# ARISTA NETWORKS


**Key Contributors: Garrett Stokes, Bryanna Parkoff & Ruby Rodriguez**

UNIVERSITY OF THE INCARNATE WORD®

**11/28/2022**

This project and the preparation of this report were funded in part by the School of Science, Math, and Engineering Cyber Security Scholars through an agreement with the University of the Incarnate Word.

# EXECUTIVE SUMMARY

*Figure 1.* Arista Networks Power Swifter 400G Adoption (Source: Westfall, 2021).

Arista Networks is a computer networking industry-leading company, contributing client to cloud networking for large data centers, campus, and routing environments. In this report we shall do a deep dive into the makeup of this titan networking company, understanding their mission, exploring their ethics and security compliance, their code of ethics, and seeing how security operations are conducted and maintained through Arista's vulnerability management and device hardening guidelines. After studying these vital concepts that make up this networking company, we should be able to realize how this allows them to strategically plan for security. Through this process, we aim to learn exactly how Arista Networks operates and conducts its own security operations. This knowledge gained will then be conveyed in class and eventually taken and applied when entering the cyber workspace.

# TABLE OF CONTENTS

**Project Schedule Management**……pg.4

**Project Milestones**

1.About Arista's Mission and Vision.....pg.5

2.Company Culture and Core Values…….....pg.6-8

3.Business Integrity and Code of Ethics….....pg.9-13

4.Cybersecurity 101 Training and Professional Certifications……..... pg.14-15

**Deliverables**

1.Ethics and Security Compliance Policies and Laws.....pg.16

2.Device Hardening and Cloud Vision Data Retention and Backup……. pg.17-18

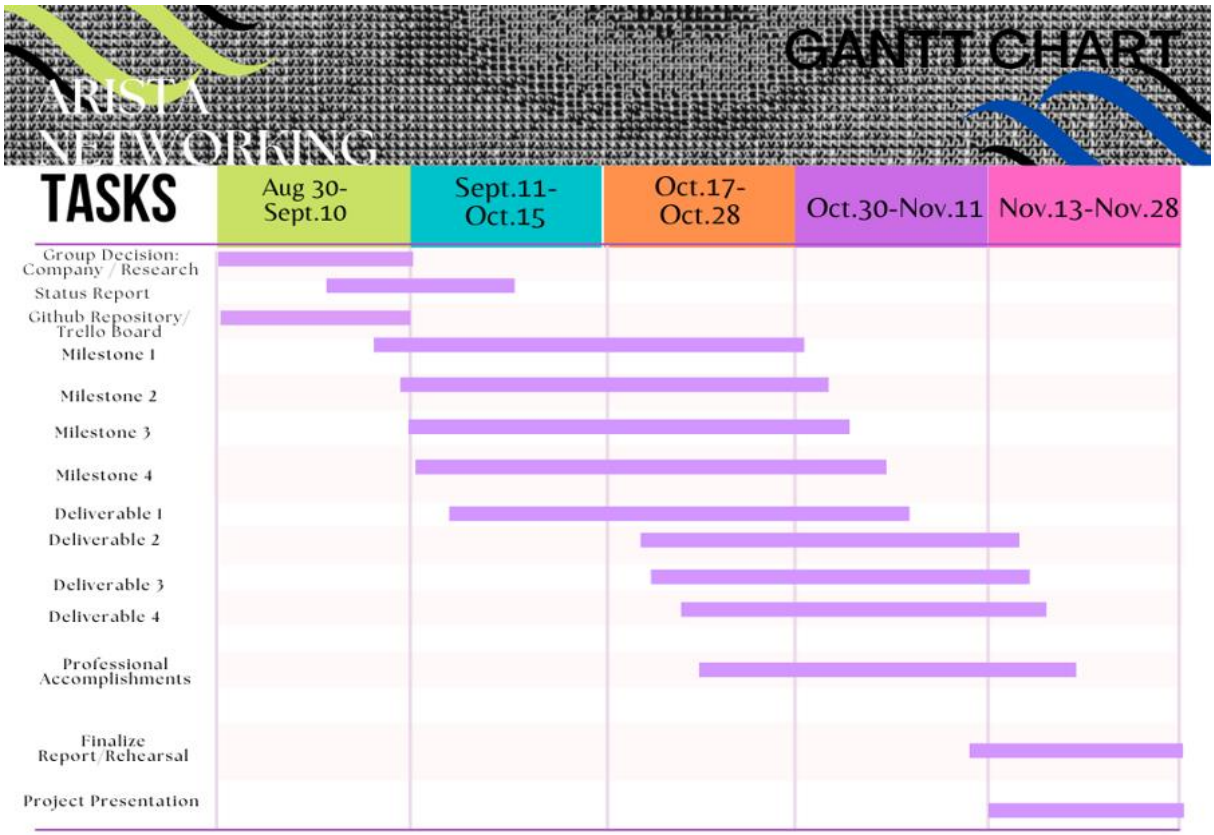
3.Vulnerability Management: Assessing and Treating Risks……pg.19

4.Arista Networks Security Measures……...pg.20-22

**Growth Reflection**…….....pg.23

**References**…….....pg.24

# PROJECT SCHEDULE MANAGEMENT




**Team Repository Link**
https://github.com/bparkoff-arch/AristaNetworks

**Team Trello Board**
F22-BP-GS-RR-Arista Networks | Trello

# Milestone 1: About Arista's Mission and Vision

Arista Networks is an industry leader in cognitive cloud networking for mission-critical data centers and campus environments. Arista's award-winning platforms deliver availability, agility, automation, analytics, and security through an advanced network operating stack. Arista was founded by industry luminaries Andy Bechtolsheim, Ken Duda and David Cheriton, launched in 2008 and is led by CEO Jayshree Ullal. Arista was recognized as a leader with the top score in current offering and strategy categories in The Forrester Wave™: Open, Programmable Switches For A Business wide SDN, Q3 2020 due to the great respected leaders that keep enriching their network platforms and innovations. This company went public in June 2014 and had more than 7,000 cloud customers worldwide.

Additionally, it has a prestigious set of customers, including Fortune 500 global companies in markets such as cloud titans, enterprise, financials, and specialty cloud service providers. The company delivers products across the data center and campus with routing and software solutions for monitoring and network detection and response worldwide. Its main headquarters is in Santa Clara, California but there are many offices worldwide.


*Figure 2.* Arista Networks Innovations Timeline (Source: Arista Networks Inc, 2021).

Arista Networks mission statement is: "We are committed to designing, manufacturing and delivering leading data-driven cloud networking solutions in an environmentally and socially sustainable manner" (Arista Networks, 2022). They believe that sustainability and business growth are closely linked to delivering products and technologies that truly enable our customer's success. Furthermore, the Arista Vision is "to drive for customer success in every aspect of what we do. We build and deliver innovative, high-quality products and services through commitment, innovation, and uncompromising focus on customer needs" (Arista Networks, 2022).

# Milestone 2: Company Culture and Core Values

Now that we know a bit more about what this titan company has to offer it is important to understand what their culture cherishes and practices. Every company defines a clear corporate culture but often, over time, the culture drifts to become something different or completely degrades to something unrecognizable to its founders and creators. Not so at Arista. The Arista Founders have underscored the importance of culture at all levels of the company and 15+ years later it is reinforced and still practiced with passion daily. Let's take a closer at the Arista's Way:

1. Drive for **customer success** in every aspect: support, quality, innovation, and experience
2. Do the **right thing** be it for products, quality, customers, and daily interactions
3. **Challenge status quo**, question traditional habits and be cost-effective
4. Develop alternative ways of achieving **disruptive** innovation in every function, preserving quality
5. Develop **agile and mobile teams** that can respond to priorities (as opposed to fixed or top-down organizations)
6. Maintain the highest level of **integrity** in conduct
7. Discuss, debate but quickly **align** to priorities
8. Treat your peers, vendors, customers with **respect** and develop a win-win partnership
9. Mentor individuals and develop teams for **overall success**, not persona, success
10. Cultivate **Arista pride** but never ego or arrogance in our culture

These top 10 practices are interconnected with one of Arista Networks core value: social responsibility. It is these practices that make them an efficient and hard-working team. The team looks out for one another and is working to meet a specific goal on time. With this in mind, the following are Arista's core values:

*Figure 3.* Arista's Product Stewardship
(Source: Arista Networks, 2022).

1. Enviroment: Arista implemented an Environmental Management System (EMS) that lays out our objectives for achieving pollution prevention, environmental protection

and monitoring, and continual improvements in the environmental performance of our operations. Backed by our Environmental Policy, the EMS provides a framework for monitoring of progress, internal employee training to embed sustainability into our business, external stakeholder engagement to promote continuous learning of best practices and setting measurable targets to drive performance. While they do not manufacture products in-house, they ensure that their contract manufacturers' facilities are ISO 14001 certified.

Arista practices this core value by committing to designing, manufacturing, and delivering data-driven cloud solutions in an environmentally and socially sustainable manner. They aim to integrate sustainability in every aspect of the product's life cycle, from the materials that make up it to the end of the product life. Also, they strive to reduce the hazardous materials in their products without degrading product performance and reliability as well as complying with applicable product related environmental laws and legislations on the restriction of certain hazardous substances.


*Figure 4.* Arista's Environmentally and Socially Sustainable IT Products. (Source: Arista Networks, 2022).

2.Social Responsibility: Arista celebrates their employees—who strive to differentiate by supporting a fun and inclusive culture that supports every member of the team regardless of background. Respect, integrity, innovation, passion, pride, and trust are all social core values valued by Arista's teams. They also encourage community engagement and partnership giving generously to numerous deserving non-profit organizations dedicated to developing impactful solutions to hunger, children's education and wellness, health, and environmental sustainability issues.


*Figure 5.* Arista provides over 1.1 million meals globally to those in desperate need. (Source: Arista Networks, 2022).

3.Governance: Arista believes that good governance leads to high board effectiveness, promotes the long-term interests of their shareholders, strengthens the accountability of the board of directors and management, and improves them standing as a trusted member of the community they served. High standards and policies ensure that Arista's team is meeting the objectives aligning with code of ethics. Furthermore, their board of directors are the gatekeepers of these standards, providing oversight in the long term strategic, financial, technical, operational, and organizational milestones of the company such as risk management and any plans designed to achieve the milestones.

*Figure 6.* Arista Governance Strategic Planning Jenga Blocks (Source: Arista Networks, 2022).

# Milestone 3: Business Integrity and Code of Ethics

Arista's success is built on a foundation of integrity, ethical business conduct, and always doing the right thing. This means adhering to the highest ethical principles in conducting our business and avoiding any activity that involves even the appearance of impropriety. You, as one of Arista's valued business partners, have a critical role in protecting the trust which investors, customers, colleagues, governments, and the global business community place in Arista. Any violation of this Code will result in action up to and including termination of your status as an Arista business partner. This Code defines minimum standards of business conduct and acceptable business practices. If any applicable laws and regulations are more permissive than this Code, you are expected to comply with this Code. If any applicable laws and regulations are more restrictive, you must always comply with those local legal requirements.

The following is Arista's Code of Ethics and Integrity Manual:

1. **Financial Integrity and Accounting**
   Arista business partners are expected to keep accurate books and records as it relates to the sale of Arista products. Any information and submissions that you provide to Arista and our joint customers will be complete, accurate, and not misleading. For Arista's resale partners this information includes, but is not limited to, deal opportunity registration, point of sale reporting, purchase orders, sales reporting, special bid or pricing requests, rebate requests, and reimbursement requests. Further, Arista partners will not engage in any false or misleading accounting practices, such as creating "slush funds", making unlawful or unethical payments to any parties involved in or exercising influence over the sale of Arista products, or paying for unauthorized expenses of such persons.
2. **Additional Discounts and Special Pricing**
   From time to time, Arista may provide partners with additional discounts, rebates, or special pricing ("Discount Pricing"). We expect that all partner requests for such Discount Pricing will be made in good faith and will provide an accurate justification and breakdown of how the monies will be used, for example, to pass on to the end customer, to account for additional services the reseller will provide to the end customer, as rebates validly earned and to be retained by business partner, etc. Please refer to your Arista partner agreement for details regarding Arista's right to audit your compliance with this policy.
3. **Anti-Bribery Compliance**
   Arista business partners must be committed to complying with all applicable US federal, state, and local anti-bribery laws, and any other applicable international and local anti-bribery laws, including but not limited to the United States Foreign Corrupt Practices Act ("FCPA"), the U.S. Federal Procurement Integrity Act, and the U.K. Bribery Act of 2010. You will not, directly or indirectly, make, offer, or issue authorization to pay any money, gift, bribes, kickbacks, or anything of value to anyone (this includes gifts, travel, meals, and entertainment), including government and public officials, employees, or representatives of any government, company, or public or international organization, or to any other party, that is or could be perceived as intended, directly or indirectly, to improperly influence or obtain any unfair competitive advantage to obtain or retain business related in any way to Arista products or services. You will fully comply with

any rules regarding tender and bid processes. You may not offer employment to government employees or officials if doing so would violate applicable laws.

4. **Antitrust and Competition Laws**
   Arista's business partners will demonstrate their shared commitment to fair competition by complying with all applicable antitrust and competition laws and regulations. It is not permissible for you and other Arista partners to do or attempt to jointly do any of the following: 1) fix or control prices for Arista offerings, 2) boycott suppliers or customers, 3) divide or allocate markets or customers, or 4) coordinate competing bids.
5. **Conflicts of Interest**
   Business partners will not engage in any activity with Arista or its employees, agents or affiliates that would interfere with contractual responsibilities to Arista or that may be perceived as a conflict of interest that could reasonably be likely to interfere with such responsibilities. Conflicts of interest may include, but not be limited to, Arista personnel being your officers, directors, or shareholders, payment of incentives to Arista personnel, or any economic or family relationship with Arista personnel. In the event you become aware of a conflict of interest, you must promptly notify Arista at www.arista.ethicspoint.com, which includes an option for making such reports anonymously.
6. **Insider Trading**
   As an Arista business partner, you may become aware of non-public information in the course of doing business with Arista. You have a duty to ensure that this information is not used for any improper purpose, for your personal gain or that of any other party, or for any other purpose that violates insider trading and securities laws. Failure to comply with these laws may expose you, and those that you inform, to severe financial and criminal penalties.
7. **Communications Regarding Arista**
   As an Arista business partner, you must ensure that all statements, communications, and representations to Arista customers are accurate, complete, and not misleading. Similarly, you will not make or attempt to make any written or oral agreements or commitments on behalf of Arista, including product feature or extended warranty commitments, without written authorization from Arista. Your communications will be conducted in a professional manner and will not defame or disparage Arista, other Arista business associates, competitors, or customers.
8. **Government Customers**
   Activities that may be appropriate when dealing with non-government customers may be improper and even illegal when dealing with government entities as well as businesses that are government-owned, government-controlled, or subject to government procurement rules ("Government Customers"). If you sell to Government Customers, you must observe all laws, rules, procurement regulations, and contract clauses that relate to the acquisition of goods and services by such Government Customers, whether such acquisition is a direct or indirect sale or is marketing or recommending Arista products and/or services for such sale. There may be special prohibitions or requirements arising from statutes, regulations, and government contracts or subcontracts that relate to the payment and/or receipt of fees and other benefits when dealing with Government Customers. In all government transactions you must ensure that payment is permitted before requesting fees or other compensation related thereto. You may be required to

disclose the potential fee in writing to the Government Customer. It is your responsibility to determine in each instance whether a potential fee is permitted and whether disclosure is required.

**9. Protection of Information**

Arista understands the importance of protecting intellectual property and other confidential information and expects the same from our business partners. Arista's business partners will maintain the confidentiality of the confidential information and other proprietary information that you may obtain in the course of your business relationship with Arista and our joint customers. You must not reproduce copyrighted software, documentation, or other materials unless properly authorized to do so. You must also observe any applicable data privacy requirements. You are responsible for making sure these restrictions are understood and followed by your employees and agents. Please see your Arista partner agreement or non-disclosure agreement for specific guidelines on your treatment of confidential and proprietary information.

In the course of your business relationship with Arista, you may be entrusted with the Personal Data of our employees and/ or customers which is protected under both regional and national data privacy laws as well as certain contractual obligations. Therefore, in additional to the foregoing, you must establish and maintain data security policies and procedures designed to ensure the following: (a) security and confidentiality of Personal Data; (b) protection against anticipated threats or hazards to the security or integrity of Personal Data; and (c) protection against the unauthorized access to or use of Personal Data. You must permit Arista to monitor and/or audit your compliance with this Section during regular business hours upon not less than 48 hours' notice to you and provide Arista copies of audits and system test results acquired by you in relation to the data security policies and procedures designed to meet the requirements set forth herein. If there is any actual or suspected theft of, accidental disclosure of, loss of, or inability to account for any Personal Data by you or any of your subcontractors and/or any unauthorized intrusions into your or any of your subcontractors' facilities or secure systems (collectively, a "Breach"), you must immediately, (a) notify Arista, (b) estimate the Breach's effect on Arista, (c) investigate and determine if a Breach has occurred with respect to Arista's Confidential Information, (d) specify the corrective action to be taken and (e) take corrective action to prevent further Breach. You must, as soon as is reasonably practicable, make a report to Arista including details of the Breach and the corrective action you have taken to prevent further Breach.

You must provide enough detail for Arista to identify and for Arista to notify the affected Data Subjects as to the facts and circumstances of the Breach. Additionally, you must cooperate with all government regulatory agencies and law enforcement agencies having jurisdiction and authority for investigating a Breach or any related known or suspected criminal activity. Except as may be strictly required by applicable law, you agree that you will not inform any third party of any Breach without Arista's prior written consent; however, if such disclosure is required by applicable law, you agree to work with Arista, at no additional cost to Arista, regarding the content of such disclosure so as to minimize any potential adverse impact upon Arista and the affected Data Subjects. Each party agrees to indemnify and hold the other party harmless against any and all third-party

claims, loss, damages, liability, and costs of any nature, including without limitation, reasonable attorneys' fees and expenses arising from: (a) the breach of this Section 8; and/or (b) the unauthorized disclosure or use of any Personal Data by you. For purposes of this section, "Personal Data" is used as such term is defined under the European Union's General Data Protection Regulation or any similar law or regulation applicable to the parties hereto as in effect now or during the term of this Agreement.

10. **Export Compliance**

    Arista business partners must have and follow a documented trade compliance program designed to ensure compliance with U.S. and all other applicable export, import and sanctions laws and regulations. Except under license or as otherwise permitted under such laws and regulations, you shall not export, re-export, transfer, divert, release, import, or disclose to any other person or entity any (1) Arista hardware, software, or service ("Arista Products") or (2) technology relating to current or future Arista Products. Nor shall you make any use of any of the Arista Products or technology in violation of the foregoing provisions, or cause Arista to unknowingly engage in any such acts.

11. **Responsible Business Partner Conduct**

    Business partners will conduct themselves in a professional manner while representing Arista products and services in the marketplace. This means treating all persons with dignity and respect in a businesslike manner while marketing, selling, or supporting Arista products and services.

12. **Relationship of the Parties**

    Arista and our business partners are independent contractors, and neither party shall be considered the agent of the other party for any purpose whatsoever. Nothing in this Partner Code of Conduct shall be construed as establishing a partnership or joint venture between the parties.

13. **Human Rights; Health and Safety**

    Arista is committed to upholding the human rights of workers and to treating them with dignity and respect as understood by the international community and expects the same from our business partners. By way of example, you must comply with fair labor standards that permit freely chosen employment, prohibit child labor and human trafficking, and allow for reasonable working hours and payment of fair wages and benefits. You must avoid inhumane treatment of workers. You must be committed to a workforce that is free of harassment and unlawful discrimination and which allows for freedom of association of personnel. You must maintain a safe and healthy work environment. You must maintain policies and procedures to address similar human rights-related workforce practices of your suppliers. In addition, where applicable, Arista's business partners must have policies and procedures in place to reasonably assure that any "conflict minerals" are obtained from sources that are committed to worker health and safety. Arista is committed to ensuring its products and services are not used to support human rights abuses, such as through mass communications surveillance activities, that are unlawful or that otherwise violate international norms. When selling or supporting Arista products or services, Arista business partners must investigate red flags that indicate an end-use may support human rights abuses and take necessary steps to resolve such concerns or terminate such activity.

14. **Diversity and Inclusion**

Arista strives to build an inclusive culture that encourages, supports, and celebrates the diverse voices of our employees. We expect that our business partners share this commitment by making efforts to hire a diverse workforce, engage with Minority- and Women owned Business Enterprises (MWBEs), and support under-represented affinity and professional organizations.

15. **Sustainability and Environmental Protections**
    Arista recognizes our important role in protecting the environment, and we expect that our business partners will share in this commitment. Arista's business partners must comply with all applicable environmental laws and regulations and make efforts to reduce waste by implementing appropriate conservation measures.
16. **Cooperation**
    Arista's business partners are expected to cooperate fully with any of Arista's periodic information and documentation requests. This includes any requests made while conducting new partner due diligence, as well as any audit requests made by Arista in accordance with your partner agreement.
17. **Certification**
    Upon request by Arista, business partners will have an authorized representative certifying that they have read and understood this Code and that your personnel are committed to upholding the standards described herein.

# Milestone 4: Cybersecurity 101 Training

*Figure 7.* Arista Cybersecurity 101 Training. (Source: Arista, 2020).

Cybersecurity is a world-wide concern and requires businesses to defend against a growing number of increasingly complex threats. This requires hardening infrastructure, scheduling regular updates, and applying patches in a timely fashion. It also requires addressing human errors in cybersecurity. It is more important than ever for businesses to take the time to provide ongoing employee education about cybersecurity threats. Employee error remains a top cybersecurity vulnerability for any business. That is why it is of upmost importance for a company to keep up with giving their employees cybersecurity training, so they are fully equipped and knowledgeable in security protocols. As a matter of fact, at Arista Networks they offer a cybersecurity training plan known as cybersecurity 101 which takes place on day one for a newly recruited employee and provide quarterly schedules to keep training them. They also host a training in October, "Cybersecurity Awareness Month."
The cybersecurity 101 training plan includes the following educational topics:

**Threats Overview**

- Malware: software specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

- Ransomware: a specific type of malware that disables a network or data and demands a ransom be paid in exchange for a key to regain access to the network or recover the data.

- Social engineering: the use of deception to manipulate individuals into sending or giving confidential information to a cybercriminal who may use the data for fraudulent purposes.

- Phishing: the act of sending emails appearing to be from reputable companies or persons in order to trick individuals into revealing personal information, such as passwords and credit card numbers.
- Emerging threats: Artificial intelligence is a quickly rising threat to cybersecurity. With deep fakes and synthetic identities, AI is allowing cybercriminals to impersonate reputable persons better than ever.

- Deep fakes: using audio or video developed using AI or machine learning to alter or create content that misrepresents someone.

**Password Policies**

- Strong passwords: create a strong password at least 16 characters long with lowercase and uppercase letters, symbols, and numbers.

- Change passwords: implement procedures to force password changes every 60 or 90 days. Use a different password for every account. Never share your passwords.

- 2FA: Two factor authentication combats human error by adding an extra layer of security. In addition to a username and password, a temporary code is sent to a trusted device as a third confirmation of identity. 2FA combats human error by preventing cybercriminals from logging into accounts with stolen usernames and passwords.

- Web Protection: if you receive a link, don't click on it, or copy/paste it. Instead, type the website address directly into the browser to log into your account.

- Email Protection: check for misspelled email addresses, misspelled words in the body of the email, a sense of urgency, email subjects that do not make sense or are out of character for the sender, or emails that do not relate to employee positions within the company. Be suspicious of emails that say, "here are the files you requested" when you have not requested anything. Cybercriminals have evolved and their techniques have become more sophisticated. If employees can only remember one thing, it should be not to click on a link or open an attachment if they're not 100% positive that it's safe.

- Social Engineering Protection: set spam filters to "high". Read the email slowly and thoroughly before responding. Be sure to research the contents of the email. Verify through alternative communication methods that the request is legitimate (call the person using the phone number in the directory or verify with your manager.

In addition to email, phishing, and social engineering there are other important topics to include such as: Wi-Fi security, VPNs, USB drives, and external websites. Arista Networks loves to motivate their employees to be mindful of security threats by hosting workshops, phishing tests, and security breach simulations, rewards those that demonstrate understanding of the concepts and at the end require them to provide feedback of the training.

# Deliverable 1: Ethics and Security Compliance Policies

At Arista governance is one of their highly valued core values. They have set policies and procedures in place to ensure that their operations, employees, and suppliers are held to rigorous standards regarding their conduct and compliance with expectations and regulations. The following are just a few of their ethical and security compliance policies:

**ANTI-CORRUPTION**

We are committed to complying with applicable international and domestic anti-corruption laws, including the U.S. Foreign Corrupt Practices Act ("FCPA") and the U.K. Bribery Act. Our Anti-Corruption Compliance Policy and Guidelines outline the parameters of what is acceptable and what is not permissible from an anti-corruption point of view. Companies like Arista can be held liable for the bribery acts of third parties, including commercial intermediaries and other agent representatives and joint venture partners. To ward against these activities, we have established procedures for conducting due diligence on channel partners engaging in international sales, and manufacturers, suppliers, logistics providers, customs agents and other third parties that may be directly or indirectly interacting with foreign officials on our behalf.

**ANTI-COMPETITIVE BEHAVIOR**

We rigorously observe applicable antitrust or competition laws of all countries or organizations. Under our Code of Ethics and Business Conduct, anti-competitive agreements are prohibited.

**WHISTLEBLOWER POLICY**

Our Whistleblower Policy encourages transparency, facilitates confidentiality, ensures appropriate handling of complaints, and provides multiple avenues for employees and non-employees alike to submit concerns around accounting or auditing matters via our whistleblower website (www.arista. ethicspoint.com), and our ethical/violation hotline (telephone numbers available at www.arista.ethicspoint.com).

**BAYSHORE'S PALLATON: DEPLOY, EVALUATE AND ENFORCE POLICY**

The flexibility of the Pallaton language enables policies to be expressed uniformly across multiple device types and security categories (firewalls, application security, etc.). Pallaton rules are applied to streams of network device data and works in terms of actual wire protocols. Pallaton is so powerful that it is capable of expressing the requirements of different security functions. This enables different teams to coordinate and synchronize policy objects. Pallaton works in a run-time context, inspecting web flows and file shares. The following features make it is easy to work with:

a) Rules are created in a GUI and include policy objects from many protocols.
b) Policies are expressed in terms of applications and users rather than in firewall rules or IDS signatures.
c) The language is predicate-based and customized to the specific context of the network.

Bayshore SE and Pallaton work in concert with Arista EOS. The Bayshore SE can plug directly into Arista data center switches at the TAP point or run virtually.

# Deliverable 2: Device Hardening

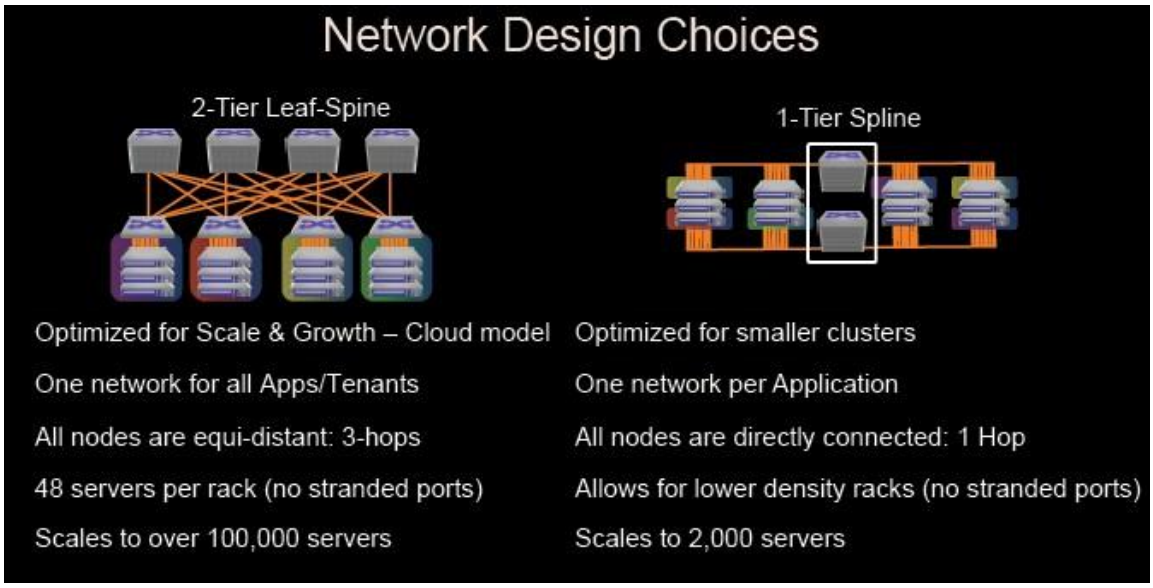



*Figure 8.* Arista Network Design Choices for Large Enterprises. (Source: Morgan, 2020).

Arista Networks security engineers complement their network and cloud security products by practicing the best configuration during the installation and operation of the infrastructure. Arista's product family encompasses a variety of software products including EOS, DANZ Monitoring Fabric (DMF), Cloud Vision (CV) and Cloud Vision Wi-Fi (CV Wi-Fi), each of which is designed with safe execution in mind. As a result, many types of common programming issues are caught during development or not able to occur due to the frameworks and policies in use.

The following list provides some examples of fundamental design choices that form part of Arista's software design process:

- Safe language choices ensure mitigation against common flaws such as buffer overflows, protection against access of uninitialized data and other memory management issues.
- Use of highly audited libraries where necessary (e.g., common security protocols).
- Prevention of resource leakage using safe memory operations, bounds checking, reference counting and Val grind analysis.
- Pipelined execution models organized around single threaded functions to avoid race conditions and deadlocks.
- Strong input sanitization for internal and external APIs to prevent malformed data injection.
- Memory-safe virtual machines and Containerized execution to provide process separation and abstraction from the underlying OS.
- Principle of least privilege to limit the permissions given to processes and users, avoiding malicious escalation.

- Both the design of new Arista features and maintenance of existing features are done with security as a goal.

    - Engineers are provided training on secure coding practices and how to implement them in their code. By having a series of guidelines and examples engineers can create features that are designed to be secure from the start and can recognize previously written insecure designs.

    - The usage of security critical open-source libraries is limited to a few well understood libraries. This serves to limit the surface of the attack as well as make analyzing the usage of said libraries in the codebase easier.

    - Awareness and review of common attack vectors and the associated mitigations is an important part of security at Arista. The PSIRT team makes sure to stay aware of common patterns in insecure code and how to detect them. Information on rising trends is integrated into the training as well as companywide announcements. By making sure to keep a dialogue open within the company on security, engineers on all teams are able to keep secure coding principles in mind when writing code.

If interested in learning more about Arista Device Hardening Guidelines, they provide regularly updated hardening guides and security recommendations through living documents available via EOS Central.

# Deliverable 3: Vulnerability Management: Assessing and Treating Risks

Arista has a four-component process they follow concerning vulnerability management. This is highly efficient, as vulnerability management is a complex process, and has many factors that need to be considered, especially in an organization as big as theirs. By breaking vulnerability management into these four processes, design choices for vulnerability avoidance, vulnerability detection, vulnerability communication, and security assessment testing, this successfully isolates and gives a clear and coherent goal of the different components and processes that must be completed to ensure a successful and efficient vulnerability management process at Arista Networks. Arista also makes it clear product security must also complemented with best practice configuration at installation and operation of infrastructure, as well as provides hardening guides and security recommendations through their support page's living documents. The Arista vulnerability management will be broken down in the section below.


*Figure 9.* Arista Networks Vulnerability Management Stages (Source: Arista Networks, 2021).

# Deliverable 4: Strategic Planning for Security

Arista Networks relies heavily on cloud networking and has taken extensive security measures to help maintain the confidentiality, integrity, and availability of their cloud networking operations. Zero Trust Networking is the approach Arista uses with its cloud operations, which is patterned on the NIST guidance in the 800-207 zero-trust framework. With this approach, the concept of trust inside the network that connects to an untrusted network through a traditional firewall is eliminated, as well as the implicit trust associated with network location. With this considered, all the responsibility is placed on continuously monitoring all devices and applications accessed for mal-intent and responding quickly.

The framework of Arista's Zero Trust Cloud Networking is based upon three foundational concepts, Situational Awareness, the visibility of all assets and workloads, Enforcement, restricting access to required connections, and Continuous Monitoring – never trust and continually verify. Arista leverages many tools that help them successfully and continually execute this zero-trust policy, keeping their cloud networking operations secure and functional. Using Arista's best switches, Cloud vision network automation, and telemetry, the Arista network detection and response (NDR) platform, and the Arista DANZ Monitoring Fabric (DMF), it is apparent they are taken many measures to ensure the security of their cloud operations. The zero-trust portfolio eliminates the need for several networking monitoring and security tools, instead delivering this unified architecture which provides real-time visibility to the threat posture across the network, with the ability to take immediate action.

Cloud Vision provides Arista profiling and classification of connected endpoints through Device Analyzer, as well as providing visibility into switch performance, network compliance, and flow analytic processing. Cloud vision provides a nicely configured GUI, which provides a simple compliance dashboard that reports observed PSIRT security advisories within a network, as well as any known exposures to software defects that are relevant, and out-of-band non-sanctioned changes made to switches under management.

Cloud Vision's compliance tab, showing us bug exposure, security advisories, and configuration and software image, showing the secure and exposure rate, as well as the compliant and non-compliant rate, and specifying the devices that have issues.

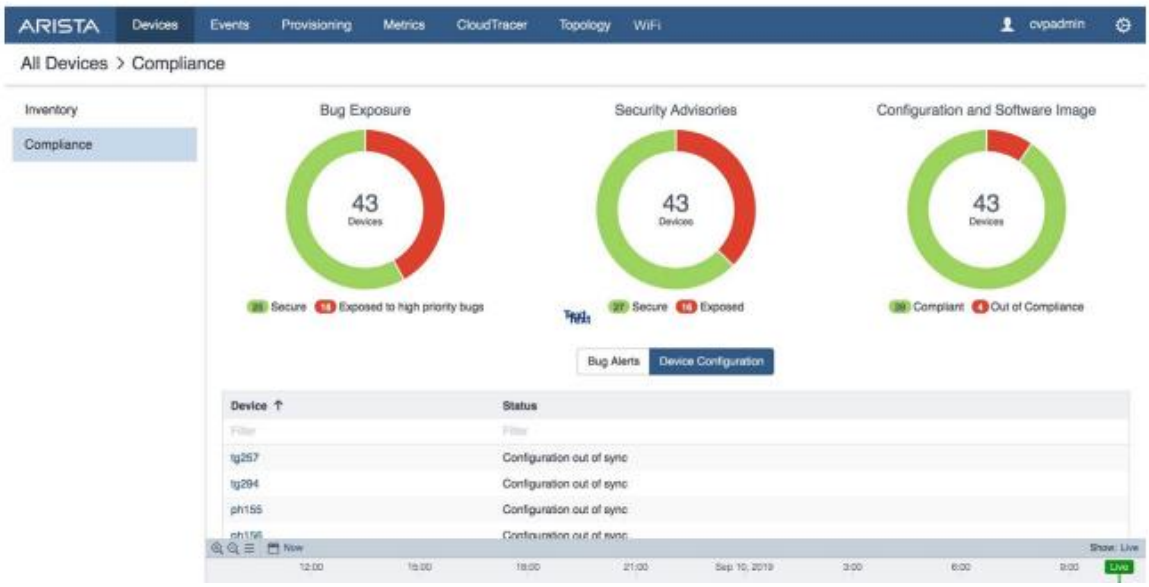



*Figure 10.* Cloud Vision Configuration Tab Content (Source: Arista Networks, 2022).

Cloud Vision also offers flow analysis, sampled or non-sampled flow information patterned via SFLOW or IPFIX, which provides the ability to query conversations of who is talking to whom and flow traffic patterns. Arista Cloud Vision makes use of advanced network telemetry, which provides linkage of the network infrastructure and critical business application performance, while ensuring visibility of critical real-time information. This telemetry works in conjunction with applications, and does not slow the pace of IT operations, it dramatically reduces application downtime as well as network operational cost through improved real-time system and network performance visibility.

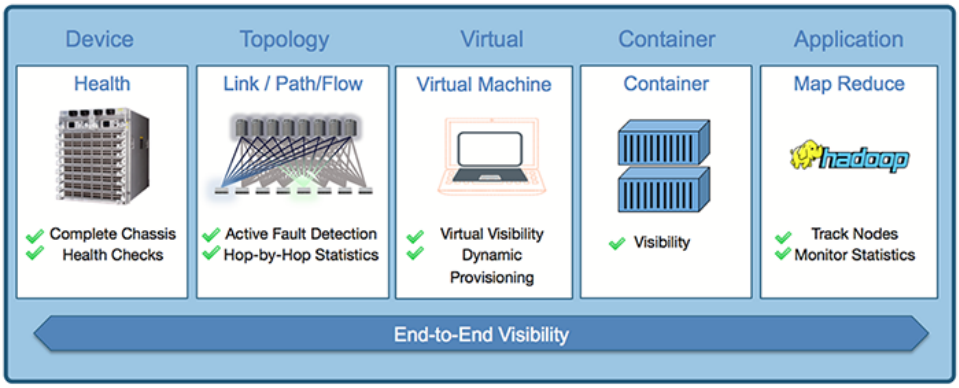



*Figure 11.* Network Telemetry (Source: Arista Networks, 2022).

The next powerhouse of a tool Arista uses in conjunction with their zero-trust policy is Arista NDR (network detection and response). Arista NDR is built upon a foundation of deep network

analysis across campus, data center, IoT, and cloud workload networks. As opposed to other NDR solutions, Arista NDR parses a little over three thousand protocols and processes, including layer 2 through layer 7 data, while performing encrypted traffic analysis. Entity, another tool, provides situational awareness by using this information thereafter by autonomously profiling entities such as devices, users, and applications, while keeping track of these communications for historical forensics.

For threat detection, Arista NDR incorporates Adversarial Modeling. This capability enables autonomous threat hunting for complex attacker tactics, techniques, and procedures (TTP), by sending a vocabulary to express and identify patterns of behavior, even if they occur over an extended period of time, across a variety of protocols and impact multiple network assets. Arista AVA (Autonomous Virtual Assist) is the world's first AI- based security expert system, which performs autonomous threat hunting and incident triage. It uses artificial intelligence, open-source intelligence, and human expertise to connect the dots across dimensions of time, entities, and protocols, which enables the solution to present end-to-end situations to the end-user. It is now becoming clear how Arista is using these different tools for constant analysis and monitoring of the network and network data to abide by their zero-trust policy.

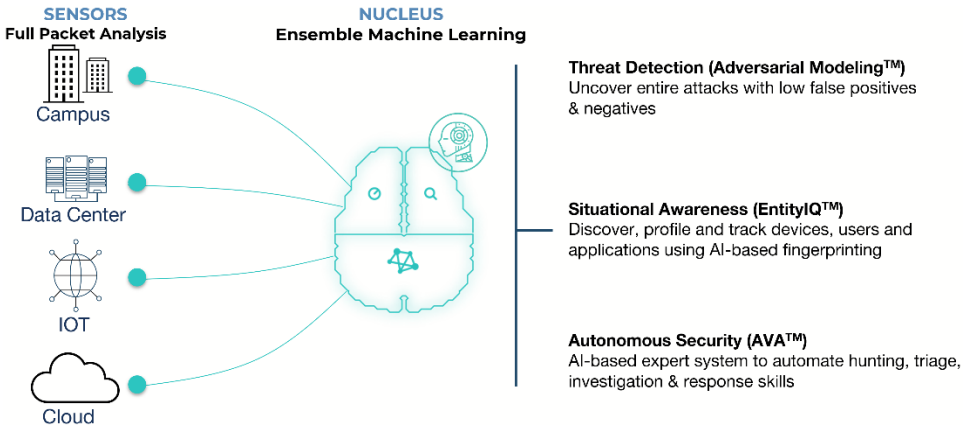



*Figure 12.* Arista NDR Graphical Representation (Source: Arista Networks, 2022).

Within their zero-trust cloud networking solution, Arista also utilizes DANZ Monitoring Fabric (DMF). DMF is a next generation NPB (Network Packet Broker) which is designed for pervasive, organization-wide visibility and security, enabling IT operators to pervasively monitor and mirror all traffic, while providing deep hop-by-hop visibility, predictive analysis, and scale-out packet capture. In Arista's zero-trust cloud networking policy, we get many insights into how Arista can consistently execute secure, efficient, and resourceful cloud networking processes.

# Growth Reflection

This project has helped us gain a deep understanding of the ways a network company implicates network theory and strategies it takes to manage vulnerabilities. Vulnerabilities are never going to go away, and it can sometimes be something a company fails to look into in depth and plan for because they are so caught up with building and deploying new technology. However, security is a vital need for those products, and we had the opportunity to engage with the process Arista takes to protect their systems and realized how cloud networking is strongly appreciated for protecting the confidentiality, integrity, and availability of their cloud networking technologies, which makes up most of their company. We also enjoyed learning about their Cybersecurity 101 Training Plan and how they motivate their employees to take the trainings by hosting workshops, phishing tests, and security breach simulations, rewards those that demonstrate understanding of the concepts and at the end require them to provide feedback of the training.

Besides all the interesting material we learned from the extensive research we conducted of their company especially, for policies and code of ethics we did ran into some challenges. I would say our greatest challenge had to do with deciding what information we should implement into the report. This company is very transparent and had a lot of white papers to offer besides what was offered on the website but, we managed to figure out what would be more relevant to the milestones and deliverables and what should be left out.

# References


[1] Westfall, R. (2021, October 18). *Arista networks: Powering Swifter 400G adoption across cloud and enterprise environments – new futurum research report*. Futurum Research. Retrieved November 22, 2022, from https://futurumresearch.com/research-notes/arista-networks-powering-swifter-400g-adoption-across-cloud-and-enterprise-environments-new-futurum-research-report/

[2] Arista Networks Inc. (2021, October 22). *The arista way: Practicing and cherishing our ongoing culture*. Retrieved November 22, 2022, from https://www.arista.com/assets/data/pdf/TheAristaWay.pdf

[3] Arista Networks Inc. (2021, October 22). *Arista Networks Corporate Responsibility Report*. Retrieved November 22, 2022, from https://www.arista.com/assets/data/pdf/Arista_CRR_2021.pdf

[4] Arista Networks. (2022, May 11). *Corporate responsibility*. Arista Networks. Retrieved November 22, 2022, from https://www.arista.com/en/company/corporate-responsibility/environment

[5] *Www.arista.com*. (2020, March 4). Retrieved November 24, 2022, from https://www.arista.com/assets/data/pdf/Whitepapers/White-Paper-Employee-Training-Cybersecurity-101.pdf

[6] Arista Networks. (2022). *Arista zero trust security for cloud networking* [White paper]. Retrieved November 15, 2022 from Arista Networks: https://www.arista.com/assets/data/pdf/Whitepapers/Arista-Zero-Trust-Security-for-Networking.pdf

[7] Arista Networks. (2021, October 6). Device hardening and vulnerability management - arista. Arista Networks. Retrieved November 16, 2022, from https://www.arista.com/en/support/product-documentation/vulnerabilitymanagement

[8] *Arista Networks, Inc. partner code of ethics and business conduct*. (2022). Retrieved November 27, 2022, from https://www.arista.com/assets/data/pdf/Arista-Partner-Code-of-Ethics-and-Business-Conduct.pdf

[9] *Bayshore Arista Solution Guide*. (2021). Retrieved November 27, 2022, from https://www.arista.com/assets/data/pdf/JointPapers/Bayshore-Arista-Solution-Guide.pdf

[10] Morgan, T. P. (2020, November 6). *Arista flattens networks for large enterprises with splines*. EnterpriseAI. Retrieved November 27, 2022, from https://www.enterpriseai.news/2013/11/04/arista-flattens-networks-large-enterprises-splines/