SOLUTION BRIEF

VERSA NETWORKS

Zero Trust Everywhere: Your Action Plan for a Secure Access Strategy

Author: Brad LaPorte, Gartner Veteran and Advisor to Versa Networks

Introduction

As organizations continue to grapple with the shift towards hybrid work and the widespread adoption of cloud technologies, they are encountering new and complex security challenges. To navigate these challenges, Zero Trust Network Access (ZTNA) solutions have become the go-to strategy for many businesses. This short guide aims to provide the insights needed to choose the best zero trust solution for the reality of today's hybrid – not just remote – workplace and the specific needs of your organization, overcoming the limitations of outdated security measures.

Recognize the limitations of traditional approaches

In a world where cyber threats grow more sophisticated by the day, traditional security measures are falling short. Too many organizations have experienced this firsthand when their legacy Network Access Control (NAC) system and VPN failed to prevent the internal lateral movement of a successful multi-step data exfiltration or ransomware attack, leading to significant data loss. Such failures highlight the risk of relying on perimeter defenses, which are ill-equipped to handle threats in east-west traffic and fail to enforce strict access controls, ultimately resulting in costly breaches. Zero trust approaches challenge the outdated assumption that anything already within the network can be trusted, instead requiring explicit authentication and continuous security monitoring.

Evaluate the extent of "zero trust everywhere" coverage

In the era of remote work and digital collaboration, your network boundaries have dissolved, and the traditional "castle-and-moat" security model is obsolete. Imagine the frustration when employees, who need to work flexibly from various locations, face inconsistent security protocols or access issues. Your graphic designer might be working from home or a coffee shop one day and needs the same consistent and secure access to sensitive marketing materials as they would when they are in the office the next day. Or consider your sales team that requires quick and secure access to the latest pricing databases while visiting clients. Without comprehensive zero trust coverage everywhere, these scenarios could introduce dangerous security gaps or hinder productivity due to overly restrictive access controls.

Therefore, it's crucial to choose a zero trust solution that extends protection uniformly and delivers a seamless user experience, whether your employees are in the headquarters, working from a home office, or on the move. Comprehensive coverage ensures that every access request is fully authenticated, authorized, and encrypted, based on real-time user and device posture assessments — no matter where the request originates. This approach not only plugs security loopholes, but also boosts efficiency and satisfaction.

By selecting a solution that offers expansive zero trust coverage, you can alleviate common pain points such as fragmented user experiences and inconsistent security policies that could otherwise lead to potential breaches or compliance issues. The goal is to enable your workforce to operate smoothly and securely, preserving productivity and peace of mind across all environments.

Prioritize application performance and inline policy enforcement

A seamless user experience hinges on exceptional application performance and robust inline policy enforcement. As a (real) example, a well-known e-commerce company's workforce encountered productivity issues attributed to the slow performance of their cloud-delivered ZTNA solution when accessing internal applications from the office. This scenario exemplifies the pain point of choosing a zero trust solution that can't keep up with performance demands, leading to delays and hampered productivity. It's critical to choose a solution that not only enforces security policies efficiently, but also excels in maintaining application performance.

Consider local resource access and OT/IoT device security

A comprehensive zero trust solution must effectively manage local resource access and secure OT and IoT devices. Manufacturing firms need to protect their production-critical OT devices, which can't accommodate traditional security clients. A robust solution addresses this traditional pain point by enabling device fingerprinting and traffic behavior analysis to safeguard these critical components of the modern enterprise.

Streamline management and optimize cost efficiency

Simplifying security management while reducing costs is a crucial factor in selecting the right zero trust solution. Universities with multiple campuses, for example, face the difficulty of managing different security systems for each location, which leads to increased costs and inconsistent security postures. A zero trust solution that offers centralized policy management and reporting capabilities can streamline administration, reduce costs, and provide consistent security across all locations.

Future-proof your investment

In the rapidly evolving digital landscape, it's essential to choose a zero trust solution that can scale with your organization. Take, for instance, an online media company's growth that is outpaced by its current solution's capacity, causing outages and performance issues. The problem here is a lack of scalability, which can lead to disruptions in service and potential losses. Therefore, it's vital to ensure that the selected solution can adapt to changing demands and accommodate future growth.

Leverage expert guidance

Finally, leveraging expert guidance can be instrumental in the successful selection and implementation of a "zero trust everywhere" solution. Financial services firms often realize the complexity of aligning their existing systems with zero trust principles and seek expert advice. The pain point in this situation is the risk of choosing an unsuitable solution without proper guidance, potentially resulting in wasted resources and time. Industry experts and trusted advisors can provide invaluable assistance in navigating the complexities of zero trust strategies, ensuring a secure and efficient transition for your organization.

Conclusion

In an era where adaptability and vigilance are the cornerstones of cybersecurity, embracing a zero trust approach and applying it across the infrastructure is not just a strategic move—it's a necessity for safeguarding your organization's future. The lessons drawn from the pain points of a multinational corporation's VPN vulnerabilities, a healthcare provider's legacy system failure, and the scalability struggles of an expanding online media company, underscore the urgency of transitioning to a robust security framework. These examples serve as cautionary tales, highlighting the critical need for a zero trust solution that transcends traditional limitations, ensures comprehensive coverage, maintains application performance, and secures both traditional and IoT devices.

The path to robust security is paved with the wisdom of recognizing that the conventional 'castle-and-moat' defenses are relics in our boundaryless digital world. By streamlining management and optimizing cost efficiency, organizations can mitigate the complexities seen in scenarios like the example of the multi-campus university, where disparate systems drained resources and introduced inconsistencies. Future-proofing is not merely an option but a requisite, ensuring that growth and innovation are not stifled by outdated security measures.

A zero trust strategy that works everywhere in the same way is the blueprint for an unassailable security posture that not only protects against the threats of today but also anticipates those of tomorrow. And you are not just fortifying your defenses—you are crafting a dynamic action plan for secure access that is resilient, scalable, and user-centric, and creating a strategic advantage in the digital battleground.

About Versa Networks

Versa Networks is a leading innovator in SASE and SSE. Versa's solutions enable service providers and large enterprises to transform enterprise digital infrastructure to achieve unprecedented business advantage. Versa's carrier-grade cloud-native software platform provides unmatched agility, cost savings, and flexibility, transforming the business of networking. The company is backed by premier venture investors Sequoia, Mayfield, Artis Ventures, and Verizon Ventures.

For more information, visit https://www.versa-networks.com

Follow us on X @versanetworks.