NETWORK INFRASTRUCTURE ON THE FRONT LINE

Threat actors continually develop new strategies and techniques in order to maximize the impact of their attacks while avoiding cybersecurity defenses. Over the past several years, attackers have found a new class of targets that fits the bill on both fronts—enterprise network infrastructure devices.

VPNs, switches, firewalls, routers, and a wide range of traffic concentrators, gateways, and delivery controllers have all been heavily targeted by ransomware groups and nation-state threat actors. Ironically, many of the same devices trusted to protect the enterprise are themselves now the first point of attack.

To mitigate this risk, security teams and leaders need to understand the driving factors behind these changes in the threat landscape, how attackers target and abuse network devices, and the best practices for protecting these critical assets. In this paper, we will dive into the details of network device security based on the most current analysis from attacks in the wild. We will cover the how and why of modern attacks as well as specific requirements and best practices that can keep enterprises safer. Specifically, readers will be able to learn the following:

- The Rise of Network Devices In Modern Attacks
- Why Network Devices Are Being Targeted
- The Critical Role of Network Devices and Firmware in Zero Trust
- Key Requirements for Protecting Network Devices
- How Eclypsium Can Help Protect Network Devices

With this information, security leaders and practitioners can identify where they may have gaps in their existing security program and determine how to take corrective action.

THE RISE OF NETWORK DEVICES IN MODERN ATTACKS_

The rise of attacks on enterprise network infrastructure has been one of the most significant cybersecurity developments in the past several years. Beginning in 2019, industry observers began to see a growing pattern of threat actors targeting vulnerabilities in enterprise devices such as VPNs. By early 2020, a CISA alert warned that vulnerabilities in Citrix and Pulse Secure VPNs had already become one of the top targets of APT groups. In the following months, cybersecurity

agencies issued repeated alerts detailing how Russian, Chinese, and Iranian state-based threat actors were targeting a variety of enterprise network devices and vendors.

This would prove to only be the start of a much larger trend as more nation-state and ransomware-based groups adopted the same techniques and expanded to target a wide range of leading enterprise network and security vendors including F5, Fortinet, NetScaler, Palo Alto Networks, SonicWall, VMware, and many others. By the end of 2021, dozens of ransomware families and virtually all of the most damaging ransomware operators were using network devices as part of their attack chain. The widespread success of these attacks led to even more threat actors, discovering more vulnerabilities, and targeting more vendors and asset types. Some recent attacks at the time of writing (September 2023) include:

- **Volt Typhoon and Attacks on Fortigate Devices** - A state-based Chinese threat actor known as Volt Typhoon exploited Fortinet security devices to gain initial access to critical infrastructure targets in the U.S. Researchers have identified the threat actor targeting CVE-2022-40684, related vulnerabilities as well as additional threat actors exploiting CVE-2022-42475.
- **Multiple Attacks on Cisco Appliances** - The Russian threat group APT28 developed a new malware dubbed JaguarTooth that collected and exfiltrated device information over TFTP, and provided attackers with unauthenticated backdoor access. It was observed being deployed via exploitation of the SNMP vulnerability, CVE-2017-6742. Cisco has also been targeted by Akira and Lockbit. ransomware operators.
- **BlackTech Modified Firmware on Network Routers** - The NSA and CISA issued a joint advisory warning of attacks by the Chinese group BlackTech on various types of network routers that took several steps to evade detection and maintain persistence.
- **LockBit Attacks on Network Devices** - LockBit is one of the most prolific and widely-deployed ransomware families. And like other popular ransomware, LockBit heavily targets network devices in order to gain initial access into organizations, specifically targeting F5 BIG-IP devices, Cisco, and Fortinet's FortiOS-based devices.
- **Barracuda Email Security Gateway (ESG)** - Researchers recently identified a global operation targeting Barracuda ESG appliances. These attacks exploited CVE-2023-2868, which is a vulnerability in the firmware of physical Barracuda appliances. After gaining access, the threat actor uses the position to perform espionage and steal data.
- **Mass Exploitation of NetScaler Appliances** - In an attack attributed to the ransomware group FIN8, the attackers set up infrastructure for a mass exploitation campaign that outpaced defenders' ability to patch since the update was released just days earlier. They reached 6% of vulnerable NetScaler devices, nearly 2,000 systems, in a matter of days. The attackers installed webshells that persisted even after the embedded OS was patched and rebooted.
- **Fortinet Devices Targeted** - The Akira ransomware group was discovered to be exploiting flaws in Fortinet VPN appliances including using a Python tool that chained vulnerabilities together.
- **Ransomware Attacks on BMCs and Data Centers** - Researchers recently identified ongoing attacks targeting Cloud Service Providers (CSPs) and Managed Service Providers (MSPs), specifically by targeting remote management and out-of-band management components such as BMCs and IPMI. Ransomware operators have also been observed targeting data centers and exploiting BMCs as a method for maintaining persistence.

WHY NETWORK DEVICES ARE BEING TARGETED_

Network devices have become one of the top initial access vectors for ransomware operators and other threat actors. In short, these critical assets are often poorly defended, yet provide extremely high value to attackers. Network devices are often overlooked by vulnerability management programs, and most organizations have virtually no tools for detecting threats and compromises of these devices. However, if these assets are compromised, their natural interconnectivity can be exploited to gain unfettered access to an enterprise and its assets.

Initial Access and Lateral Movement

Naturally, network devices often must be accessible in order to serve end users and allow technical teams to manage the device. However, this can also leave devices exposed to exploits from external attackers. Any exposed vulnerabilities in network devices can provide attackers with a strategic foothold into an enterprise without the need for phishing or other user-dependent infection methods.

This has made network devices a top priority for Initial Access Brokers (IABs) who specialize in gaining access to enterprise networks, which they then resell to other criminal threat actors. In response to the spike in attacks, the U.S. government issued Binding Operational Directive 23-02, which requires that all federal civilian executive-branch agencies take measures to protect management interfaces for network devices and BMCs. This includes ensuring that these critical interfaces are not directly exposed to the Internet and are protected by Zero Trust access controls.

Once compromised, network devices can play a devastating role in the subsequent phases of a cyberattack. As the central nervous system of an enterprise, network devices are naturally connected to almost everything else within the organization, making them ideal for lateral movement and persistence.

For example, they can provide a path to end-user devices, allowing attackers to deliver additional malware and payloads. Likewise, network devices can be used to pivot to other connected internal assets. Their networking capabilities can be abused to allow attackers to monitor, copy, or redirect traffic. Depending on the device, attackers can alter DHCP settings or perform DNS poisoning in order to direct users to malicious sites or to establish a machine-in-the-middle.

Compromising network infrastructure can also break the boundaries between IT/OT and other high-value areas of the enterprise. Attackers can also simply “brick” network devices in order to cripple enterprise operations.

Gaps in Vulnerability Management and Threat Detection

Network devices and BMCs are different from most enterprise assets. They don’t run standard commodity operating systems, and thus, don’t support standard security tools such as EDR. Instead, they rely on specialized code that is almost entirely defined in the supply chain. For example, network devices run custom integrated OS/firmware that is unique to each vendor. These are often full-fledged operating systems based on Linux or BSD, such as F5 TMOS, Cisco IOS, Citrix Netscaler OS, Fortinet FortiOS, etc. BMCs likewise run on their own separate integrated hardware and firmware that is fully independent of the host hardware and OS.

The resulting lack of standard endpoint security not only leaves these assets more open to attack, it also makes it far harder for security teams to detect when a device has been compromised. Even laptops are increasingly targeted at the level of supply chain components and integrated code that lives below the level of the operating system. But network devices and BMCs are at an even much greater risk because organizations have limited visibility and control over what is going on in the devices themselves. Mandiant reported that the APT group UNC3524 persisted undetected in victim networks for at least 18 months by tunneling through compromised network devices.

The reliance on specialized, low-level code also introduces challenges for vulnerability management. The assets themselves are often not part of the regular vulnerability scanning process, which typically focus on commodity laptops and workstations. The low-level nature of the code means that vulnerabilities can be hard to see even when organizations know to look for them. And once problems are found, updates are often slow due to the challenges of taking critical devices offline. Together this means that network devices and BMCs are a great place for attackers to go looking for exploitable vulnerabilities.

Complex Supply Chains and Custom Code

Network devices are highly sophisticated and complex assets. And this means they have highly complex supply chains. A network device can have over 100 internal components, which are often provided by outside suppliers and subsuppliers. Each component can have its own software, firmware, and related vulnerabilities. System-level firmware within a device is the first code to run and some of the most privileged code in any device. Compromise of any of these critical components can give an adversary a highly stealthy way into an organization.

The complexity of the supply chain also means there are more opportunities for an adversary to attack. While the main vendor may be well-defended, attackers can target dozens of suppliers in order to compromise components and insert malicious code upstream, before the component is ever delivered to the final manufacturer. Update mechanisms have also proven to be highly popular supply chain vectors. Like all code, firmware and device code needs to be regularly updated. By either compromising or finding weaknesses in update mechanisms, attackers can deliver malicious code within the guise of valid updates. This has consistently proven to be one of the most common vectors of supply chain attacks.

Zero Trust Depends on the Integrity of Network Devices

Network and security devices occupy a uniquely critical role in any Zero Trust architecture. In many cases, they *are* the devices that deliver and analyze traffic and ultimately enforce Zero Trust policies. With the rise of attacks on these devices, attackers are looking to undermine the technologies that quite literally define an organization's Zero Trust strategy.

These organizations must be able to "trust" that what a switch says is on the wire is actually what is on the wire. They must be able to trust a firewall or IPS to accurately analyze traffic and block threats or unauthorized access. They must be able to trust that traffic remains confidential and is only sent to the intended destination.

Most organizations implicitly trust these devices to do their jobs. However, Zero Trust challenges security teams to seek out the areas of implicit trust in their IT and OT stack. Given the foundational role of network devices in Zero Trust, it is imperative that teams verify the integrity of these devices.

KEY REQUIREMENTS FOR PROTECTING NETWORK DEVICES_

Network device security requires organizations to extend their security best practices and operations to a new class of devices. However, traditional security tools are designed to protect commodity operating systems and software and fail to address the unique risks and threats tied to the tightly integrated device code, firmware, and hardware of network devices. This leads to a "risk gap" where some of an organization's most high-value devices receive the least protection.

The following requirements can help security leaders, architects, and practitioners to address this gap and ensure that their network devices receive the protections and operational rigor that they deserve.

Supply Chain Verification

An organization's security practice should begin even before a network device is physically or virtually delivered. Security teams should scan prospective network devices for vulnerabilities and misconfigurations as a standard part of the evaluation process during the vendor selection phase.

Modern technology supply chains are constantly changing as manufacturers seek to lower costs or address supply shortages. To keep pace with these changes, enterprises should require that their vendors provide an up-to-date software bill of materials (SBOM) that includes all device software and firmware. Teams should scan newly received devices to verify that the actual code in the device matches SBOM and is free from vulnerabilities.

Supply chain problems can also occur after a device is deployed due to mistakes or threats introduced during updates. Network devices should be scanned and monitored after an update to ensure that all security settings are properly enabled and to detect any anomalies or signs of a threat.

Integrity Monitoring and Threat Detection

Security teams must be armed to proactively identify any active threats or signs of compromise. This can take a variety of forms when applied to network devices. First, teams should verify the integrity of the device's firmware and code by cryptographically comparing the actual code on the device to the valid, published code supplied by the vendor. This whitelisting approach is a powerful first step since the firmware on a device remains far more stable and predictable than other code on a more traditional device.

Next, teams should scan for the presence of known threats or signs of compromise, such as changes in firmware and OS binaries, modified configuration and backup files, and the presence of reverse shells and persistence modules.

Attackers regularly reuse and repurpose components of previous threats when developing implants and backdoors. In-depth scans of devices will be important as many threats make subtle configuration changes to a device that may not be immediately apparent.

Lastly, organizations should be able to monitor the behavior of the code on the device. Firmware, once again, is far more predictable than traditional software and will conform to relatively narrow types of behavior. Deviations from this baseline can help staff to identify signs of threats even in the case when the threat is unknown or has been introduced as part of a valid vendor update.

Automated Discovery and Visibility

Organizations must have visibility of their network devices, and when possible, have visibility into their internal components. This can be a challenge as most enterprises will have large numbers of network devices, which typically do not support traditional security agents.

As a result, organizations should have tools that automatically discover network devices anywhere in a distributed enterprise without the need for an agent to be deployed on the network devices themselves. Any discovery process should be tightly controlled to protect user privacy and ensure that non-corporate environments are not inadvertently analyzed.

Ongoing Vulnerability and Risk Management

Security teams must have proactively visibility into the security posture of their network devices. This will include the ability to scan for vulnerabilities and device misconfigurations unique to network devices. Many firmware-level vulnerabilities will not be detected via simple unauthenticated vulnerability scans. As a result, teams will need to use tools to support authenticated scans whenever possible. If a device cannot support regular authenticated scans, teams will need to be able to fingerprint devices and collect data via alternate methods such as APIs in order to identify vulnerable devices.

Teams should also strive to establish a vulnerability management program that is consistent across its many vendors and device types. Most enterprises will have multiple network and security vendors, and relying on periodic, vendor-specific scans will quickly lead to teams missing critical risks. An automated, vendor-agnostic approach is critical to ensure comprehensive and reliable visibility of the attack surface.

Security teams should ensure that they have the right tools and processes in place to prioritize network device vulnerabilities when they are detected. Teams may want to consider dedicated views of network devices to ensure vulnerabilities aren't missed in the thousands of vulnerabilities detected during a traditional network-based scan. Teams should also be able to automatically prioritize the CVEs that are actively being exploited in the wild.

Device Patching and Updating

Teams will need to be able to quickly address any vulnerabilities with as little effort as possible. Teams may want to consider tools that can automate many of the manual steps of an update such as checking for new firmware versions, downloading and verifying the appropriate packages, and even applying the updates themselves.

Separation of Data and Control Plane

NIST's SP 800-207 extensively covers the importance of maintaining a logical separation between the data and control planes within a Zero Trust architecture. In the case of a network device, the control plane provides an independent path for administrators to manage the device, update policies, and manage other configurations, while the data plane serves application traffic between endpoints. By separating the control plane, the organization can limit access to devices and apply stringent controls to ensure that any policy changes are valid and authorized.

However, while the data plane and control plane can be logically separated on a network device, they will often share the same underlying firmware. Thus a compromise to the firmware would allow an attacker to gain access to both planes. Even when devices have separate physical firmware, such as in a server baseboard management controller (BMC), research has shown how a compromise of either the data or management hardware can allow an attacker to pivot to the other. Once again this highlights the critical importance of verifying the posture and integrity of all firmware and device code on network devices.

NETWORK INFRASTRUCTURE HAS A SUPPLY CHAIN SECURITY PROBLEM

CISA Director Jen Easterly put it well when she wrote that organizations should expect IT products to ship securely by default. "We've normalized the fact that technology products are released to market with dozens, hundreds, or thousands of defects, when such poor construction would be unacceptable in any other critical field," said Easterly.

That ransomware groups and APTs are seeing so much success targeting network infrastructure gear indicates a supply chain security problem with enterprise IT infrastructure in general. IT and security practitioners cannot blindly trust all manufacturers to ship these network appliances without vulnerabilities and to have well established and secure update processes. Instead, defenders need to anticipate and control the supply chain risk. The old approach of network scanning alone is neither effective nor sufficient, as security operations teams are overwhelmed and can't keep up with constant patching of critical IT infrastructure.

INTRODUCTION TO ECLYPSIUM_

Eclypsium helps organizations build trust in their IT infrastructure, including network infrastructure, by providing simple, automated security for low-level hardware, firmware, and software components of assets. Organizations can assess the risk of products during the procurement stage, validate the integrity of those assets upon receipt, and then continuously monitor and remediate risk in production. With the Eclypsium supply chain security platform, security teams have full visibility and control over their networking infrastructure without the need to install agents on the devices themselves. Key capabilities include the ability to:

Inventory_	Harden_	Detect & Respond_
Know what is in your environment	**Identify and mitigate risk**	**Fill a critical gap in your detection program**
• Track assets in production • Correlate vulnerabilities, components, products, and assets • Compare products from different vendors before purchase	• Assess exposure to new vulnerabilities • Find insecure configurations • Track compliance issues • Automate firmware updates	• Detect threats that are not covered by EDR • Set baselines for firmware integrity • Quickly respond to supply chain incidents • Send data to SIEM and SOAR for correlation

LOOKING FORWARD AND NEXT STEPS_

Network devices continue to be one of the most active areas in cybersecurity. The landscape has evolved quickly over the past months and all indications are that attackers will continue to accelerate their attacks on network devices. Large-scale ransomware and financially-motivated groups have adopted the techniques previously proven by APT threat actors and continue to operationalize them at an unprecedented scale. Initial access brokers (IABs) continue to identify and exploit new vulnerabilities as they seek to gain a competitive advantage over competing criminal groups.

At Eclypsium, we are dedicated to driving the industry forward with security research and controls to ensure that these critical devices remain as safe as possible. Our platform gives security teams the tools they need in order to keep their fleet of network devices as safe as possible.

To learn more about how Eclypsium can protect your organization, please contact us at info@eclypsium.com.