Multi-Layered Network Security

for Your Nonprofit

Nonprofit organizations come in all shapes and sizes - from large scale museums and healthcare facilities to smaller, community-based organizations, but they all have one thing in common, Nonprofits are high value targets for cyber criminals. Nonprofit organizations manage and handle large amounts of data every day. This data can range from donor information, staff and volunteer information to the personal information of those who take advantage of their services. And, similar to small-to-medium sized businesses, nonprofits continue to suffer from limited IT budget and staffing, leaving easily detectable vulnerabilities within their network.

Nonprofits can increase their network security policies and protocols by implementing a multi-layered security solution that builds a formidable and, at times, flexible, wall against cyber attack.

Building a Multi-Layered Solution

When network administrators or IT professionals think of a multi-layered security solution, they approach it like putting together a puzzle. Within this puzzle there are pieces that work together, building up to the larger image when everything is in place.

So, what are some steps that nonprofits can take to build their multi-layered solution?

1. **Pair a Next-Generation Firewall with Endpoint Security**

   Next Generation Firewalls (NG Firewalls) prevent malicious Internet traffic and content from entering the network at the gateway, while endpoint security protects authorized devices that routinely connect to the network. These technologies pair well together because policies and protocols can be established within the NG Firewall system and, with endpoint security, the same protections can be set for mobile devices, laptops, printers, or other IoT devices when they connect to the main network.

2. **Use Both Cloud-based Infrastructure and On-premises Data Centers for Data Backups**

   Backing up data should be done in multiple places. If an attack does occur, accessing the cloud-based data can significantly reduce any downtime while systems are being restored. The back up at an off-network location is a safety net to be accessed in large scale situations where internet access is denied.

3. **Combine Captive Portal Login with Active Database Management**

   With so many employee types associated with a nonprofit (staff, volunteer, and vendor organizations), credential security and network access is critical. Ensure each person who accesses the network is logging in through a captive portal will decrease the likelihood of credentials being compromised. Maintaining an active database where data access is defined by employment type will also create a secondary layer of security, giving access to only pertinent information needed at the time.

4. **Password Maintenance with Continued Employee Education**

   We all understand the importance of keeping passwords updated, but adding two-factor authentication (2FA) along with continued employee education will create a proactive working environment against cyber attack. Employees will know how to identify suspicious emails or network activity and passwords will be tied to a secondary authentication method to reduce stolen credential access.

Nonprofit organizations will remain targets for cybercriminals as long as they continue to collect data from donors or clients. What will also remain is their need for several security layers to ward off these attacks. By implementing outlined security measures, increasing network security, and remaining vigilant, organizations can prevent cyber attack with minimal financial investment.

ARISTA

Guide

About Arista Cognitive Unified Edge (CUE)

Arista's CUE solutions help SMBs and distributed enterprises optimize their networks while safeguarding their data and devices. CUE redefines networks with enhanced security and connectivity, flexible PoE switching, and Wi-Fi 6/6E offerings that work together seamlessly to ensure connectivity, protection, monitoring, and control across the entire network from headquarters to the network edge.

Centralized Cloud Based Management

- Visibility across globally dispersed networks & endpoints
- Zero touch deployment for hardware appliances
- Advanced alerting & reporting for CIPA compliance

Next Generation Firewall

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

WAN Optimization

- Secure, WAN-optimized connectivity for every location
- Seamless scalability with centralized policy management
- Optimal predictive routing technology for first packet, dynamic path selection

Wired Connectivity

- Scalable PoE compact switches with 12 to 48 ports
- Based on Arista's Extensible Operating System (EOS)
- Wire rate encryption/tunneling
- Multi-gigabit uplink speeds from 1 to 100 Gbps

Wi-Fi 6 Access Points

- Enterprise class Wi-Fi 6 and Wi-Fi 6E technologies
- Optimized performance to scale from 1 to hundreds of users per AP
- Multi-gigabit uplink choices based upon bandwidth needs
- Open, published APIs for integration with ITSM and monitoring tools

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

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