Solution Overview

Trend Vision One™ – Network Security

Detect the unknown, protect the unmanaged

Network Security is More Relevant Than Ever

Your network is the foundation of your IT environment, acting as the fabric that connects users, applications, customers, and overall operations. In turn, your network is foundational for effective cybersecurity strategy, as assessing the cyber risk of your environment across all layers and defenses relies on the cyber health of your network.

According to **Verizon's 2023 Data Breach Investigation Report,** phishing makes up 44% of social engineering incidents. Unfortunately, it doesn't stop at the mailbox or endpoint. Insecure networks can then be abused to spread malware throughout your environment making the situation worse.

Network security has long been thought of as a silo of deeply technical tools, often saddling both network and security operations. With the rise of extended detection and response (XDR), a new opportunity is presented where such tools can effectively sit in both camps– delivering rich detection telemetry to advanced platforms and affecting response orchestrations, without sacrificing network performance or introducing complexity.

This combination is critical as we consider XDR as a subset. To effectively mitigate cyber risk across your entire environment both are needed. Only tightly integrated sensors and platforms across endpoints, email, cloud applications, and networks can deliver this.

Trend Vision One – Network Security

As a part of our Trend Vision One™ cybersecurity platform, Trend Vision One – Network Security delivers powerful network security capabilities that detect unknown cyber assets and protect unmanaged entities in your environment. Unlike point solutions that leave gaps in between siloed products, Network Security combines risk analysis and XDR methodologies with Trend Vision One. Your team can seamlessly surface events and orchestrate the response actions across the entire network fabric–alongside other sensors such as endpoint and email.

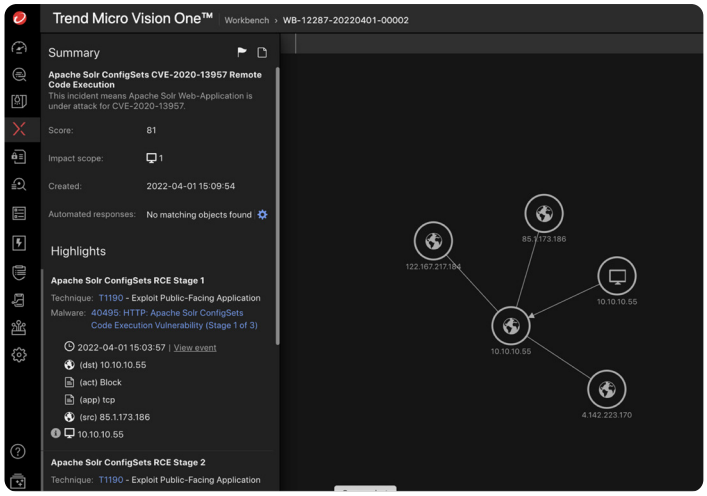
FORRESTER®
WAVE LEADER 2023
Network Analysis And Visibility

Network Security Focuses on Three Key Areas:

1. Enterprise Network

The nature of networks is changing, with control of the network fabric used to connect assets together becoming more dynamic and often less controllable. The enterprise network focuses capabilities on these new challenges in places such as public clouds (IaaS) while continuing to provide strong protection for the more well-known challenges of operating a network in the data center.

ise network begins on the strong base of vulnerability-based protection that can be performed in real-time, at line rates. Through Trend Vision One, the network telemetry from an enterprise network sensor is then analyzed alongside other sensor telemetry to surface actionable information. Tying this together is the seamless sharing of dynamic threat intelligence to provide protection at all stages of a threat's lifecycle through the network.

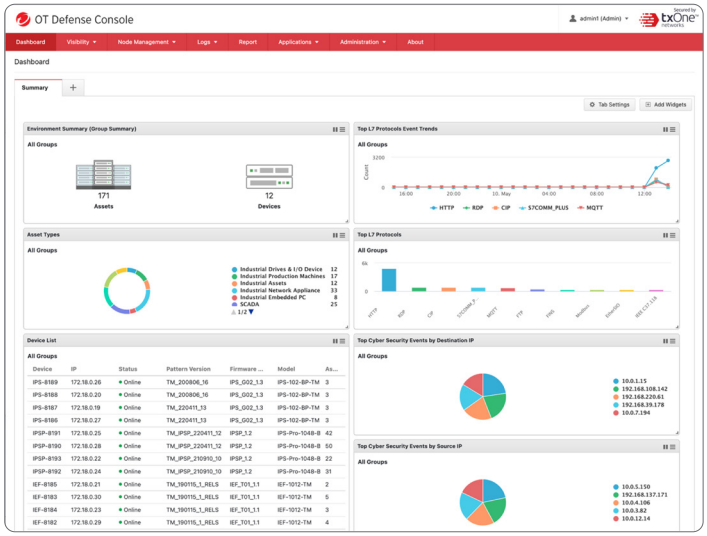


As is the nature of many networks though, standalone operations using best-of-breed technologies is a common use case where Enterprise Network continues to excel. When high performance, highly accurate network protections are needed and tight scrutiny may limit the use of SaaS solutions, you can rest assured that industry-leading capabilities are available and ready to protect your organization.

2.ICS/OT Network

Operational Technology, which includes industrial control system (ICS), communication infrastructure, and the industrial internet of things (IIoT) spans wide, requiring specialized protection. As an example, an MRI machine must be regularly updated to patch vulnerabilities. But patches are not always available, or the machine does not allow for timely updates. IIoT security can provide non-intrusive coverage until a permanent fix can be applied, leaving the organization's risk posture stronger through mitigating controls.

These types of scenarios equally apply to industrial shop floors, connected cars, private 5G networks and critical infrastructure, where downtime must be avoided. With an ICS/OT control in place, updates can more safely be incorporated into regular maintenance cycles and security posture improvements without unacceptable impacts to plant operations.

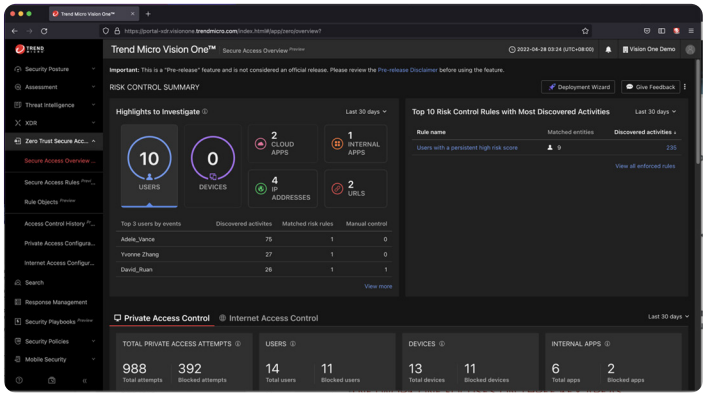


3. Secure Access Service Edge (SASE)

SASE, and industry names for similar capabilities like Security Service Edge (SSE) and Zero Trust Edge (ZTE), all drive towards the re-envisioning of trust as a part of a zero-trust architectures and methodologies.

The zero-trust methodology flips the concept of trust to assume that devices and users are untrusted until proven 'all clear'. SASE introduces continuous assessment for users and devices, automatically altering or revoking permissions dynamically if the nature of the connection or risk profiles change. With this capability, the security analyst benefits from significantly improved contextual information, and an automated solution to maintain security at the network connection level.

This risk evaluation and visibility capability is surfaced in Trend Vision One, leveraging Risk Insights and XDR. SASE components gather telemetry and limits the activity of suspicious and nefarious attempts to circumvent point product controls and the gaps that exist within them.



Building the Network Security Foundation

In the rapidly changing digital world we operate in, it is required that security strategies include the network not as a silo, but as an innate and essential component in proactive protection. As network boundaries continue to blur, protections will benefit from the underpinning network understandings being applied in new ways including in cloud environments, service edges, and organizational application edges.

As existing network controls are assessed, a view of how your organization's assets, applications, and users will interact with one another will drive projects that provide more streamlined, higher performance, and more secure connectivity. For these projects, the availability of detection and response, adoption of IoT and connectivity of OT, and workforce office locations should be contributing factors when determining how best to manage cyber security risk.

North-South, East-West Detection and Response

Enterprise network capabilities provide a strong base to block known, unknown, and undisclosed threats and monitor network segmentation implementations, reducing the blast radius if a breach does occur. Network Security offers layered and early warning defenses to protect the environment from high risks such as unmanaged endpoints–which, when compromised, spreads to higher-value managed targets. This visibility and active response capabilities help ensure that if an incident does occur, it will not cripple the entire business.

The Right Protection in the Right Place

Organizations who conflate IT and OT protection under the same product capabilities often find one or the other lacking. This is not because the products are not feature-rich and capable, it's just the nature of the infrastructure is simply different.

Taking these specially tuned, simplistically designed tools that focus on advanced security problems without disrupting business operations is a guiding principle for this capability area. Network Security and TXOne Networks allow security teams to easily take a holistic view of the entire organization across IT and OT zones, building confidence that your business is well protected and built on a solid foundation.

As Workforces Change, Maintaining Protection is a Challenge

Across the diverse network landscape, the concept of a network boundary is becoming more blurred. Existing network security capabilities can no longer provide the complete protection needed to allow access to internal network resources from users outside its boundary–because the boundary is gone. The new architecture based on zero-trust methodologies is effective but should not be viewed as a silver bullet to solve all challenges that have arisen from a shift to remote workforces.

While organizations should move towards a zero-trust strategy, early projects in this space should focus on tactical problems being faced, such as VPN overload, unsanctioned app usage, and performance issues related to network doglegs. By completing such projects over time, the journey towards zero trust becomes achievable, with meaningful security improvements along the path.

Bringing Information to the Surface to Focus Efforts and Provide Automated Action

The network sees a lot of data, including any data that is not entirely self-contained within an endpoint. Even though this data can be a source of increased visibility and context for events, the sheer volume of data would leave security teams overwhelmed. This is where XDR comes into play.

XDR ingests data from across the environment and distills it down to critical events. With network telemetry included, Trend Vision One delivers insights far beyond the limitations of endpoint detection and response (EDR) by enriching other sensor data with network context. Bringing this network telemetry to XDR can feel like a complex and expensive undertaking, even in smaller networks. Network Security combats this problem by making smart decisions on what data should be sent, and how much context is needed for it to be actionable.

Network Security, as part of our Trend Vision One cybersecurity platform, delivers intelligent detection and powerful response capabilities. As your organization migrates from point solution-based security to an XDR focus, greater resiliency against new vulnerabilities and threats will be seen and risk management-focused security strategy will be within reach.