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.

HOW CAN UNTANGLE HELP?

Customers choose Untangle for next generation web filtering which includes application control, SSL inspection and bandwidth management, along with the ability to block, flag and alert on search terms, enforce safe search, and log YouTube searches, breaking down the glass wall of how students and teachers can safely access educational materials from across the internet.

PROTECT

Untangle's Web Filter helps cybersecurity teams get a handle on rogue applications and malicious content that causes harm when accessed from web pages. Advanced web filtering technology also deploys "safe search" parameters, blocking harmful content on the most common search engines, such as Google, Yahoo, and Bing.

FILTER

Untangle's Web Filter helps cybersecurity teams get a handle on rogue applications and malicious content that causes harm when accessed from web pages. Advanced web filtering technology also deploys "safe search" parameters, blocking harmful content on the most common search engines, such as Google, Yahoo, and Bing. In addition, KidzSearch filtering ensures that all results are filtered through an additional layer for age-appropriate content.

CONNECT

Untangle's OpenVPN and Tunnel VPN solutions help cybersecurity teams keep users and data safe, no matter their location or level of access.

Administrative teams can create private and secure connections for remote students, teachers, and other district employees, and thus maintain visibility and control over remote workers.

MANAGE

Untangle's Policy Manager lets administrators define network privileges based on username, group, device, time, protocol, and more to control who can access websites, data, or apps. In addition, the Reports app provides teams with detailed views of network traffic, and Command Center enables staff to manage network traffic across multiple locations.

BACKUP

Schools and districts can utilize NG Firewall's Configuration Backup tool to ensure uninterrupted protection, availability, and business continuity. Recover easily from unavoidable hardware failures and unforeseen disasters by safeguarding policies and other settings in the cloud, via either Untangle's Command Center or Google Drive.