SOLUTION BRIEF

Fortinet and Astelia Preemptive Exposure Management Solution

Eliminate Vulnerability Noise

Executive Summary

Fortinet and Astelia have partnered to provide a preemptive exposure management solution that helps organizations quickly identify and remediate the 1–2% of vulnerabilities that are both reachable and exploitable. By combining Astelia's network mapping and vulnerability analysis with Fortinet FortiGate Next-Generation Firewalls (NGFWs), the solution delivers evidence-based vulnerability classification and actionable remediation guidance beyond patching.

The Challenge

AI is accelerating vulnerability growth and collapsing time-to-exploit, leaving organizations buried under "critical" risks that don't translate to real-world exploitability. Traditional scanners and exposure management solutions fall short because they depend on probability-based scoring and incomplete external context.

Joint Solution

Fortinet and Astelia combine FortiManager and FortiGate control-layer visibility with Astelia's reachability and exploitability engine to identify vulnerabilities that truly matter. Using read-only API access, Astelia ingests NAT policies, firewall rules, and configurations at scale without disrupting operations. Agentic AI determines each CVE's technical requirements, highlighting the vulnerabilities that are both reachable and exploitable, and recommending remediation paths beyond patching. The result: no more endless tickets, no wasted effort, just accurate, efficient, and actionable exposure management that unites security and IT teams.

Solution Components

Astelia Preemptive Exposure Management Platform

Astelia identifies reachable, exploitable vulnerabilities by correlating network topology with agentic vulnerability analysis. Using read-only API integrations, it models and maps an organization's network environment and evaluates each CVE against its technical exploit requirements to determine true risk. Astelia leverages compensating controls to recommend practical remediation paths beyond patching, enabling security and IT teams to reduce exposure when patching isn't feasible.

Fortinet FortiManager

FortiManager revolutionizes network management and security operations by automating routine tasks and acting upon intelligent insights. It accelerates zero-touch provisioning with best-practice templates for deploying hybrid mesh firewalls, SD-WAN, and SD-Branch.

Fortinet FortiGate

FortiGate NGFWs protect data, assets, and users across today's hybrid environments. Built on patented Fortinet security processors, FortiGate NGFWs accelerate security and networking performance to effectively secure the growing volume of data-rich traffic and cloud-based applications.

Solution Components

- Fortinet FortiManager and FortiGate NGFW
- Astelia Preemptive Exposure Management Platform

Solution Benefits

- **Focus on real risk** by identifying the 1–2% of vulnerabilities that are truly reachable and exploitable in your environment.
- **Save time and costs** for both security and IT teams by eliminating false-positive vulnerabilities.
- **Gain full visibility** into reachability and exploitability for every scanned vulnerability.
- **Remediate faster and smarter** with actionable guidance that goes beyond patching, including firewall rule updates and other compensating controls.
- **Unparalleled security protection** using the Fortinet Security Fabric.

FORTINET FABRIC-READY

Solution Integration

Astelia integrates with FortiManager and FortiGate via read-only APIs to ingest network control-plane data, including firewall policies and NAT rules. This data is used to construct an accurate model of the effective network topology and traffic flows. Astelia then correlates this model with the exploit prerequisites and attack paths of each scanned CVE, analyzed using agentic AI. The result is an evidence-based determination of the 1–2% of vulnerabilities that are both reachable and exploitable, accompanied by actionable remediation guidance that extends beyond patching to include firewall policy modifications and other compensating controls.

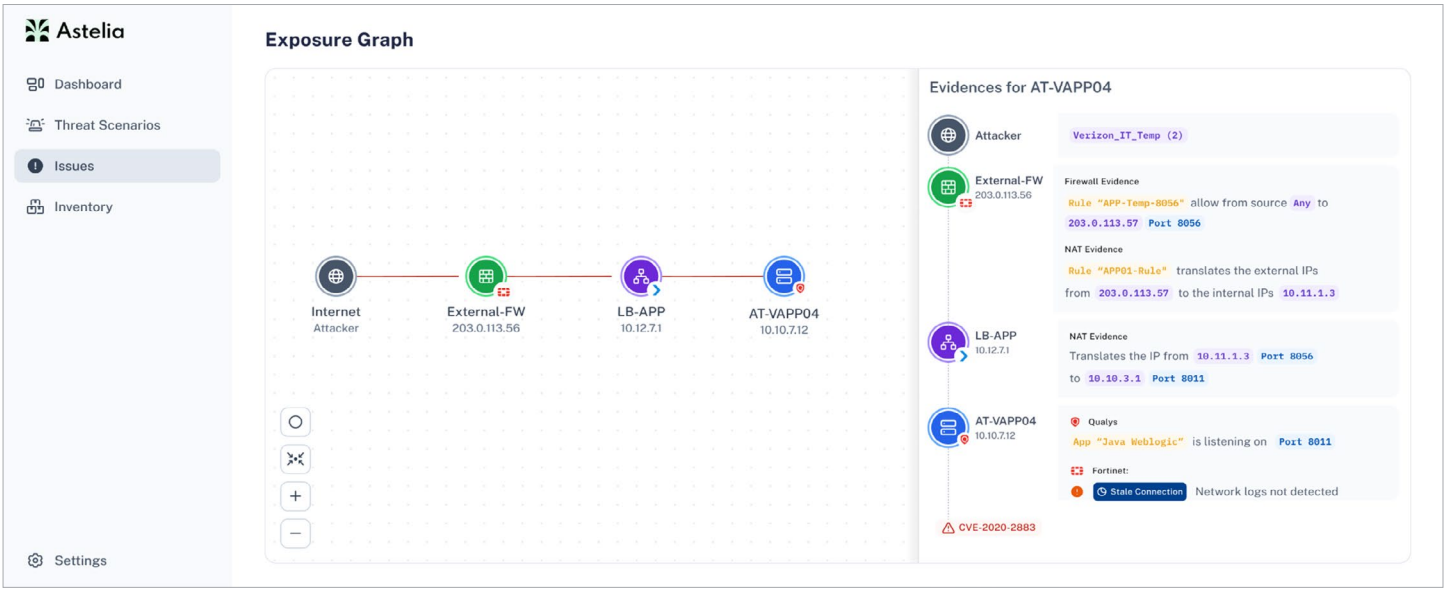

Figure 1: CVE reachability and exploitability analysis based on Astelia and Fortinet

Joint Use Cases

Use case #1: Eliminating non-reachable vulnerabilities

Astelia pulls configuration data, NAT rules, and firewall policies from FortiManager via read-only APIs and correlates them with CVE requirements to assess true reachability. For example, if an exploit depends on an unexposed port, security teams can remove it from their backlog and focus on genuinely exploitable vulnerabilities.

Use case #2: Identifying unscanned external assets

Astelia uses FortiGate and FortiManager configuration data to model network behavior, map traffic flows, and identify externally exposed assets. This “inside-out” approach uncovers assets often missed by vulnerability scanners, giving security teams actionable insights to remediate misconfigurations, enforce access controls, and reduce network exposure.

About Astelia

Astelia is a cybersecurity company founded by former leaders of the Israeli National Red Team, combining deep offensive and defensive expertise with firsthand understanding of how vulnerabilities are actually exploited. Using proof-based reachability analysis, Astelia enables organizations to identify the 1-2% of reachable vulnerabilities in their environment and choose from multiple remediation paths.

About Fortinet

Fortinet (NASDAQ: FTNT) is a driving force in the evolution of cybersecurity and the convergence of networking and security. Our mission is to secure people, devices, and data everywhere, and today we deliver cybersecurity everywhere you need it with the largest integrated portfolio of over 50 enterprise-grade products. Well over half a million customers trust Fortinet's solutions, which are among the most deployed, most patented, and most validated in the industry. The Fortinet Training Institute, one of the largest and broadest training programs in the industry, is dedicated to making cybersecurity training and new career opportunities available to everyone. Collaboration with esteemed organizations from both the public and private sectors, including CERTs, government entities, and academia, is a fundamental aspect of Fortinet's commitment to enhance cyber resilience globally. FortiGuard Labs, Fortinet's elite threat intelligence and research organization, develops and utilizes leading-edge machine learning and AI technologies to provide customers with timely and consistently top-rated protection and actionable threat intelligence. Learn more at https://www.fortinet.com, the Fortinet Blog, and FortiGuard Labs.
fortinet.com

January 30, 2026 12:47 PM / MKTG-2775-0-0-EN