VERSA

WHITE PAPER

From breach to resilience: Eliminating threats through network transformation

Contents

Introduction

Modern software-defined networking (SDN) represents a fundamental shift in how networks are designed, managed, secured, and operated. The transition to a modern software-defined local area network (SD-LAN) presents a significant challenge that continues to impact organizations across all industries. Over time, legacy design decisions, operational constraints, and incremental security requirements have introduced gaps and limitations within network environments, hindering the ability for organizations to evolve towards a cohesive, secure, and scalable network architecture.

In this whitepaper, we'll explore how one manufacturing company was impacted by their legacy network, and how they addressed the challenges of evolving its software-defined network infrastructure to address the demands and requirements of today's modern workloads, its distributed workforce, and constantly evolving security threats.

Company background

A global manufacturing company that is privately owned and has expanded to over 12 manufacturing plants in the past 25 years.

Growth challenges

While recognized as experts in food manufacturing, XYZ Global Manufacturing were not experts in infrastructure technology (IT). With a small staff and a mindset focused on maximizing revenue through up-time of their food processing equipment, their investments in scaling up their business happened quickly and unevenly, as is typical for companies when rapid growth occurs in response to business opportunities.

Within their networking infrastructure, port density requirements doubled nearly every year as they added new equipment onto their manufacturing floors. Their network design relied on a relatively flat Layer 2 (L2) topology using a mix of enterprise and commodity ethernet switching solutions, a self-managed MPLS network, and perimeter firewall appliances to interconnect sites over the Wide Area Network. Despite their planning efforts to design their network for this explosive growth, they could not keep up with the increasing needs which resulted in a fragmented infrastructure spanning across their global sites and corporate offices. This infrastructure created a challenge for the company to understand what devices it was operating, and where they were connected within the network.

In addition to a fragmented network, not all locations were architected with an equal focus on delivering robust network security. Firewall protections were not always consistent between their network segments. At one location, they had a data center firewall deployed. At other locations, there were no firewalls deployed between network segments. This patchwork of network security ensured key systems were protected, but left several other systems exposed and vulnerable to threats.

Security incident & root cause analysis

While the fragmented network design held up and kept the equipment running at maximum efficiency, the perimeter firewalls only protected XYZ Global Manufacturing from outside network threats. Inside the network, it was unrecognized that significant operational security and network challenges were developing that could impact operations. In the past, the company experienced a damaging ransomware attack which exposed critical vulnerabilities in their network infrastructure and network security, as well as their inability to deliver adequate threat identification and containment.

Incident root cause analysis

XYZ Global Manufacturing conducted a thorough triage and post-mortem of the security breach. For example, during the triage of the ransomware event, the CTO of XYZ Global Manufacturing realized his network operations center (NOC) and security operations center (SOC) teams could not see all traffic flows during the incident. The analysis also determined that they could not adequately identify all devices on the network, suggesting that unknown endpoints could have been brought online on the network and associated with the attack.

The root cause analysis report uncovered several key areas with significant shortcomings, which included:

- **Inadequate segmentation:** The flat network architecture based on deployed virtual LANs (VLANs) allowed lateral movement for ransomware once it had breached the perimeter. Their perimeter firewalls were ineffective at stopping threats within the internal LAN network segments.
- **Ineffective perimeter defense:** Existing firewalls, while present, were positioned primarily at the network edge (in the demilitarized zone, or DMZ) and core, failing to provide granular control over internal traffic flows and devices within the network.
- **Policy debt & configuration chaos:** The fragmented network utilized a diverse mix of platforms from different vendors with non-standardized configurations. This lack of consistency created security risks including open ports, weak access control lists (ACLs), and inconsistency between configurations, making troubleshooting and management extremely difficult. Device management also differed across vendors, preventing IT staff from automating key security requirements, such as tracking of individual Media Access Control (MAC) addresses of endpoints.
- **OT/IT convergence complications:** Because IT and Operations (OT) systems were increasingly interconnected for efficiency, the organization struggled to deliver clear separation and appropriate security controls between critical OT environments and traditional IT systems, increasing the attack surface exposed during the incident.
- **Limited network visibility:** There was no comprehensive understanding of what devices were connected to the network, their roles, or their communication patterns. This hindered security monitoring and policy enforcement and lengthened the root cause analysis while devices were identified and cleared from participation in the incident.
- **Failed 802.1X rollout:** Initial attempts to implement 802.1X for network access control faced compatibility issues with legacy switches and were deemed too costly and technically complex to complete.

Separately, XYZ Global Manufacturing identified an additional limitation of their network architecture that they wanted to address with the network architecture transformation:

- **Spanning Tree Protocol (STP) complexity & performance:** The reliance on a large, multi-VLAN L2 domain running STP led to slow convergence times during network changes and performance bottlenecks. For example, the company had a standard Core-Distribution-Access network architecture based on STP which used a single link, limiting network throughput across the LAN.

Versa Secure SD-LAN solution selected for network transformation

This wakeup call deeply affected the business and drove the company's leadership to finally undertake fundamental changes needed to address their legacy network and security shortcomings that had accumulated over the past two decades of infrastructure buildout. XYZ Global Manufacturing evaluated several solutions, and selected Versa Networks Secure SD-LAN to address their network and security challenges. The Versa solution was selected because it allowed them to fully evolve their legacy network architecture, address their past concerns, and prepare for current and future workload and security needs - without impacting their core growth goals in their core food processing business.

Versa Secure SD-LAN capabilities

Versa's SD-LAN solution leverages components and technologies from its Unified SASE solution, such as the Versa Operating System and Director management console, and applies it to deliver modern next-generation network and security at scale for the LAN. By deploying Versa switches in a software-defined fashion from the Versa Director, XYZ Global Manufacturing was able to rapidly and securely employ several modern SD-WAN capabilities made available through the solution:

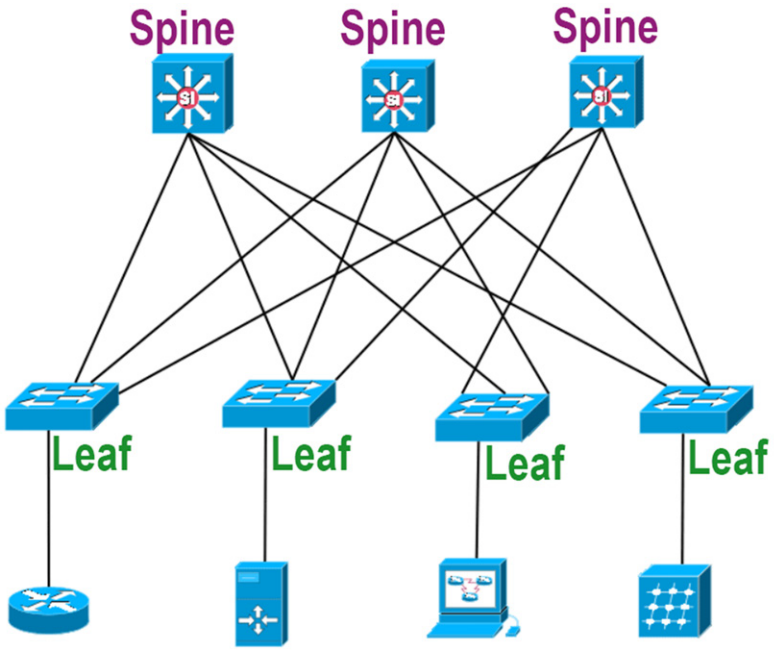
- **Switch configuration & standardization:** Versa's template workflows provide consistent, repeatable switch configurations. The Director management console delivered precise visual details of all ethernet ports, complete with layer2 and layer3 information for each port including descriptions and firewall zones.
- **Zero-Trust Provisioning & secure management:** Each Versa switch can be configured and updated using Zero Trust Provisioning (ZTP) from the Director management console to accelerate network deployments across plants, and to standardize configurations and updates as new network or security mandates are identified, architected, and released.
- **802.1X secured ports:** Versa switches support full stack 802.1X port-based network access control with supplicants that authenticate agents and devices before they are granted network access. XYZ Global Manufacturing also connected the Versa switches to their corporate identity provider (IdP), to ensure all agents and devices were properly managed and visible to the NOC and SOC teams, and to block all non-company devices that were not vetted and aligned with company security policies.
- **LAN firewall:** Versa switches offer firewall capabilities that blocks malicious traffic as close to the client as possible, giving XYZ Global Manufacturing greater security control over their network in the event of a future internal network incident or insider threat.
- **Zero Trust Network Access (ZTNA):** Versa ZTNA provides additional security mechanisms across users and devices that want access to the network, qualifying them and evaluating their security posture prior to granting network resource access. Knowing the user, type of device, and the device's real time posture gives XYZ Global Manufacturing more visibility and control over their network and who has access to it, and under what terms.
- **Comprehensive analytics:** Versa Analytics delivers real-time visibility into traffic flows of users, devices, applications and systems. This allowed XYZ Global Manufacturing to build reports, perform audits, forecasts, and make more insightful decisions in near real-time.

Network & security posture benefits realized from the SD-LAN solution

After deploying the Versa SD-WAN solution to its plants, XYZ Global Manufacturing identified additional benefits to its network and security posture as a result of the implementation. These were identified as follows:

- **Macro-segmentation**: Evolving their firewall from only perimeter-based security to Versa's Next-Gen Firewall (NGFW) technologies allowed XYZ Global Manufacturing to more vigilantly monitor and control traffic within and between various IP subnets within the networks of its plants and data center. Versa's NGFW capabilities delivered advanced port, IP, and application awareness, contextual security based on identities, with deep packet inspection to ensure data threats were quickly identified, blocked, and contained from infecting other parts of their internal network.

- **Micro-segmentation:** Expanding NGFW technologies further, XYZ Global Manufacturing implemented Security Group Tags (SGT) to label and enforce traffic between hosts in the same subnet. This provided additional safeguards to ensure undesired traffic was blocked as close to the host as possible, further limiting potential threats to reach beyond the initial target system. When combined with further network security policies implemented at L4-7, XYZ Global Manufacturing had complete control of all traffic across the network.
- **Configuration harmony:** By defining network-wide common configurations (VLAN, WAN, LAN) using templates, administrators reduced the configuration chaos caused by intensive manual CLI configuration on individual devices, saving significant time, reducing gaps, and eliminating technical limitations and inconsistencies between disparate network appliances. Delivering consistency to the network ensured that the company was protected across all points of access, regardless of whether it was at the perimeter or within the network.
- **Physical port visibility & control:** Having a standard switch configuration template across the enterprise also helped ensure that every single unused port was disabled until needed. Unused ports represented attack surfaces that could be used by insider threat actors or contractors to breach the network. Disabling all unused ports guaranteed that physical access to the network was protected at all times. This also validated the physical separation requirement between IT and OT, since disabling unused ports ensured IT staff could not cable a connection between the two distinctively separate spaces and create an entry point for a threat to propagate.
- **Complete visibility:** With the Versa SD-WAN solution, XYZ Global Manufacturing achieved its goal of gaining network visibility across all sites, devices, and traffic flows. With detailed logs of activity captured by Versa Analytics, including encrypted traffic, they can now pinpoint any activity and source quickly and conclusively.
- **True full-mesh network:** Standardizing on Versa switches allowed XYZ Global Manufacturing to architect a modern two-layer leaf/spine topology and fully utilize the underlaying LAN network and eliminate shortcomings from their traditional network architecture based on STP including limits to bandwidth and single points of failure. Transitioning to this modern network topology ensured that maximum bandwidth could be achieved for their data center and modern application needs, ensuring full utilization of their networking investments. In addition, the SD-LAN was now able to integrate with SD-WAN using multi-protocol border-gateway-protocol (MP-BGP) to deliver a true global network solution across all plants managed by a single vendor and management plane.



Summary

It took a painful event for XYZ Global Manufacturing to realize it had to evolve its legacy network to meet the demands and requirements of today's modern workloads, its distributed workforce, and constantly evolving security threats. By partnering with Versa Networks to deploy the Secure SD-LAN solution, XYZ Global Manufacturing gained greater security and control over its network, including across all layers and protocols, and across all points of entry both internal and external. With a dynamic, policy-driven, zero-trust approach enforced at the endpoint, they were able to provide their NOC and SOC teams much more granular control, consistent enforcement, and better visibility, while also significantly reducing the attack surface related to lateral movement and endpoint access. Further, delivering the Versa SD-WAN solution through zero-touch provisioning allowed XYZ Global Manufacturing to standardize, simplify, and accelerate deployments. They achieved improved overall network performance and resiliency, eliminated years of gaps and limitations that had been built up around their prior network infrastructure deployments, and more quickly realized their return on investment to achieve their network and security goals.

Versa Networks, Inc
2550 Great America Way, Suite 350
Santa Clara, CA 95054
Tel: +1 408.385.7660
Email: info@versa-networks.com
www.versa-networks.com

About Versa
Versa, a global leader in SASE, enables organizations to create self-protecting networks that radically simplify and automate their network and security infrastructure. Powered by AI, the VersaONE Universal SASE platform delivers converged SSE, SD-WAN, and SD-LAN solutions that protect data and defend against cyberthreats while delivering a superior digital experience. Thousands of customers globally, with hundreds of thousands of sites and millions of users trust Versa with their mission critical networks and security.

Part# WP_SDLANSEC-01.0