10 个不可或缺的零信任数据中心要素

真正的零信任数据中心会将最终用户体验作为优先考量。

这意味着：

- *网络访问需要快速、可靠且可扩展*
- *用户和设备需要受到保护*
- *应用和工作负载需要为数据保驾护航*
- *安全性需要为业务敏捷性提供助力*

10 化无形为有形

您无法保护看不见的东西。

您需要纵观横跨不同环境的整个网络，了解如何保护从客户端到工作负载的每一网络部分。

9 多点分段

我们需要细分到每一部分。

从用户和设备，到应用和工作负载之间，精细化分段和控制可以防止恶意访问，避免出现防御漏洞。

8 为用户、设备和工作负载设置身份

身份不仅仅适用于用户...

身份也适用于设备和工作负载。身份由多重因素组成，有助于在任何特定时刻发现网络中的风险。

7 不受位置限制的无缝策略

随时随地跟随用户、设备和应用。

用户、应用和工作负载无时无刻不在移动。确保安全策略紧跟应用对象，可以限制潜在的攻击媒介。

6 了解网络流量的意图

流量的目的地在哪？当前状态如何？

尽可能多地了解所有网络流量及其目的地，包括还没有解密的流量。但如何了解呢？可以从观察特定的流量指标和行为着手。

5 随时随地实现自动化

让自动化成为您的超能力！

自动化能让您的工作更轻松，增强团队间的工作效率。这项技术可以确保将数据中心中的个别变更应用到所有位置，并在攻击事件发生之前做出响应。

4 监控并使用所有连接点

将安全性扩展到传统应用之外。

利用路由器和交换机检测威胁，并提供强制措施来保护数据中心环境。

3 有效阻断基本问题

真实情况：如果安全技术不能捕获已知威胁，那就不值得投资。

数据是不会说谎的！做一些调查，看看哪些安全供应商是在正面应对威胁并阻止网络攻击。

2 让应用保持良好的正常运行时间

永不言败。

业务的成功取决于网络的正常运行和资源之间的联系。有效的安全性不能以网络故障为代价。确保您的安全解决方案固若金汤，提供闪电般快速的故障切换，并提供业务所需的吞吐量。

1 不断进步！

一定要坚持不懈！

如果您还没有完全捋清楚，不用担心。只要您对零信任感兴趣，这就是一个好的开始。接下来，选择要实现的元素，您就能最终实现零信任数据中心。一步一个脚印要比停滞不前强得多。**您一定可以做到！**

别忘了还有边缘！

数据是所有安全方案的核心。保护数据中心的秘诀还在于确保边缘安全性能够有效保护对相关数据的访问。确保用户和设备安全访问数据中心环境中的应用和数据，同时更有效地保护整个网络。

JUNIPER NETWORKS

3050187-001-ZH 2023 年 8 月