Zero Trust: Accelerating Your Maturity via the Network

Introduction

Zero trust as a concept has been around for a while[1] and over the last decade, many organizations have embarked on a path towards building and maintaining a zero trust architecture. These efforts have accelerated as insider threats, ransomware, and nation-state attacks quickly get past the hard perimeter and then roam freely within the "squishy inside" of the network. This is especially significant as most attacks now tend to be malware-free, leveraging insider credentials and legitimate applications already deployed in the environment. In other words, the attacks targeting organizations are predominantly "insider attacks," even if they are not orchestrated or willfully launched by a legitimate insider.

With all the efforts and investment in zero trust, one cannot help but wonder where organizations are in their zero trust efforts. In talking to prospects, customers, partners, and industry analysts, it is apparent that there has been progress. For instance, just in the last couple of years, organizations have come to terms with the fact that zero trust is an ongoing journey rather than a destination. Furthermore, many have embarked on this journey and achieved some early wins through mechanisms such as multi-factor authentication, and single sign-on that enhance security. However, we also find that even the most diligent organizations seem to stall on the journey as they attempt to achieve zero trust across the domains of identity, applications, devices, networks, and data.

This paper examines some of the hurdles in the zero trust journey. We also discuss how best-in-class organizations have approached this journey as a maturity effort and with that in mind we review the maturity model from the Cybersecurity and Infrastructure Agency (CISA). Based on these models we look at ways a pervasive network strategy can help compensate for a lack of maturity in other domains. Finally, we map Arista's security solutions to the CISA model and highlight how these solutions can accelerate your zero trust journey.

Zero Trust Security: Are We There Yet?

Based on the premise of explicit trust, zero trust security ensures complete visibility and control over any enterprise network activity, regardless of which device, application, or user is accessing that resource. This approach eliminates the implicit trust associated with network location and instead places the onus on continuously monitoring and assessing the security posture of the requester before allowing access to resources. Furthermore, if malicious intent is uncovered during this process, zero trust requires a quick response.

While zero trust is a very pertinent concept, the devil is very much in the implementation details. Early attempts focused on buying a "zero trust product or solution." Much credit for this approach is due to vendor marketing that claimed to be the one-stop solution for zero trust. More recently, most organizations now realize that zero trust is much more of a journey that involves multiple domains from identity, data, and workloads to devices and the network. And while this might appear daunting given the scope of any zero trust effort, organizations have over the last few years made progress on several fronts such as:

- Training employees and stakeholders. Most organizations have rolled out the basics of security awareness training for their employees: how to avoid phishing lures and other social engineering attempts, ensure employees have good password hygiene, and other basics such as using encryption when dealing with sensitive data.
- Implementing multi-factor authentication (MFA). Industry statistics[2] show more than 80% of organizations have implemented some form of MFA, a number that continues to grow year over year as the benefits of MFA in mitigating risk are now noticeably clear.
- Enforcing least privilege access. While closely related to MFA, this control is less widely implemented by organizations due to legacy applications and data access needs that are often disrupted when least privilege is rolled out.
- Identifying critical assets including devices and data stores. Customers tell us that, while they know what needs to be protected, they are challenged in mapping where all that data sits in today's complex IT environment that spans the campus, data center, and cloud.

[1] https://en.wikipedia.org/wiki/Zero_trust_security_model

[2] https://www.watchguard.com/wgrd-resource-center/infographic/state-password-security

- Regular assessments of security posture. Organizations do have a regular cadence of penetration tests and compromise assessments, but they struggle with understanding and assessing the security of their entire attack surface. This is especially true given IoT, supply chain, and contractors as well as cloud-based infrastructure.
- Deploying endpoint and network security controls. Endpoint detection and response (EDR) are increasingly common and now often integrated with so-called endpoint protection platforms (EPP) that include basic anti-virus at the minimum. Similarly, on the network customers are using perimeter firewalls, IDS/IPS with more mature customers rolling out network detection and response (NDR) solutions.

But is that enough? If you tackle the aforementioned items, can you truly claim to have achieved zero trust? As you might expect the answer is a bit more nuanced. A better perspective is to focus on maturity on the zero trust journey.

Zero Trust Maturity Models

The Cybersecurity and Infrastructure Security Agency (CISA)[3] defines itself as "the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience." This agency, formed in 2018, connects private and public sector organizations while delivering information and tools that support the development of their cyber and physical security and resilience programs.

The Colonial Pipeline ransomware attack[4] in 2021 and other newsworthy security breaches put renewed focus on cybersecurity and brought CISA to the forefront of mitigating the risk from attacks such as these. One of the great resources produced consequently was the CISA Zero Trust Maturity Model, most recently updated in April 2023[5]. This document delivers prescriptive guidance for the transition to zero trust, building on previous work produced by NIST and other organizations. The CISA model focuses on making incremental progress over time with the goal of optimal zero trust. CISA provides guidance across five foundational pillars: Identity, Devices, Networks, Applications and Workloads, and Data along with visibility and analytics, automation and orchestration, and governance considerations for each pillar (Figure 1).

[3] https://www.cisa.gov/

[4] https://en.wikipedia.org/wiki/Colonial_Pipeline_cyberattack

[5] https://www.cisa.gov/sites/default/files/publications/CISA%2520Zero%2520Trust%2520Maturity%2520Model_Draft.pdf

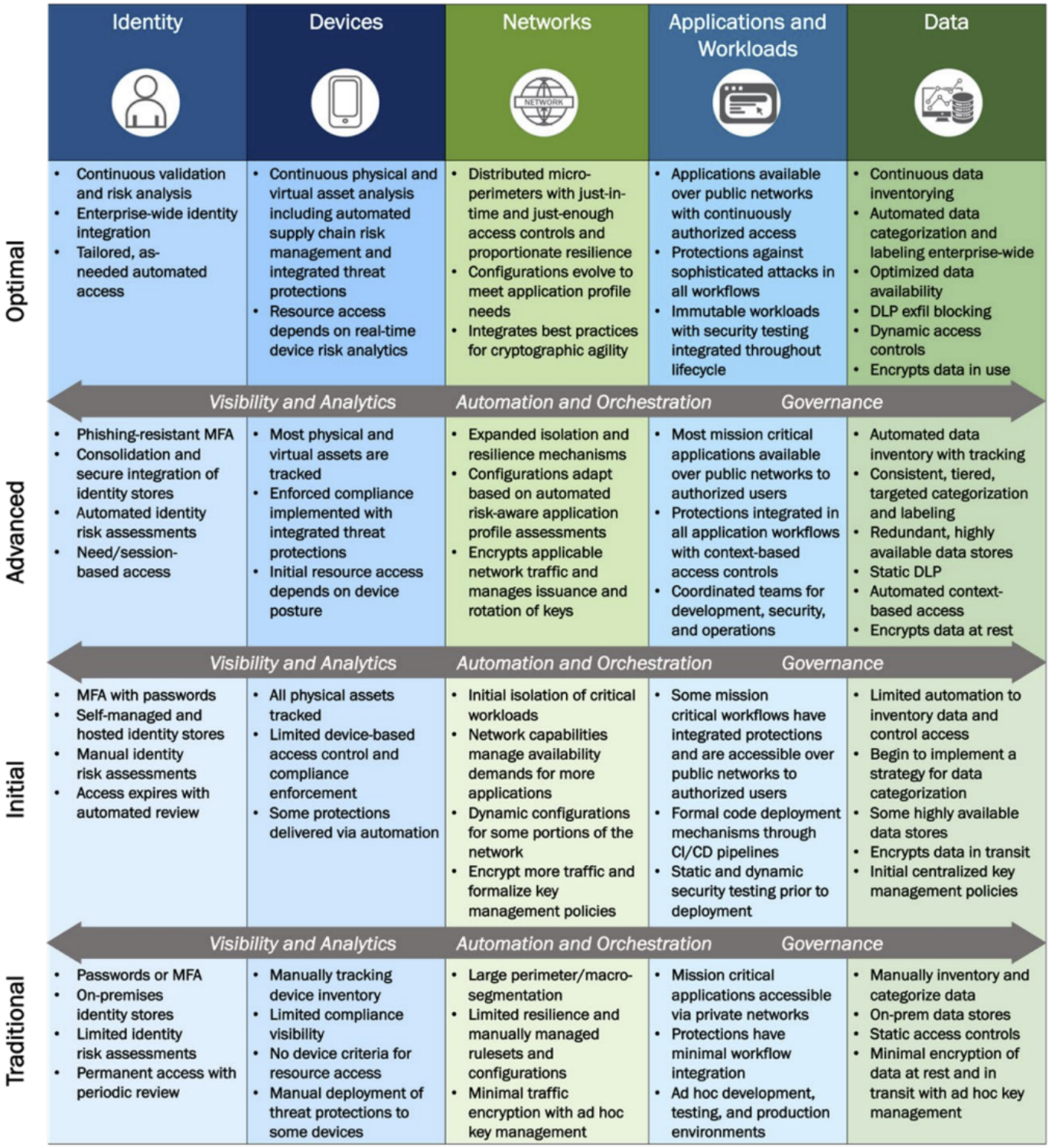

Figure 1: Cybersecurity and Infrastructure Security Agency Zero Trust Maturity Model

Challenges to Zero Trust Maturity

The frameworks we discuss in this paper help assess progress on the zero trust journey. The bad news is that after talking to customers and industry experts we concluded that most organizations are at the "Traditional" or "Beginner" level depending on which model is used. Why is this the case?

The reality is that implementing zero trust security can be challenging, and the hard stuff is especially hard. Organizations run into several roadblocks that stall their journey including:

- Legacy networks, systems, and applications that cannot be easily replaced and are often critical to the business. And yet they can be hard to integrate with modern identity, data protection, and other security solutions. In fact, many of these applications were specifically designed and built with the idea of implicit trust which is counter to the principles of zero trust.
- Inventorying the devices, applications, data, and users sounds simple but in the age of IoT, BYOD, DevOps and shadow IT, most organizations often have 50% or less of these entities tracked within their configuration management databases. Furthermore, organizations lack the tools and processes to even gain this visibility, and so are left to "best effort discovery."
- Data protection and encryption come with their own sources of complexity around key management, and the performance implications associated with encryption everywhere. One simply must look at the prevalence of clear text and insecure protocols such as SMBv1 and HTTP to understand how, despite best intentions, organizations struggle to eliminate weak and clear text protocols from their environments.
- Human behavior and resistance can also doom zero trust efforts. Let us face it, the very idea of not trusting by default seems disrespectful when it comes to an organization's employees and stakeholders. Achieving success and maturing zero trust, therefore, requires a culture change that of course is never easy to orchestrate.

One might expect the network to be an easier target for zero trust, but on the contrary, as mentioned above, the experts recommend tackling this last. Why is this the case? Some of it comes down to the fact that the very definition of the network has changed, and it is no longer simply a set of switches and routers. Today, most organizations have networks that span across multiple domains, from campus and data centers to the cloud, operational technology (OT)/IoT, etc. And while network security controls like firewalls, segmentation, network access control (NAC), and network intrusion detection have been around for decades, they all have significant drawbacks:

- Often segmentation and NAC have a negative connotation due to excessive operational overhead or due to the use of custom packet formats and vendor lock-in. These controls are also often the cause of outages due to vendor software quality and operator errors.
- Firewalls are expensive and add additional management overhead, therefore they are used only where they bring the most value: at the perimeter or in the DMZ. So much for microperimeters everywhere!
- Centralizing analytics for data gathered from the network has been an ongoing challenge with proprietary data formats, multiple consoles, and the limited visibility mentioned above.
- And finally, network threat detection is still focused on pattern matching or anomaly detection at best. Both generate high false positives and negatives resulting in operational overhead and invisible and unmitigated risk to the organization.

Accelerating Zero Trust Maturity

This brings us to the all-important question of whether we should just be content with the 10-year process to zero trust maturity. Is there potentially a better way? At Arista, we believe there is, and it starts by putting the network at the core of the zero trust journey.

A Thesis for Starting with the Network

Given the risks mentioned above about zero trust in the network, why would an organization even consider starting with the network? It would behoove us to consider some of the advantages offered by a network-centric approach:

- The network is pervasive – every communication hits the network at some point enabling observability, threat detection, and access control to be transparently enabled. This provides risk mitigation for the legacy devices, workloads, and data stores that cannot be easily "ZT-fied." As a result, implementing zero trust on the network can accelerate the overall zero trust program and buy time to address deeper challenges in the other domains – like data or workloads.
- The network does not care whether the devices are managed or unmanaged -- instead, it can identify those devices and apply policies for authentication and authorization, irrespective of what they are and where they are currently.
- The network is much more homogenous than devices, workloads, users, data, etc. Protocols like TCP/IP are universal unlike the complexity involved with different operating systems or application server software.

Of course, some would argue the network does have blind spots, for instance, remote endpoints or branches that do not backhaul network traffic but route directly to the Internet. These setups may not hit the organization's traditional network and thus be "invisible" to the organization's zero trust controls. This is why any zero trust networking architecture must include tight integrations with complementary solutions such as endpoint detection and response or zero trust network access technologies.

The Rise of the Microperimeter

What does zero trust for the network come down to? CISA provides a lot of prescriptive guidance in its maturity model (Figure 1). If you dive deeper into the model, CISA details the most critical network controls, along with key network capabilities for visibility and analytics, automation and orchestration, as well as governance (Figure 2).

Function	Traditional	Initial	Advanced	Optimal
Network Segmentation	Agency defines their network architecture using large perimeter/macro-segmentation with minimal restrictions on reachability within network segments. Agency may also rely on multi-service interconnections (e.g., bulk traffic VPN tunnels).	Agency begins to deploy network architecture with the isolation of critical workloads, constraining connectivity to least function principles, and a transition toward service-specific interconnections.	Agency expands deployment of endpoint and application profile isolation mechanisms to more of their network architecture with ingress/egress micro-perimeters and service-specific interconnections.	Agency network architecture consists of fully distributed ingress/egress micro-perimeters and extensive micro-segmentation based around application profiles with dynamic just-in-time and just-enough connectivity for service-specific interconnections.
Network Traffic Management (New Function)	Agency manually implements static network rules and configurations to manage traffic at service provisioning, with limited monitoring capabilities (e.g., application performance monitoring or anomaly detection) and manual audits and reviews of profile changes for mission critical applications.	Agency establishes application profiles with distinct traffic management features and begins to map all applications to these profiles. Agency expands application of static rules to all applications and performs periodic manual audits of application profile assessments.	Agency implements dynamic network rules and configurations for resource optimization that are periodically adapted based upon automated risk-aware and risk-responsive application profile assessments and monitoring.	Agency implements dynamic network rules and configurations that continuously evolve to meet application profile needs and reprioritize applications based on mission criticality, risk, etc.
Traffic Encryption (Formerly Encryption)	Agency encrypts minimal traffic and relies on manual or ad hoc processes to manage and secure encryption keys.	Agency begins to encrypt all traffic to internal applications, to prefer encryption for traffic to external applications[27], to formalize key management policies, and to secure server/service encryption keys.	Agency ensures encryption for all applicable internal and external traffic protocols,[28] manages issuance and rotation of keys and certificates, and begins to incorporate best practices for cryptographic agility.[29]	Agency continues to encrypt traffic as appropriate, enforces least privilege principles for secure key management enterprise-wide, and incorporates best practices for cryptographic agility as widely as possible.
Network Resilience (New Function)	Agency configures network capabilities on a case-by-case basis to only match individual application availability demands with limited resilience mechanisms for workloads not deemed mission critical.	Agency begins to configure network capabilities to manage availability demands for additional applications and expand resilience mechanisms for workloads not deemed mission critical.	Agency has configured network capabilities to dynamically manage the availability demands and resilience mechanisms for the majority of their applications.	Agency integrates holistic delivery and awareness in adapting to changes in availability demands for all workloads and provides proportionate resilience.
Visibility and Analytics Capability	Agency incorporates limited boundary-focused network monitoring capabilities with minimal analysis to start developing centralized situational awareness.	Agency employs network monitoring capabilities based on known indicators of compromise (including network enumeration) to develop situational awareness in each environment and begins to correlate telemetry across traffic types and environments for analysis and threat hunting activities.	Agency deploys anomaly-based network detection capabilities to develop situational awareness across all environments, begins to correlate telemetry from multiple sources for analysis, and incorporates automated processes for robust threat hunting activities.	Agency maintains visibility into communication across all agency networks and environments while enabling enterprise-wide situational awareness and advanced monitoring capabilities that automate telemetry correlation across all detection sources.
Automation and Orchestration Capability	Agency uses manual processes to manage the configuration and resource lifecycle for agency networks and environments with periodic integration of policy requirements and situational awareness.	Agency begins using automated methods to manage the configuration and resource lifecycle for some agency networks or environments and ensures that all resources have a defined lifetime based on policies and telemetry.	Agency uses automated change management methods (e.g., CI/CD) to manage the configuration and resource lifecycle for all agency networks and environments, responding to and enforcing policies and protections against perceived risks.	Agency networks and environments are defined using infrastructure-as-code managed by automated change management methods, including automated initiation and expiration to align with changing needs.
Governance Capability	Agency implements static network policies (access, protocols, segmentation, alerts, and remediation) with an approach focused on perimeter protections.	Agency defines and begins to implement policies tailored to individual network segments and resources while also inheriting corporate-wide rules as appropriate.	Agency incorporates automation in implementing tailored policies and facilitates the transition from perimeter-focused protections.	Agency implements enterprise-wide network policies that enable tailored, local controls; dynamic updates; and secure external connections based on application and user workflows.

Figure 2: CISA Zero Trust Maturity Model for the Network

In this section, we examine each of the functions in Figure 2 and discuss the approaches available and the challenges they present.

Network Segmentation

Many organizations today segment using VLANs or firewalls and other coarse forms of macrosegmentation. This effort partitions the network based on business needs. Some common examples include the DMZ, separation of development and production environments, and isolating different functional units e.g., human resources from the finance network. The CISA guidance encourages organizations to enhance their zero trust posture with a move toward microperimeters where the segmentation can move as close to the workload or data store as possible. Moreover, this approach must automatically learn, enforce, and spot deviations in application workflows.

Microsegmentation solutions have gained popularity recently and are effectively used in virtual hosted environments. With bare metal workloads, they require an agent installed on the server which presents challenges such as operating system and application compatibility, potential performance issues, and the operational burden of maintaining an agent.

Network Traffic Management

This function of the CISA maturity model focuses on the ability to monitor network traffic, identify anomalies, and audit when traffic patterns change. As organizations move from the traditional to the optimal maturity level, many of these functions are automated and self-learning based on a risk-aware approach to monitoring. Many organizations used network/application performance management tools to perform these functions but most often this effort lacks context on mission criticality, risk, and impact on the organization. Moreover, alerting relies on anomaly detection which can create a fair amount of noise and as a consequence often ends up being filtered out or ignored entirely.

Traffic Encryption

The goal for optimal zero trust maturity is to encrypt all data in transit both in the north-south direction i.e., between the organization and the outside world, as well as internal east-west traffic. Most organizations today use TLS to perform this function for web applications. Protocols like SSH are also common. However, as mentioned above legacy applications especially those that use custom ports and protocols are hard to retrofit with encryption. And so often the compensating control organizations are left with, at best, is to try and isolate traffic from and to these applications to its own segment in a bid to minimize who can see the clear text traffic. Our experience however has been that clear text secrets and passwords are pervasive across every organization. Further, even those that have encryption widespread struggle with some of the foundational aspects such as key management and other cryptographic best practices.

Network Resilience

The network resilience function as the name suggests tasks organizations with paying attention to providing and maintaining access to business-critical network capabilities. As organizations progress on the maturity curve, much of this process is automated and adapts automatically to changing availability demands. The network is also able to automatically recover from a threat or other event that impacts availability. Finally, like the other functions described in this section, the capabilities must be context-aware and can be tuned in proportion to the criticality of the applications and workloads.

Visibility and Analytics Capability

For visibility and analytics, the agency recommends centralized aggregation and analysis from perimeter sensors, to begin with. The goal however is to have these sensors all over the network with the ability to automatically alert operators to changes in state as well as potential threats. With today's diverse networks, organizations struggle with answering simple questions such as "What is on the network?" let alone being able to perform automated analytics and threat analysis on the telemetry from network sensors. Most are therefore constrained to legacy methods such as SNMP polling and network log monitoring from a limited set of sensors and/or pulling data from multiple consoles and then having analysts manually make sense of the information. We would argue this lack of visibility is the single biggest reason experts often recommend delaying zero trust on the network.

From a threat protection perspective, CISA maturity evolves from a purely perimeter-based and traditional signature-based approach that can at best identify known threats to a machine learning-based solution that detects the likes of non-malware and insider threats deep inside the network. These new AI-based offerings understand the context behind each entity interacting over the network and their activities, can cluster entities into cohorts, and identify outliers. These solutions can also be significantly more impactful in risk reduction when they deliver this context and explainability, thus making analysts more productive and reducing the operational overhead on security and network teams.

Automation and Orchestration Capability

Today automation and orchestration of network changes are uncommon due to the brittle nature of the underlying infrastructure. Most mature organizations do have explicit change management workflows but those must be manually triggered. On the other hand, CISA recommends pervasive automation which can operate with an infrastructure-as-code paradigm and leverages the continuous integration/continuous deployment (CI/CD) processes that are popular among software developers.

Governance Capability

Governance focuses on who can connect to the network and what they can do after they connect. As organizations continue to struggle with their expanding attack surface, the path to maturity in this area is to move from a manual process to identify sanctioned networks, devices, and services to fully automated discovery and policy enforcement for these entities. Similarly, remediating unauthorized entities discovered in this process must also be automated via network policies that quarantine or isolate as appropriate. While a lot of organizations will run periodic automated scans of the network to discover IP-enabled devices, as you might expect this lacks a real-time view and enough context to automate remediation, leaving it to human operators to investigate what is behind the IP—a process that could easily take days or weeks and involve many different parts of the organization.

Arista Accelerates Your Zero Trust Maturity

Arista partners with organizations of all sizes to rapidly set them on the path for optimal zero trust maturity by using the very underlying infrastructure that is already deployed on the network. Arista Extensible Operating System (EOS®) is the core of Arista networking solutions for next-generation data centers, campus, and cloud networks. Networks built with Arista EOS scale to hundreds of thousands of nodes with management and provisioning capabilities that work at scale. Through its programmability, EOS enables a set of software applications that deliver workflow automation, high availability, unprecedented network visibility, security, and analytics and rapid integration with a wide range of third-party applications for virtualization, management, automation, and orchestration services.

The EOS network data lake (NetDL) builds upon the EOS's core publish-subscribe state capabilities with datastores and analytics for network data sources such as alerts, flows, full packet capture, control plane traffic, and device state streaming as well as third-party and external data integrations. This enables a wide range of applications to process, analyze, and derive operational insights and predictions from this data set (Figure 3).

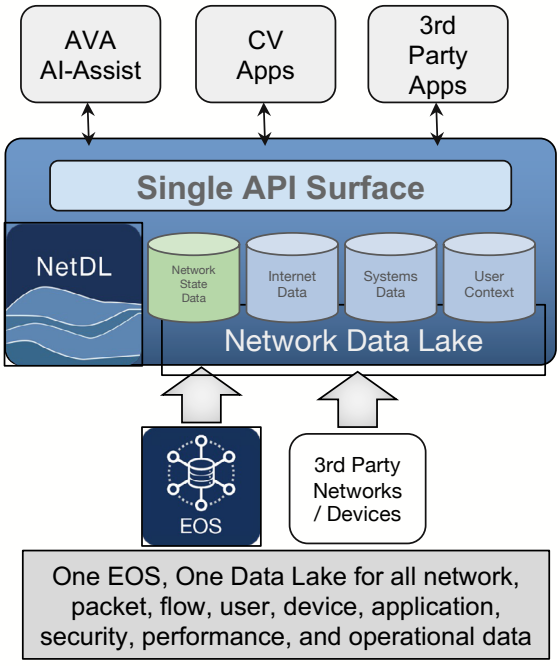

Figure 3: Arista EOS and NetDL Architecture

NetDL provides a single source of network data 'truth' and a common sensor/collector architecture that enables forensics and analytics for threat hunting, network packet brokers, network detection and response, as well as network and application performance monitoring. By collaborating with a variety of industry leaders, Arista can deliver powerful production customer benefits. These data-driven network models can be transformed into insights that deliver actionable operational outcomes.

Arista Autonomous Virtual Assist (Arista AVA™) utilizes machine learning and other AI technologies to augment all aspects of pervasive visibility, continuous threat detection, segmentation, and access control. AVA is extensible across many other operational use cases. For example, AVA can address challenges in network detection and response, quality of experience management, and proactive NetOps as well as network access control. Combined with distributed network-wide state and telemetry data, distributed sensor networks, and third-party data sources in NetDL, it can drive automation and extensibility in network design to a new and unprecedented level and can dramatically reduce the manual operational burden of securing and supporting networks.

This foundation of core technologies in turn enables a suite of capabilities that integrate with each other to form Arista's zero trust networking solution (Figure 4).

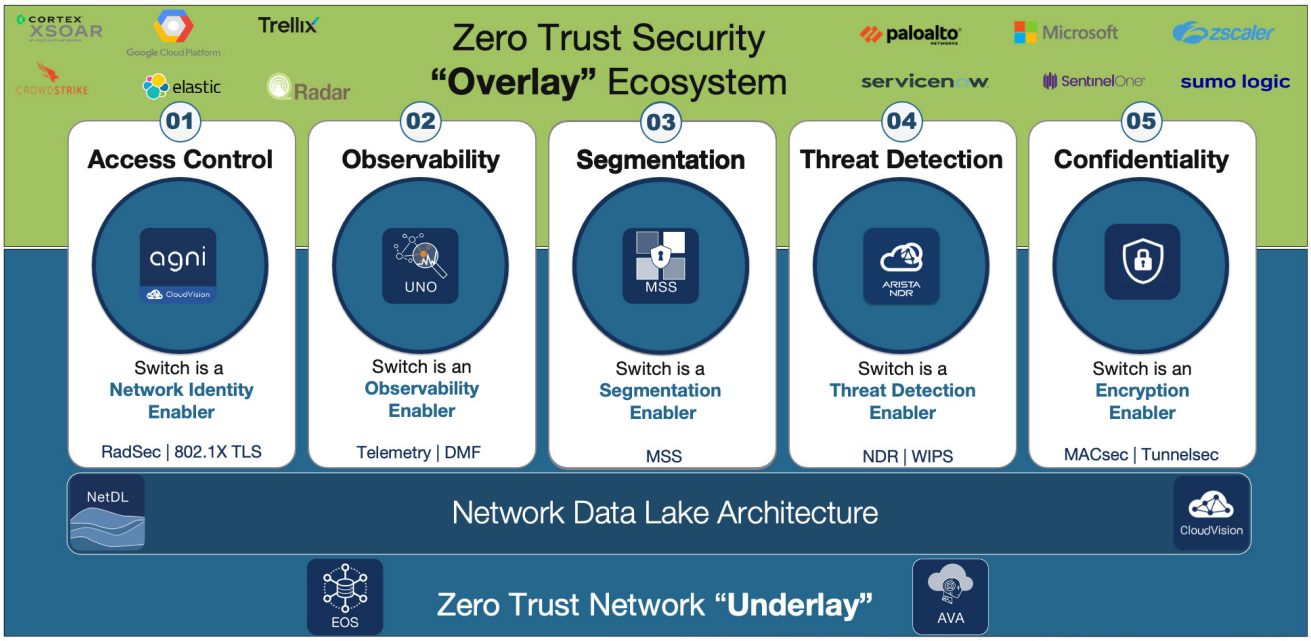

Figure 4: Arista Zero Trust Networking Solution

In the section below we show how the Arista offerings map to the CISA zero trust maturity model for networking and importantly why this enables organizations to accelerate their path to optimal maturity.

Network Segmentation

Function	Traditional	Initial	Advanced	Optimal
Network Segmentation	Agency defines their network architecture using large perimeter/macro-segmentation with minimal restrictions on reachability within network segments. Agency may also rely on multi-service interconnections (e.g., bulk traffic VPN tunnels).	Agency begins to deploy network architecture with the isolation of critical workloads, constraining connectivity to least function principles, and a transition toward service-specific interconnections.	Agency expands deployment of endpoint and application profile isolation mechanisms to more of their network architecture with ingress/egress micro-perimeters and service-specific interconnections.	Agency network architecture consists of fully distributed ingress/egress micro-perimeters and extensive micro-segmentation based around application profiles with dynamic just-in-time and just-enough connectivity for service-specific interconnections.

Figure 5: CISA Zero Trust Maturity for the Network Segmentation Function

Arista's Multi-Domain Segmentation Service (MSS) is a comprehensive microsegmentation solution that provides fine-grained security policies based on microperimeters defined around the identity of endpoints or applications.

MSS offers a consistent architecture across multiple network domains, is both network and endpoint-agnostic, and enables the distributed enforcement of stateless policies at wire speed within the Arista EOS-powered switches or can redirect traffic to a third-party firewall for stateful L4-7 inspection. Arista MSS thus enables lateral segmentation offloading the capability from firewalls that would have to be explicitly deployed for this purpose.

Arista MSS also automates the management of microperimeters by connecting to external sources and dynamically identifying and tagging the endpoints and workloads. To get this information, Arista MSS can connect to various external sources, such as NAC, CMDB, IPAM and server virtualization systems.

Network Traffic Management

Function	Traditional	Initial	Advanced	Optimal
Network Traffic Management (New Function)	Agency manually implements static network rules and configurations to manage traffic at service provisioning, with limited monitoring capabilities (e.g., application performance monitoring or anomaly detection) and manual audits and reviews of profile changes for mission critical applications.	Agency establishes application profiles with distinct traffic management features and begins to map all applications to these profiles. Agency expands application of static rules to all applications and performs periodic manual audits of application profile assessments.	Agency implements dynamic network rules and configurations for resource optimization that are periodically adapted based upon automated risk-aware and risk-responsive application profile assessments and monitoring.	Agency implements dynamic network rules and configurations that continuously evolve to meet application profile needs and reprioritize applications based on mission criticality, risk, etc.

Figure 6: CISA Zero Trust Maturity for the Network Traffic Management Function

The network traffic management function requires the ability to first identify applications and then classify them for optimal user experience. These capabilities are operationalized through quality of service and bandwidth reservations as well as granular monitoring policies. Arista EOS provides robust quality of service features as well as the ability to classify the traffic for appropriate prioritization within the network relative to other applications. The Arista DANZ Monitoring Fabric (DMF)[6] enables IT operators to pervasively monitor all user, device/IOT and application traffic (north-south and east-west) by gaining complete visibility into physical, virtual and container environments. Deep hop-by-hop visibility, predictive analytics and scale-out packet capture — integrated through a single dashboard — provides unprecedented observability to monitor, discover, and troubleshoot network and application performance issues, as well as accelerating discovery of root causes of security breaches and other outages.

Traffic Encryption

Function	Traditional	Initial	Advanced	Optimal
Traffic Encryption (Formerly Encryption)	Agency encrypts minimal traffic and relies on manual or ad hoc processes to manage and secure encryption keys.	Agency begins to encrypt all traffic to internal applications, to prefer encryption for traffic to external applications[27], to formalize key management policies, and to secure server/service encryption keys.	Agency ensures encryption for all applicable internal and external traffic protocols,[28] manages issuance and rotation of keys and certificates, and begins to incorporate best practices for cryptographic agility.[29]	Agency continues to encrypt traffic as appropriate, enforces least privilege principles for secure key management enterprise-wide, and incorporates best practices for cryptographic agility as widely as possible.

Figure 7: CISA Zero Trust Maturity for the Traffic Encryption Function

[6] https://www.arista.com/en/products/danz-monitoring-fabric

Arista network infrastructure natively supports encryption capabilities such as MACsec and TunnelSec. These capabilities, implemented on the switches, enable organizations to encrypt data to and from legacy applications and workloads without having to change those systems but instead relying on the network to protect data from unauthorized access, interception, and tampering.

TunnelSec uses industry-standard protocols like IPSec and SSL/TLS to establish secure tunnels across any network, including the public internet and thus enable secure communication and data exchange between remote locations. This is particularly useful for organizations with multiple branch offices or data centers that need to communicate securely with each other over a public network.

MACsec operates at the link layer of the network stack and provides data encryption between campus or data center network devices. MACsec is used to secure communications between devices on the same physical network, such as within a data center.

Network Resilience

Function	Traditional	Initial	Advanced	Optimal
Network Resilience (New Function)	Agency configures network capabilities on a case-by-case basis to only match individual application availability demands with limited resilience mechanisms for workloads not deemed mission critical.	Agency begins to configure network capabilities to manage availability demands for additional applications and expand resilience mechanisms for workloads not deemed mission critical.	Agency has configured network capabilities to dynamically manage the availability demands and resilience mechanisms for the majority of their applications.	Agency integrates holistic delivery and awareness in adapting to changes in availability demands for all workloads and provides proportionate resilience.

Figure 8: CISA Zero Trust Maturity for the Network Resilience Function

Arista EOS and CloudVision[7] bring a modern approach to continuous application delivery and performance. The key to resilience in a zero trust context lies in the ability to dynamically expand or reduce with network demands. For instance, this could mean having the ability to burst and use a utility cloud for the times when the demand is higher or availability is threatened. Similarly, network operations could use capacity from disaster recovery sites or backup data centers. Arista's Cloud Vision and EOS work hand in hand to dynamically provide onboarding and connectivity to any public utility clouds securely and with optimal performance. In many instances, customers striving for zero trust maturity in this function deploy data centers in active/active configuration using robust EOS features such as EVPN that provide the entire capacity as a single virtual data center while still providing geo-specific fault tolerance. CloudVision in turn provides single pane of glass management for both the traditional data center as well as the hybrid cloud.

Visibility and Analytics Capability

Function	Traditional	Initial	Advanced	Optimal
Visibility and Analytics Capability	Agency incorporates limited boundary-focused network monitoring capabilities with minimal analysis to start developing centralized situational awareness.	Agency employs network monitoring capabilities based on known indicators of compromise (including network enumeration) to develop situational awareness in each environment and begins to correlate telemetry across traffic types and environments for analysis and threat hunting activities.	Agency deploys anomaly-based network detection capabilities to develop situational awareness across all environments, begins to correlate telemetry from multiple sources for analysis, and incorporates automated processes for robust threat hunting activities.	Agency maintains visibility into communication across all agency networks and environments while enabling enterprise-wide situational awareness and advanced monitoring capabilities that automate telemetry correlation across all detection sources.

Figure 9: CISA Zero Trust Maturity for the Visibility and Analytics Capability

[7] https://www.arista.com/en/solutions/telemetry-analytics

Arista NDR[8] is an AI-enabled platform that analyzes billions of network communications to autonomously discover, profile, and classify every device, user, and application across the new network—perimeter, core, IoT, and cloud networks. Based on this deep understanding of the attack surface, the platform detects threats to and from these entities, while providing the context necessary to respond rapidly.

Arista NDR can deliver visibility and analytics enterprise-wide by utilizing existing deployed switches as network security sensors. As a result, organizations can benefit from broad situational awareness without the need to deploy additional network tapping infrastructure or network visibility solutions, but instead by relying on infrastructure that is already deployed. This is especially important in campus and branch locations where such components can be hard to deploy and maintain without dedicated rack space and local IT expertise.

Automation and Orchestration Capability

Function	Traditional	Initial	Advanced	Optimal
Automation and Orchestration Capability	Agency uses manual processes to manage the configuration and resource lifecycle for agency networks and environments with periodic integration of policy requirements and situational awareness.	Agency begins using automated methods to manage the configuration and resource lifecycle for some agency networks or environments and ensures that all resources have a defined lifetime based on policies and telemetry.	Agency uses automated change management methods (e.g., CI/CD) to manage the configuration and resource lifecycle for all agency networks and environments, responding to and enforcing policies and protections against perceived risks.	Agency networks and environments are defined using infrastructure-as-code managed by automated change management methods, including automated initiation and expiration to align with changing needs.

Figure 10: CISA Zero Trust Maturity for the Automation and Orchestration Capability

The Arista CI Pipeline[9] provides an advanced CI environment for managing network and security operations built upon the visibility provided by the Arista CloudVision platform. This capability along with Arista Validated Designs (AVD) provides additional features and integrations that greatly simplify and enhance the automation of network and security operations workflows.

Governance Capability

Function	Traditional	Initial	Advanced	Optimal
Governance Capability	Agency implements static network policies (access, protocols, segmentation, alerts, and remediation) with an approach focused on perimeter protections.	Agency defines and begins to implement policies tailored to individual network segments and resources while also inheriting corporate-wide rules as appropriate.	Agency incorporates automation in implementing tailored policies and facilitates the transition from perimeter-focused protections.	Agency implements enterprise-wide network policies that enable tailored, local controls; dynamic updates; and secure external connections based on application and user workflows.

Figure 11: CISA Zero Trust Maturity for the Governance Capability

CloudVision Arista Guardian for Network Identity™ [10] (CV AGNI) is a software-as-a-service network access control (NAC) solution that simplifies the onboarding and ongoing governance of network identity across users, their associated devices, and the Internet-of-Things, for both wired and wireless networks. CV AGNI uses existing identity providers such as Microsoft Azure AD or Okta and acts as the policy decision point (PDP) and policy enforcement point (PEP), both of which are critical for an effective zero trust architecture. CV AGNI performs dynamic authorization via real-time posture assessments based on data from Arista NDR and third-party technologies such as endpoint detection and response solutions. Based on these assessments and policies defined by the organization, unauthorized entities or those violating security policies can be automatically quarantined.

[8] https://www.arista.com/en/products/network-detection-and-response

[9] https://www.arista.com/assets/data/pdf/Arista-CI-Pipeline-Tech-Brief.pdf

[10] https://www.arista.com/assets/data/pdf/Arista-AGNI-Solution-Brief.pdf

Arista's Integrated Solution for Zero Trust

The combination of capabilities described above delivers a unified and integrated solution (Figure 12) to take organizations from a legacy or traditional approach to zero trust to an optimal level of maturity, all while leveraging the underlying network infrastructure, simplifying the rollout, and reducing operational overheads.

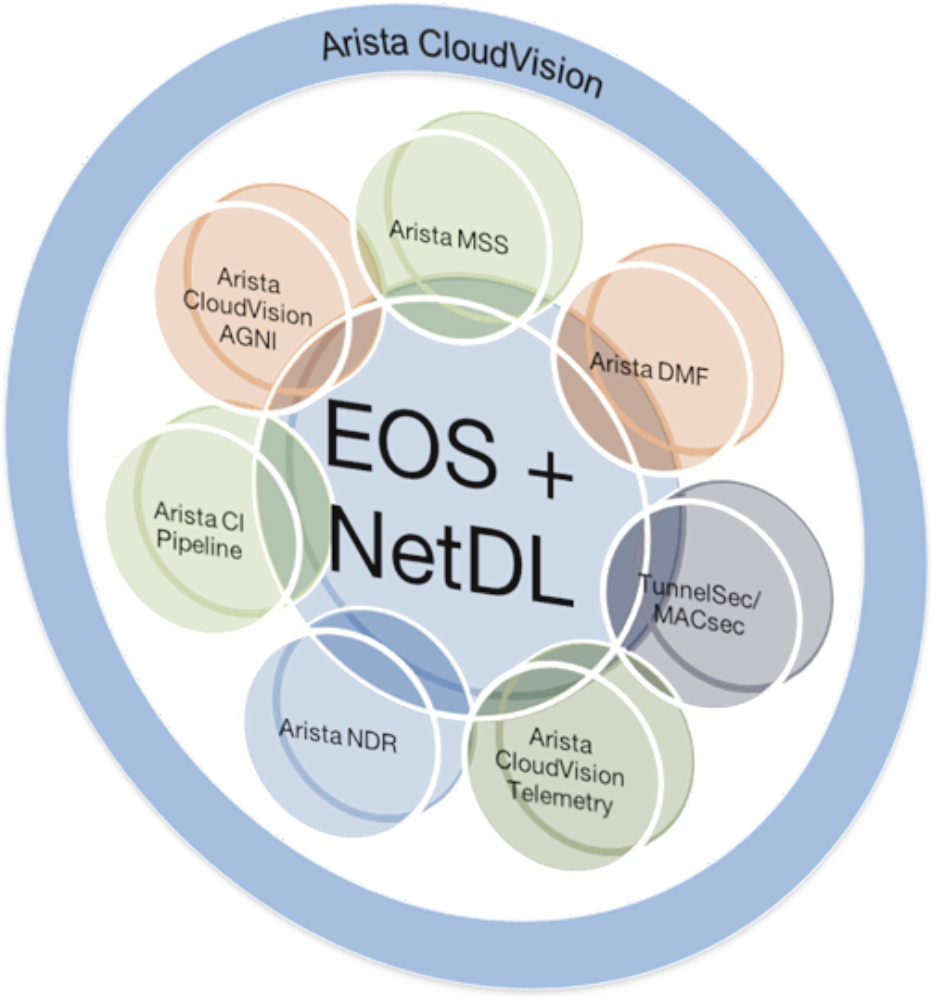

Figure 12: Arista Solutions to Accelerate Zero Trust Maturity

Summary

Zero trust architectures attempt to mitigate risk associated with cyber threats by eliminating implicit trust in a device simply because it is on the internal network. However, this is easier said than done given today's changing definition of the network that spans campus, data center, cloud, and more. The approach of adding additional network security layers such as firewalls, network access control, and threat detection among others comes at tremendous cost, complexity, and brittleness, while the benefits are often hard to quantify. As a result, many organizations must roll the risk management dice, especially deep inside the network where the organization's crown jewels are often housed.

Arista offers a full suite of security solutions built on the foundations of our unified operating system in EOS and the common management plane in CloudVision. These solutions map to the CISA Zero Trust Maturity Model and help organizations accelerate their journey toward optimal maturity. Moreover, these network security controls can help compensate for gaps in the organization's zero trust posture in other domains such as identity, devices, workload, and data. Most importantly, this integrated security toolset uses the underlying network infrastructure from switches to WAN routers to deliver key security capabilities and integrates seamlessly with the organization's existing security program and tools. We believe Arista's approach can convert security from a noun to an adjective, or in other words enable organizations to move from a bolt-on network security stack to a built-in secure network.

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