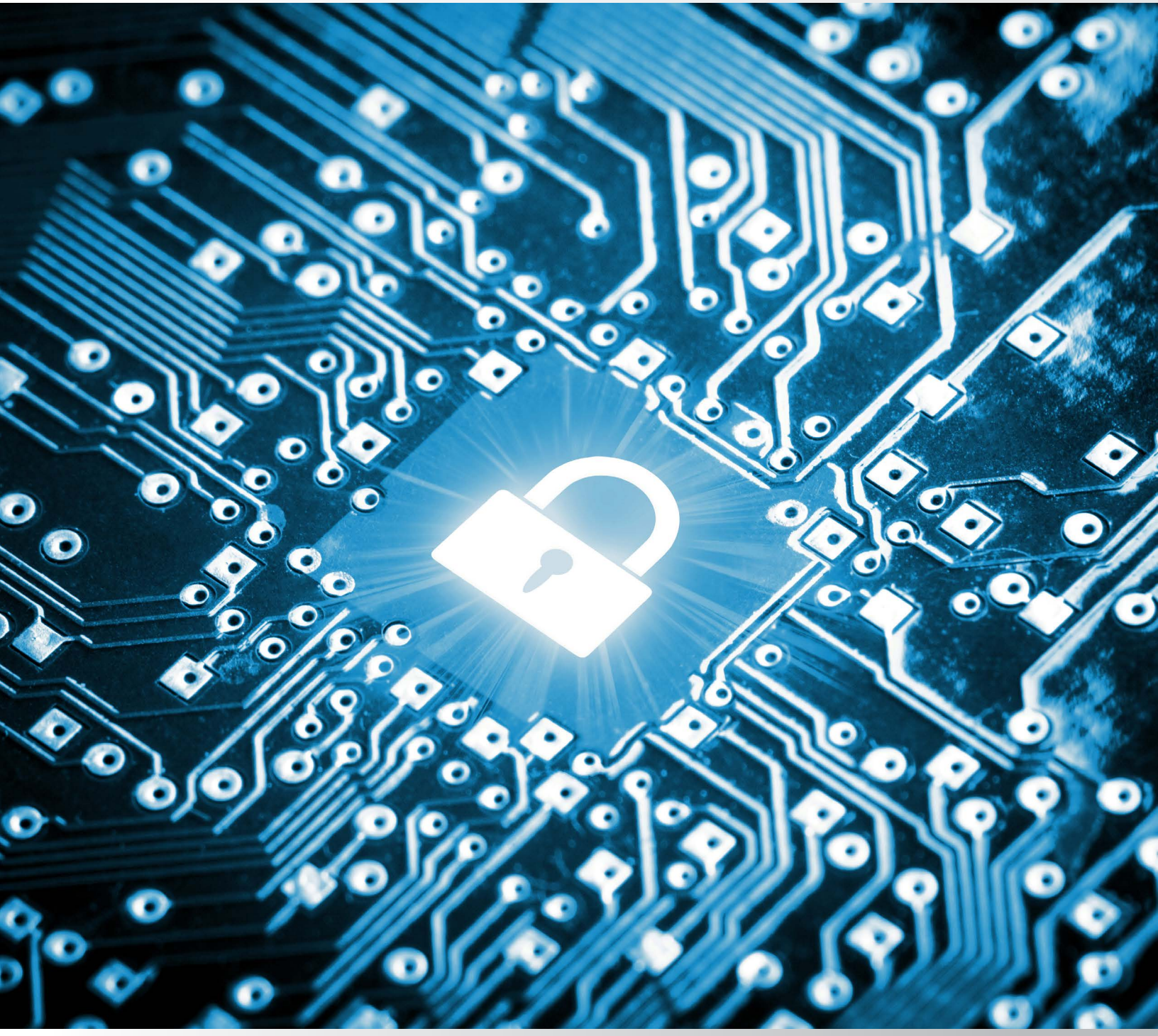
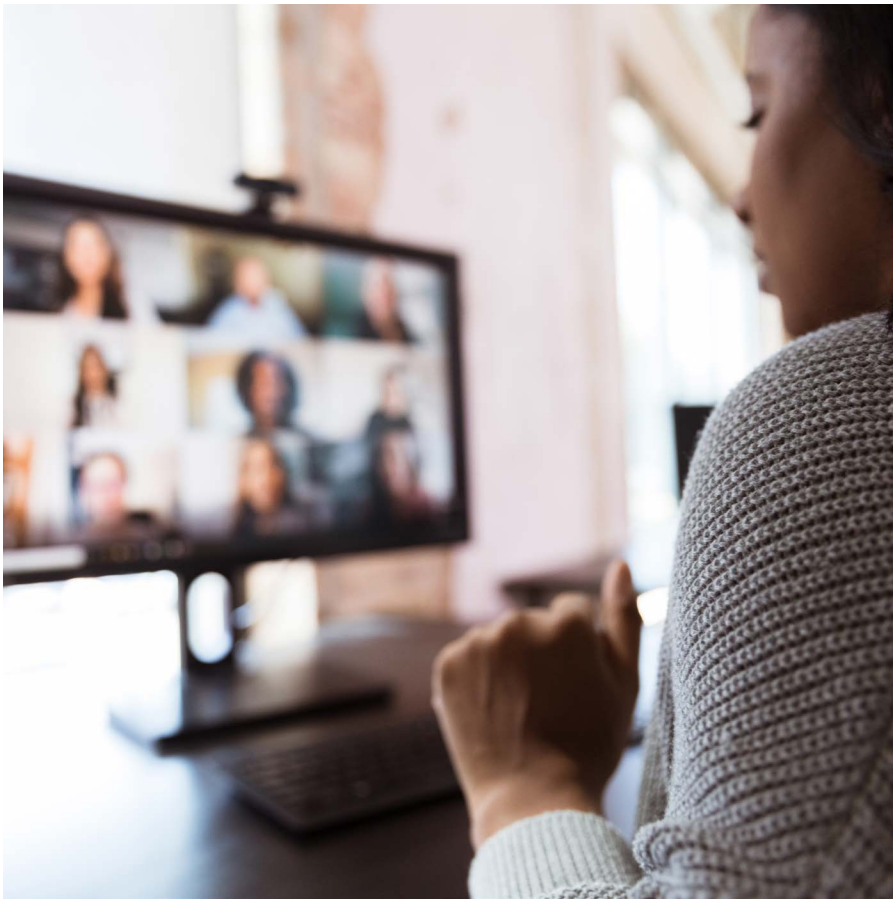
Employee Training: Cybersecurity 101



A survey conducted in January 2022 found that 2 in 5 employees sent emails to the wrong recipients, sometimes resulting in being fired or losing clients, and 1 in 4 employees fell for a phishing scam at work.[1]

Introduction

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 the human element 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. Network Administrators can implement security measures with endpoint security, data encryption, and virus blocking, but human error and psychology are still variables at the root of many cyberattacks. A survey conducted in January 2022 found that 2 in 5 employees sent emails to the wrong recipients, sometimes resulting in being fired or losing clients, and 1 in 4 employees fell for a phishing scam at work.[1]

These types of errors result in more opportunities for cybercriminals to take advantage of vulnerable network access points and deliver malware to hold business data for ransom. It is imperative to act strategically in the fight against cyberattacks. The most effective mechanism is to have well-informed employees, fully equipped and proficient in security protocols.

The Human Element

- A payroll account employee at Scotty's Brewhouse was the victim of an email phishing scam that resulted in 4,000 employee W-2's being sent directly to a cybercriminal.[2]
- Due to an employee mistake at Wyze Labs, camera information, Wi-Fi network details, and email addresses of 2.4 million customers were exposed.[3]

Similar stories echo across the digital landscape as hackers use employee error as points of entry. Every employee must methodically adhere to a step-by-step procedure and employ the same practices for it to become second nature. When security protocols are properly enforced, understood and followed by every employee, it is one of the best defenses against malicious threats.

All it takes is one wrong click from a well-meaning employee to compromise company data. In many cases, that one click is all a cybercriminal needs to gain access to an entire network. The number one cyber attack scheme in the US in 2021 was phishing or similar (54% of all reported attacks).[4] Phishing attacks rely on a person to take an action to collect confidential information, gain access to systems, or receive payments.

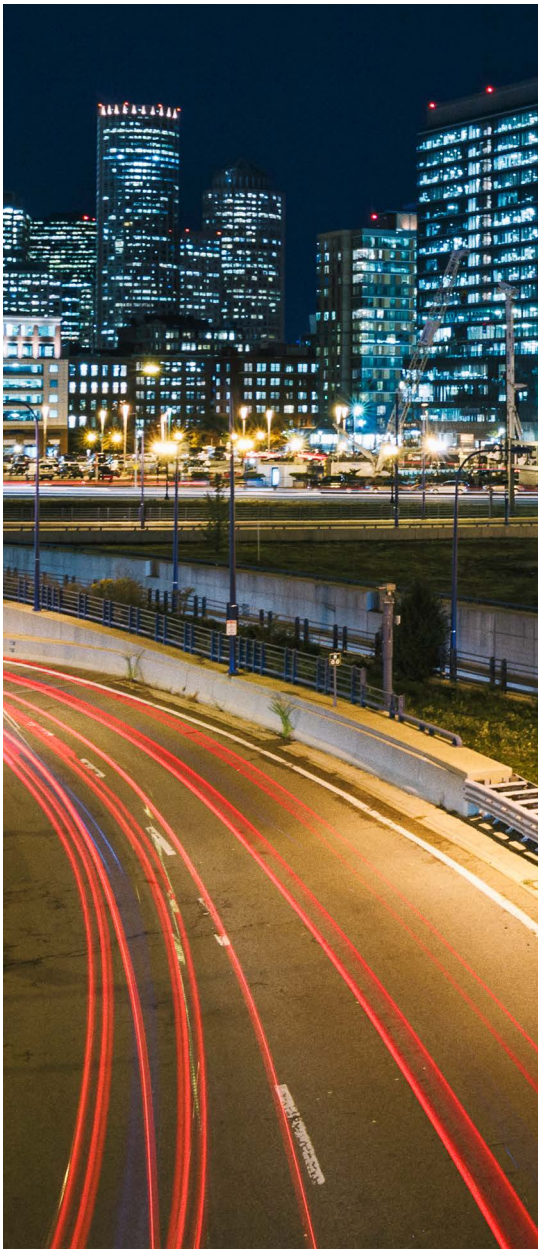
Types of Human Error include:

- **Email Error:** Sending an email to the wrong recipient and accidentally disclosing confidential information. According to a 2020 survey both corporate and personal email are the leading applications for accidental data leaks.[5] Sharing files with sensitive information should be done via secure links. These links should include an option of withdrawal in case data is sent to the wrong recipient.
- **Phishing attack:** There are many cases of employees thinking they are communicating with a colleague, boss, or authorized vendor when it is really an imposter gaining access to critical business information. This tactic involves a level of deception where the victim provides vital information to a fraudulent source that appears credible.
- **Lack of security awareness:** Technological competence is a critical security barrier. A survey for Canon found that one third of respondents said a tech skills gap hinders the adoption of cybersecurity solutions more so than budget constraints.[6]

Because the risk to businesses is so great if they are hacked, it is imperative to provide continual training of cybersecurity threats and their prevention.

Cybersecurity Education Plan and Topics

When providing cybersecurity training, create a quarterly schedule to communicate with employees. Focus on one or two topics below and rotate through all the topics over time. Cybersecurity can be an overwhelming subject for employees, and breaking down training into smaller training components delivered periodically will make it easier for employees to retain. Training should include the following Cybersecurity Education 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:** A common form of social engineering. This is 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

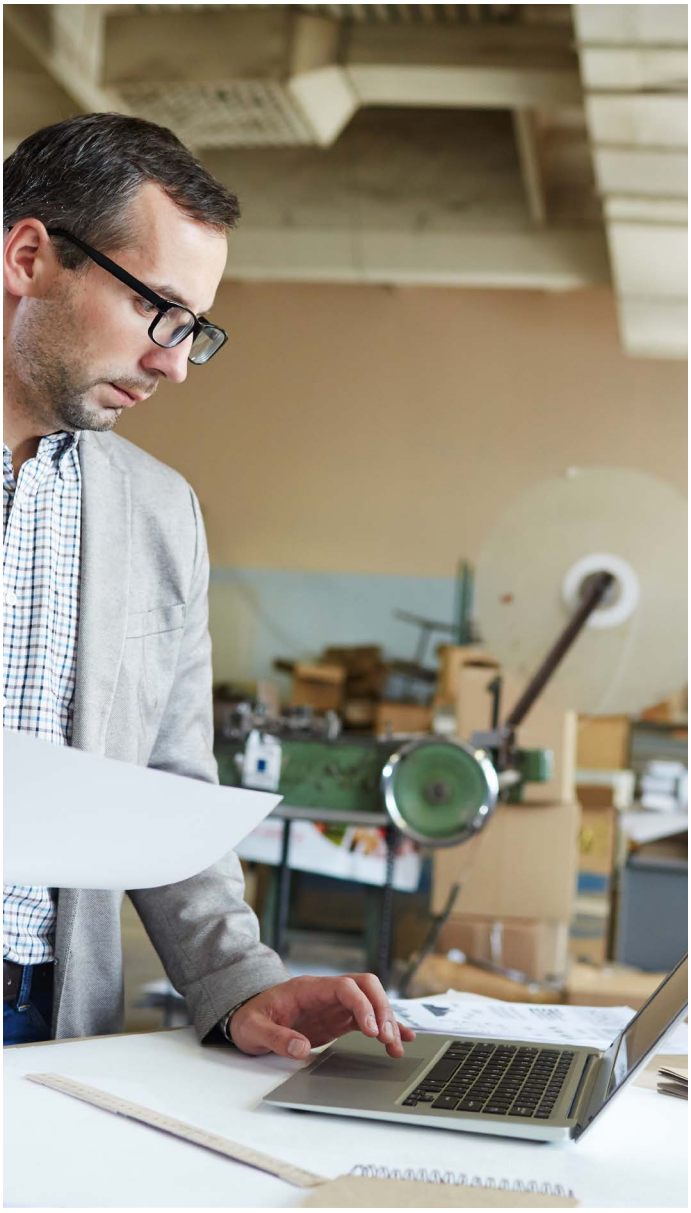
- **Strong passwords:** Create a strong password at least 16 characters long with lowercase and uppercase letters, symbols, and numbers.
- **Change passwords:** Implement procedures to force password changes every 60 or 90 days. Use a different password for every account. Never share your passwords.
- **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

- **What to look for:** Criminals will clone well-known websites to make themselves look legitimate. 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.
- **What to avoid:** Do not pass on confidential data to external websites or accounts that are unfamiliar or unencrypted. Remember the rule of thumb: if in doubt, don't give it out.

Email Protection

- **What to look for:** 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.
- **What to avoid:** Do not respond to an unfamiliar or unrecognized email. Be sure to follow standard protocol or checks and balances prior to sending any critical data such as payment or account information.



Social Engineering Protection

- **What to do:** 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).
- **What to avoid:** Do not send private or confidential information via email unless the request has been fully vetted and verified.

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. Direct employees to IT for any concerns about suspicious emails or links. The lessons employees learn about privacy and security are lessons that can be applied in their personal lives outside of work.

Cybersecurity Training Tips

Cybersecurity training should start on Day 1 as part of the employee onboarding process, followed by the quarterly training updates. A training program equips employees to feel more knowledgeable and secure with practical skills needed to identify possible attack scenarios and how to collect incident data to submit to Network Administrators. Additionally, it encourages employees to adopt the mindset of the company's culture and put cybersecurity at the forefront.

Cyber Awareness

Having a security process in place is the backbone of a strong business infrastructure. A security process is only fortified over time with continuous training. Therefore, training shouldn't begin and end on Day 1 of onboarding. Throughout the year employees should be refreshed to stay updated. A fun way to infuse the importance of cybersecurity into the veins of your company is to celebrate National Cybersecurity Awareness Month in October.

The larger goal is to create a company culture committed to "Cyber Awareness". This awareness directly correlates to risk reduction. What this does is build an army of employees who essentially act as a "human firewall".

Engage Your Employees

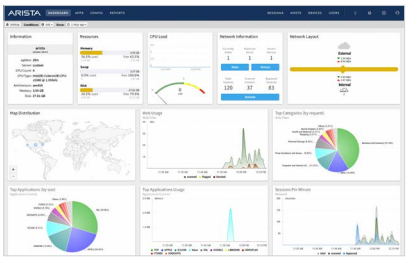
Make employee awareness a priority to keep employees motivated. Workshops, phishing tests, and security breach simulations are all excellent ways to train employees and keep them mindful of threats. Make exercises interactive to encourage employee engagement, and reward those employees who show understanding of proper security practices. At the end, provide an evaluation, feedback, or results to give employees something to work towards and to motivate them to stay alert.

Sources

1. https://www.tessian.com/resources/psychology-of-human-error-2022/
2. https://www.scmagazine.com/news/breach/4k-w-2-compromised-in-scottys-brewhouse-phishing-attack
3. https://www.geekwire.com/2019/wyze-data-leak-key-takeaways-server-mistake-exposed-information-2-4m-customers/
4. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
5. https://cisomag.eccouncil.org/psychology-of-human-error-could-help-businesses-prevent-security-breaches/
6. https://www.securitysales.com/research/tech-skills-gap-cybersecurity/

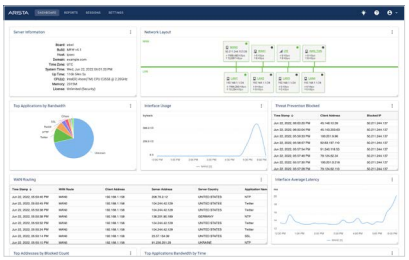
About Arista Edge Threat Management

Arista's Edge Threat Management solutions help small-to-medium businesses and distributed enterprises optimize their networks while safeguarding their data and devices. Edge Threat Management provides cloud-managed security and connectivity options that work together seamlessly to ensure protection, monitoring, and control across the entire digital attack surface from headquarters to the network edge. The award-winning products are trusted by thousands of customers and protect millions of people and their devices. We are committed to bringing open, innovative and interoperable solutions to customers through a rapidly growing ecosystem of technology, managed services, and distribution partners worldwide.



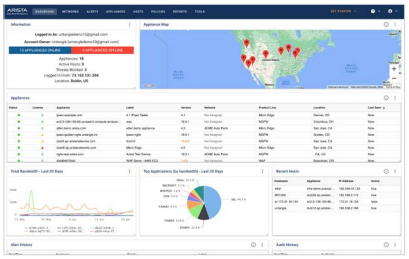
Advanced Security

- Protection, encryption, control & visibility anywhere
- NG Firewall, IPS, VPN & more
- Onboard security for small network appliances & IoT devices
- Full security processing on-premises or in the cloud



Intelligent Edge Optimization

- Secure, WAN-optimized connectivity for every location
- Seamless scalability
- Optimal predictive routing technology for first packet, dynamic path selection
- Centrally manage one or many appliances



Cloud Management at Scale

- Zero touch deployment
- Configure & push policies
- Advanced alerting & reporting
- Visibility across globally dispersed networks & endpoints

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

Phone: +1-866-233-2296
Email: edge.sales@arista.com