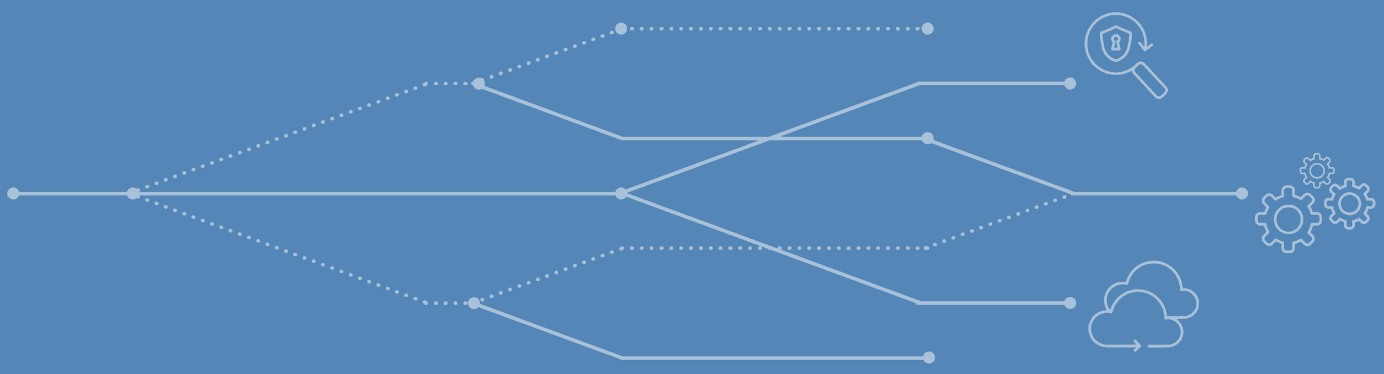
ARISTA

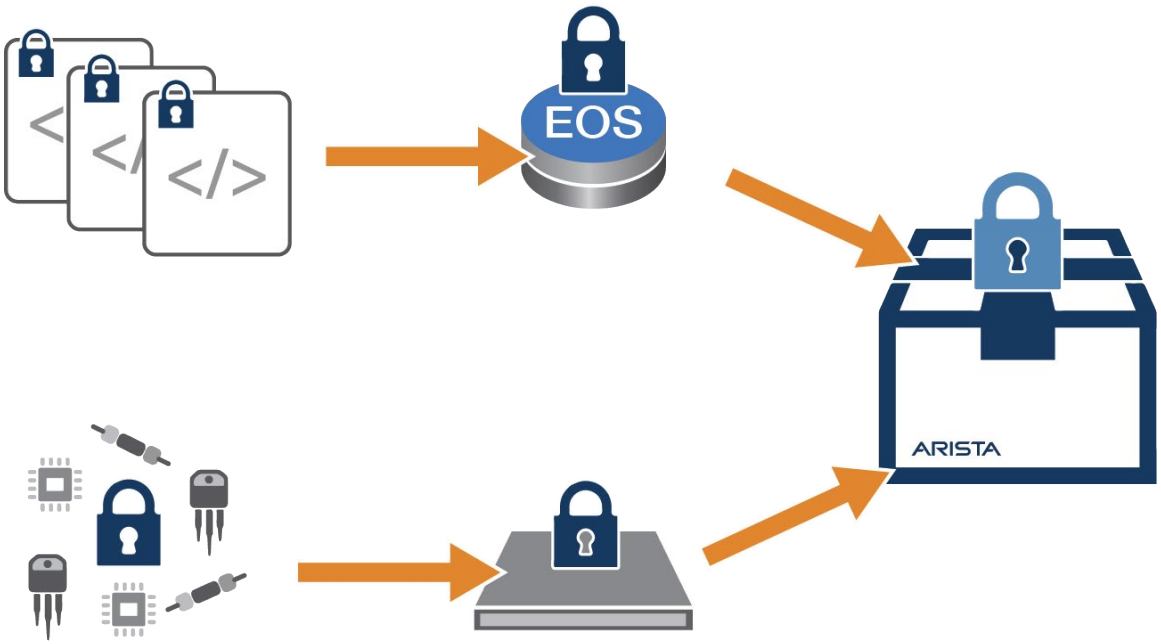


Trust Assurance in Arista Platforms

Introduction

As the backbone of modern business, the network infrastructure is a mission critical platform entrusted to carry high value commercially sensitive information. Increasingly, networking products are seen as vectors for malicious actors to infiltrate organisations and exfiltrate large amounts of sensitive data with lower risk of detection when compared to the direct targeting of workstation and server compute.

Arista is committed to the highest levels of security and employs a ground up approach to securing its products beginning with hardware design and manufacture and adopting industry best practices in secure software engineering. It is an engineering goal to ensure customers and their data are safeguarded. This document provides a high level overview of key processes and design choices that provide that assurance.



Security Starts With Design

Arista designs its unique hardware and software switching and routing platforms entirely in-house unlike the approach taken by other networking vendors to outsource design and development or to leverage a reference design. Critical security components are built around standard, well understood open software libraries and implemented against the FIPS 140-2 standard. Arista explicitly does not rely on any closed source 3rd party software Intellectual Property (IP) for tasks critical to the intended operation of the system.

Products including a Trusted Platform Module (TPM) provide a hardware root of trust, an immutable verification of core functionality and prevent unauthorised modification of the system as well as storing a uniquely identifiable key that allows remote attestation of each individual product.

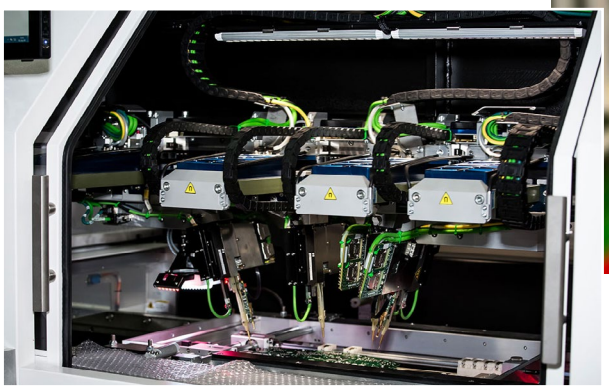
Leveraging the embedded TPM Arista's Extensible Operating System (EOS) binaries can also be signed and cryptographically validated before they are allowed to be loaded onto a system, ensuring that illegitimate, tampered-with EOS software cannot be booted unknowingly on devices.

Trustworthy Manufacturing

Building a trustworthy system inevitably begins with a trusted manufacturing process. As networking products are highly sophisticated devices, manufactured from thousands of components on a global scale, this is an area for focus in eliminating the risk of both counterfeiting and malicious intervention.

Arista's manufacturing process is designed to navigate these challenges in multiple ways, controlling and separating component supply, assembly, test and validation processes in silos. This ensures that no single area can circumvent the end to end manufacturing process and the final critical diagnostic and manufacturing functions are isolated from each other. The diagnostic software operated in the manufacturing process is owned and controlled by Arista and is subject to the same secure processes as for EOS.

Strict process controls implemented between manufacture and shipment are augmented by advanced test and validation systems including Automated Optical Inspection (AOI) and In Circuit Test (ICT). These tools provide hardware quality assurance and validation that products are assembled as originally intended by checking the hardware physical layout and expected properties of system components compared to reference models.



Software Engineering & Open Source

Arista's EOS operating system and CloudVision platform was designed from the ground up for secure modularity. Optimising the software stack into small, concise functional modules not only ensures overall product quality, but further removes the opportunity for typical software exploitation vectors.

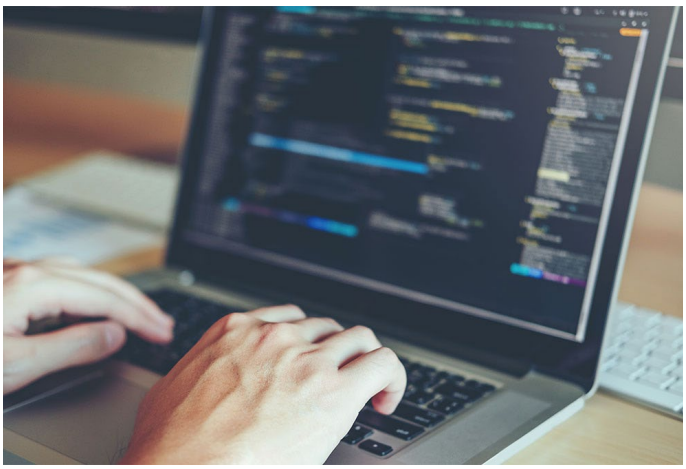
Commits to the EOS and CloudVision codebase are cryptographically signed and validated prior to being added to the product codebase, providing an additional internal layer of protection within the complete software bundle.

Arista is a strong supporter and contributor to open-source projects and leverages open source software to benefit from the extensive community scrutiny and broad global adoption, providing the largest possible test, verification and validation coverage available.

When making decisions on which open source software to use, Arista aims to select widely deployed industry standard software as deployed by industry titans and security researchers. The use of a common cryptographic toolkit ensures that both Arista and the community benefits from combined knowledge and improvements. To quote Linus Torvald's law of Software Development: "Given enough eyeballs, all bugs are shallow."

Finally, Arista's Product Security Incident Response Team (PSIRT) continuously analyzes and validates both the software we develop and any open source components, including analysis of relevant issues registered with the MITRE Common Vulnerabilities and Exposures (CVE) database (cve.mitre.org). The team also works closely with component suppliers, customers and the broader security community to closely monitor and respond to emerging vulnerabilities in both software and hardware.

Arista's PSIRT team publishes best practice guides for device hardening and configuration which can be implemented, monitored and enforced through the CloudVision platform. CloudVision proactively notifies customers of open bugs and security vulnerabilities to assist customers in maintaining software currency and quickly mitigating known risks.



Protecting Customer Networks and Data

Arista offers a number of cloud based management solutions, such as CloudVision as a Service (CVaaS), where multiple tiers of security are deployed to protect customer data. These include strong access controls, two-factor authentication, regular vulnerability scanning and management, encryption of data and personally identifiable information (PII) data privacy. Where appropriate, these security measures are certified to SSAE SOC 2 Type II and FIPS 140-2.

Customers leveraging the cloud service may enable ZTP-as-a-service. This enables secure authentication of devices against Arista's product build and customer ownership database. The remote attestation service prevents the installation of rogue or unauthorized devices, ensuring products are registered to the correct owner and validating the authenticity of each device to protect the customer network against infiltration.

Arista also maintains strong operational and security controls over its internal systems. A centralized directory delivers a consistent picture of user identity allowing enforcement of consistent roles and segmentation across all resources. External services are similarly protected through multi-factor authentication against the same policies, maintaining consistent logical access controls across the organisation.

Arista is committed to compliance with the US-EU Privacy Shield and regularly reviews and updates its sub-processors to ensure our customers' data is secured, protected and continues to be private.

Summary

Arista products are deployed globally in mission critical roles across many industries in which security is paramount.

Maintaining strong security is deeply important for all aspects of Arista's product family and represents a core engineering goal that applies across platforms, software, cloud and information technology systems. Tools like CloudVision also make the task of maintaining configuration consistency and vulnerability management significantly less of a burden for our customers.

The success of Arista's innovative approach to ground up security is validated through the networking industry's lowest exposure to CVE, despite deployment at the largest scale and in public Internet facing environments where exposure to malicious attack is continuous.

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 & B, 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