Arista Statement on AI-Enhanced Security and Resilience

At Arista Networks, the quality of our products has always been our highest priority. We understand the responsibility that comes with being entrusted to be part of our customers' infrastructure. We believe that security is an important part of that quality. As the threat landscape evolves with the emergence of automated vulnerability discovery and next-generation AI models, Arista remains at the forefront of defensive innovation.

The Velocity of AI-Driven Threats

Highly capable AI models represent a shift in the speed at which cybersecurity attacks can occur. AI-driven vulnerability discovery has already compressed the time between identifying a software flaw and weaponizing it. To counter this, Arista is layering AI-driven discovery and assessments through partnerships such as Project Glasswing and others into our development and testing lifecycles. This initiative augments our existing practices involving current-generation tools for static and dynamic analysis (SAST/DAST), and human-led threat modeling, software security practices as well as testing of extreme and edge cases. By deploying a multiplicity of automated security solutions and tools across our pipelines, we have identified complex logic flaws and other issues before we ever release software.

Arista Architecture and Design

Arista EOS is built on a firm, resilient, scalable, and fault-tolerant architectural foundation. This architectural advantage allows us to be both resilient to security flaws as well as minimize the attack surface and blast radius if a defect were to exist. Specifically, our modular, state-sharing architecture provides a hardened structure with:

- Plane Separation: EOS provides inherent separation between the control plane (software management) and the data plane (hardware forwarding) to help ensure that failures in the control plane do not affect traffic on the data plane.
- Agent Isolation: Within a plane, there is further separation between software agents running inside the network operating system. Issues impacting a single protocol are contained within that agent and do not spread to other parts of the system. This separation of agents also enables targeted fixes to affected components with minimal impact on the overall system.
- Memory and Message Safety: Arista EOS code uses a framework that enforces best practices for memory management, message passing, and other parts of the code that have historically been sources of vulnerabilities. This framework is designed to prevent these common categories of security defects from occurring in the first place.

In short, Arista EOS is designed from the ground up so that even as automated tools seek to exploit software vulnerabilities, the system ensures core traffic forwarding remains isolated and secure.

Open Source Software

Arista products, including EOS, utilize Open Source Software. This software is shipped in the products in a locked-down manner where unnecessary features are turned off and components are removed from the base operating system. Our proactive monitoring of upstream libraries and triage of components enable us to remediate or prevent issues before they become exploits. As a recent example, consider the "copy.fail" flaw[1] that impacted many technology products. Due to our highly locked-down use of open-source software that disables non-essential services, Arista EOS images remained unaffected.

[1] https://www.arista.com/en/support/advisories-notices/security-advisory/24004-security-advisory-0136

Customer Recommendations in the AI Era

To mitigate machine-speed threats, we recommend a posture of awareness and architectural resilience and that our customers follow our best practices and security advisories as they are published:

- Arista's Security Advisories: Subscribe via email or RSS feed to our security advisories that are published on our website.
- Adhere to the EOS Hardening Guide: Minimizing the attack surface remains the most effective defense against automated discovery.
- Maintain Real-Time Visibility: Ensure you have a detailed, live inventory of your infrastructure. When security advisories are issued, the ability to identify and update impacted nodes instantly is your greatest defensive asset.
- Implement Zero Trust Networking: Minimize your attack surface by leveraging traffic encryption (MACSec/IPSec), network access control (NAC), macro- and microsegmentation, and network traffic analysis to ensure that any potential compromise is identified immediately and contained before an attacker can move laterally across the network.

Controlled Disclosure and Partnership

Arista maintains a policy of controlled disclosure regarding our internal security research, private testing initiatives, and specific defensive tooling. This ensures we maintain a robust security posture while protecting operational security and the strategic advantages of our customers and software development process. We welcome high-level discussions with our partners on general AI security challenges and industry-best defense practices. To engage, please reach out through your Arista account manager.

References

Arista Security Advisories: https://www.arista.com/en/support/advisories-notices

Arista EOS Hardening Guide: https://arista.my.site.com/AristaCommunity/s/article/arista-eos-hardening-guide

Arista Vulnerability Management Process: https://www.arista.com/en/support/product-documentation/vulnerability-management-process

Arista Zero Trust Networking: http://www.arista.com/security

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062