子通常使用九种“初始访问技术”获取网络访问权限（*参见下图*）。[vi] 研究表明，在基于云的环境中，传统的防御措施无法保证端点的安全。攻击者只需要一个进入点。通过端点，威胁行为体可以在设备的整个生命周期内利用许多漏洞。

随着网络中设备数量的增加，端点变成了越来越大的攻击载体。

零信任模式中的安全策略详尽地定义了“已知良好的行为”，除这些行为之外，其他任何行为都会被阻止。之后，威胁管理功能密切监视偏离已知良好行为情况的发生，标记反常行为，并触发相应修正操作来防范潜在威胁。



第 3 幅图，共 3 幅

关于做好零信任准备的三点建议

做好充足准备，助力组织成功实现零信任转型。

1

建立正确的策略和控制来支持您的业务优先事项。

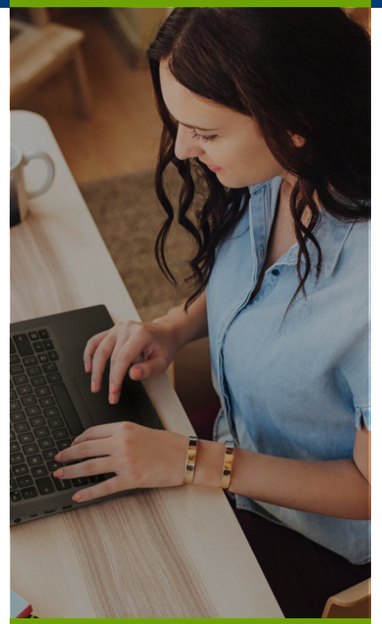
策略引擎和策略管理是有效实施零信任的关键。但是，任何组织用于保障安全的预算都是有限的，因此首先要确定您的业务优先事项。您想要保护的最关键资产和 IP 是什么？根据贵组织可承受的风险评估攻击面。

然后，审核当前实施的策略和控制。如今的风险来自于我们所生活的基于云的环境。您的策略引擎是否考虑到了这一点？

有了控制对最重要资产访问的策略，您就可以扩展范围了。

了解详情

有关详细信息，*请观看此视频*，视频中多名戴尔网络专家一起讨论了组织当前面临的主要安全风险。



随着公司网络之外的用户、应用程序、数据和设备比以往显著增多，**82%** 的 IT 安全决策者表示，他们不得不重新评估其安全策略。[x]

关于做好零信任准备的三点建议

做好充足准备，助力组织成功实现零信任转型。

2 从安全的设备开始。

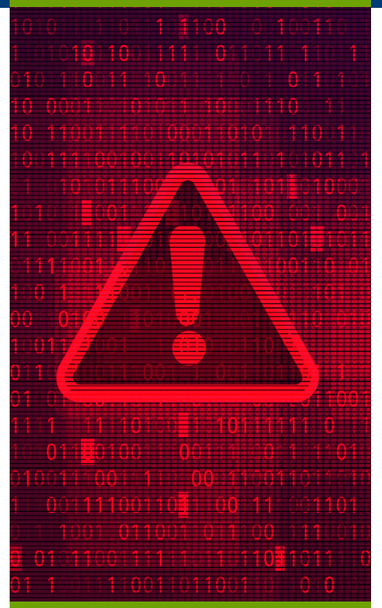
在坚实的基础上实施零信任计划。借助在设计和开发时充分考虑安全性的设备加强防御。其中包括：

A. **基于硬件和固件的保护**，旨在保护端点堆栈并提供可见性（例如，检测 BIOS 是否已被入侵并向 IT 发出警报）。为贵组织配备相应技术，能够针对每个新的访问请求验证身份，尽可能减少对员工工作效率的影响。

B. **供应链保护和完整性控制**，旨在保护 PC 生命周期的每一步。正如我们在近年来所看到的，供应链攻击可能是毁灭性的。在一个真正的零信任体系结构中，身份验证、权限验证和监视等安全手段均已在供应链端部署。合作的供应商要满足以下条件：1) 采用安全实践 2) 从采购到制造再到交付，允许您全程验证设备的完整性。

了解详情

有关设备安全性最佳实践的详细信息，请查看戴尔和英特尔联合发布的白皮书《Achieving Pervasive Security Above and Below the OS》。



2021 年，一家 IT 管理公司至少向 1,500 家客户传播了勒索软件攻击。[xi]

关于做好零信任准备的三点建议

做好充足准备，助力组织成功实现零信任转型。

3

努力实现整个生态系统的无缝集成和互操作性。

要实现有效的安全态势，概括来说，需要从以下三个关键方面入手：

A. 集成整个 IT 生态系统的所有防御

B. 实时可见性以及

C. 有能力在需要时采取行动。

在基于云的环境中，最小的漏洞即使放任不管，也可能会成为梦魇，因此所有系统都必须能够识别潜在威胁，并随时做好采取必要行动的准备。

您的系统是集成的，还是单独运行的？当 IT 管理员收到网络上出现损坏的 BIOS 的警报时，您的策略引擎能否触发特定的工作流？在集成环境中，应立即自动隔离有问题的 BIOS，限制此后发生的所有访问并运行修补。

您能否查看所有端点？理想情况下，从供应链（例如装货码头）到固件（例如 BIOS 级篡改警报），在每一层都有丰富的遥测数据流入。

但是，遥测的效果取决于集成情况。您是否能操作您的数据？您有必要配置合适的资源（例如技能娴熟的网络安全人才），从而利用数据和程序工作流来解决问题。

41% 的组织正在部署零信任模型[xii]

DELL Technologies

要点

未来的安全之道是部署零信任模型。

- 随着我们接受未来的工作方式，攻击载体的数量也会倍增。
- 漏洞是不可避免的。部署防御措施，尽量减小攻击面，为最坏情况做好准备。
- 零信任是思考安全性的一种全新方式，为组织提供了一种显式控制 IT 环境的手段。
- 启用零信任原则来保护端点安全，对于确保现代基础架构的安全至关重要。
- 准确找出最关键的资产，为其优先构建零信任体系结构。
- 从可提供内置保护并在其供应链控制上进行深入投资的供应商购买设备。
- 评估安全性和 IT 互操作性。继续嵌入工作流以增强您的安全态势。

采取下一步行动

对于各种规模的组织来说，安全都是一个令人生畏的话题。携手经验丰富的安全技术合作伙伴，优化您的零信任转型过程。

Dell Trusted Workspace 可帮助您保护端点，打造零信任就绪型现代 IT 环境。借助戴尔特有的全面硬件和软件保护产品组合，减小攻击面。我们高度协调、以防御为基础的方法通过将内置的保护与持续的警戒功能相结合来抵抗威胁。专为当今基于云的环境而构建的安全解决方案可以让终端用户高效工作，让 IT 充满信心。

联系我们： global.security.sales@dell.com
访问我们： Dell.com/Endpoint-Security
关注我们： LinkedIn @DellTechnologies | Twitter @DellTech

[i] 网络安全年鉴第 2 版，Cybersecurity Ventures，2022 年，https://cybersecurityventures.com/cybersecurity-almanac-2022/

[ii] Ponemon Institute 和 IBM：《Cost of a Data Breach Report 2024》，https://www.ibm.com/security/data-breach

[iii] 美国心脏病学会：《You Will Be Hacked.Plan Now: Cybersecurity in Health Care》，2021 年，https://www.acc.org/Latest-in-Cardiology/Articles/2021/11/01/01/42/Feature-You-Will-Be-Hacked-Plan-Now-Cybersecurity-in-Health-Care

[iv] Ponemon Institute 和 IBM：《Cost of a Data Breach Report 2024》，https://www.ibm.com/security/data-breach

[v] 《ESG Complete Survey Results: Security Hygiene and Posture Management》，2022 年，https://www.esg-global.com/research/esg-complete-survey-results-security-hygiene-and-posture-management

[vi] MITRE ATT&CK https://attack.mitre.org/tactics/TA0001/

[vii] Futurum Group：《Endpoint Security Trends 2023》，https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/industry-market/futurum-group-endpoint-security-trends-research-report.pdf

[viii] Verizon 数据泄露调查报告，2022 年 https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[ix] Verizon 数据泄露调查报告，2022 年 https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[x] Absolute 端点风险报告，2021 年，https://www.absolute.com/go/reports/endpoint-risk-report/

[xi] TechTarget，2021 年，https://www.techtarget.com/searchsecurity/news/252503605/Kaseya-1500-organizations-affected-by-REvil-attacks

[xii] Ponemon Institute 和 IBM：《Cost of a Data Breach Report 2022》，https://www.ibm.com/security/data-breach

版权所有 © 2024 Dell Inc. 或其子公司。 保留所有权利。 Dell Technologies、Dell 和其他商标为 Dell Inc. 或其子公司的商标。 其他商标可能是其各自所有者的商标。