TREND MICRO

LIVE UNITED

United Way of Greater Atlanta

United Way of Greater Atlanta Upgrades Endpoint Security in Response to Changing Needs of a Mobile Workforce

Website
www.unitedwayatlanta.org

Region
North America, United States, Atlanta, Georgia

Sector
Nonprofit

Employees
220

IT Environment
260+ endpoints, 50-60 virtual desktops, Microsoft Office 365, VMware, Mac

Trend Micro Solutions
- Smart Protection for Endpoints (OfficeScan, Endpoint Encryption, Data Loss Prevention, Control Manager)
- Deep Security

Business Benefits
- Delivers fast and easy deployment and configuration
- Prevents sensitive information from leaking out of the network
- Blocks unwanted traffic: flags bad websites and personal email and stops malware coming from spam
- Simplifies problem resolution with central view of security and granular visibility
- Automates policy setting for greater operational efficiency

Trend Micro Smart Protection for Endpoints Safeguards Donor Information without Increasing IT Workload

OVERVIEW

For more than 100 years, United Way of Greater Atlanta has been serving its community. Today, it works in 13 counties in and around the greater metropolitan area. As one of the largest United Way organizations in the country, it invests $100 million annually in more than 200 programs. The charitable organization focuses on helping children succeed in school, helping families become financially stable, improving health outcomes for people of all ages, and reducing chronic homelessness.

A 10-member IT team supports 200 staff members at eight offices and 20 remote call center agents who take community calls for assistance from their homes. More than 50 seasonal workers join the organization on virtual desktops during the fall pledge drive. Several years ago, United Way of Greater Atlanta virtualized servers and desktops and today runs a completely virtualized environment on the VMware platform.

To honor their mobile workforce, the organization supports a bring-your-own device (BYOD) program with Airwatch management and has replaced about 70% of staff desktops with laptops. IT recently deployed Microsoft Office 365 and now encourages staff to move from other cloud file sharing programs to Microsoft OneDrive.

CHALLENGE

When a big retailer suffers a breach, people don't necessarily stop shopping with that retailer. A breach at United Way of Greater Atlanta, however, could send donors looking for a safer place to put their information and contributions. That's why protecting donor or recipient data is so important for the nonprofit. "We face the same security challenges as many large organizations, such as data leakage, data loss prevention and intrusion detection. For us, there is a higher degree of risk because we are a volunteer-led, donor-driven organization," said Orinzal Williams, Executive Director of IT for United Way of Greater Atlanta.

Not only does United Way of Greater Atlanta compete with other nonprofits, but it competes with organizations that deliver transaction services to nonprofits as a way to expedite contributions. United Way vows to return 90% of its funds back to the community, which requires keeping overhead low. "We have to remain competitive while keeping our donor information secure," said Williams.

"Smart Protection for Endpoints allows us to be more efficient and compliant. When IT is efficient, the organization is being efficient with donor dollars and more money goes to the community. That's a huge benefit."

Orinzal Williams, Executive Director of IT, United Way of Greater Atlanta

CHALLENGE *Continued*

Like many large organizations, United Way of Greater Atlanta needed to revisit its endpoint security solution to address changes in how today's workers do their jobs. An endpoint solution that had served the organization for about seven years was inadequate in an environment of laptops, mobile phones, and security issues around public cloud file storage solutions like Dropbox or Box.

With 268 endpoints to secure and an additional 50 or 60 virtual desktops during the fall fund drive, the small IT team was usually reacting to a problem rather than proactively preventing it. "We needed a more robust endpoint security solution that would help us stay on top of security without devoting a lot of time to it," said Williams.

WHY TREND MICRO

To protect sensitive information on laptops, United Way of Greater Atlanta sought a new endpoint security solution capable of on- and off-premises protection. While Williams did look at solutions from other well-known security vendors, Trend Micro was always top of mind. "I'm a huge fan of Trend Micro Deep Security," said Williams, who uses the solution to protect the organization's VMware environment. "I called the Trend Micro rep to ask if they had anything to help us out. We had a 15-minute conversation about Smart Protection for Endpoints, and I was sold," he added.

"The members of my team wear multiple hats. We can't have something that is so complicated it requires a dedicated resource to manage it. We needed the best combination of robustness and ease of use, where we can set it up but not babysit it all day. For this reason, Trend Micro was the best solution for us," said Williams. "We started using Smart Protection for Endpoints immediately without additional training, because the dashboard is just like Deep Security," he added.

"We used to put everything else on hold to combat the spread of malware on files on the server. With Smart Protection for Endpoints, we get an alert that the firewall has quarantined a machine on its own. Now we have one machine to check and nothing else that has to be done – no issue on the server or on other machines."

Orinzal Williams, Executive Director of IT, United Way of Greater Atlanta

SOLUTION

With help from a simple setup program, it took Williams about 45 minutes to deploy Smart Protection for Endpoints and install it on ten IT machines before launching a staged deployment to the rest of the organization. The suite offers protection against traditional attacks and the latest targeted attacks. "Smart Protection for Endpoints works with our Mac hardware, has BYOD functionality, and is lightweight and easy to deploy to our remote workforce," said Williams.

To ensure protection now and in the future, IT decided to purchase a full suite of complementary endpoint solutions that deliver multiple layers of interconnected threat and data protection. "We may not use everything, but it's there if we need it or auditors request it," said Williams. The Security for Mac module adds a layer of protection for a growing number of Apple Mac clients in the network. The organization also uses the solution's firewall, built-in compliance rules, endpoint encryption, and data loss prevention (DLP) module. They are currently testing virtual patching.

The DLP module ensures compliance with IT policy by blocking any attempts to send out sensitive information or inadvertently store it on the local hard drive. "When I know certain people are working with sensitive information, I can target their machines for DLP. Once we install the agent on the desktop, I can activate it from the console, and DLP is automatically put in place," Williams added. "With DLP and other plug-ins, we are confident we are not leaking information out."

Setting policies is an important part of controlling user behavior, such as ensuring users can't execute dangerous applications on endpoints. "We manage our remote agents by setting up a profile for on-network use and strengthening it for off-network," said Williams.

The IT team makes extensive use of Trend Micro Control Manager, which provides a central view and reporting across connected Trend Micro security. "I really love the visibility into the machines and the control we have. We can do a little or a whole lot with it – we can have a basic level of protection or go deep and block certain applications at the firewall process. This really fits how we work," said Williams, who jumps to many different tasks in the course of a day.

Alerts and reports help Williams and his team respond quickly to issues in the environment. Williams can target machines that don't have the current version of security software, so the IT team can find out why they didn't update. He can also follow an alert on a quarantined machine with a scan, if necessary.

"Smart Protection for Endpoints was the best solution for us. It's easy to set up and operate, easy to deploy and maintain, and it keeps us safe and secure."

Orinzal Williams, Executive Director of IT, United Way of Atlanta

"Smart Protection for Endpoints helps us stay on top of security without having to commit a lot of time to it."

Orinzal Williams, Executive Director of IT, United Way of Atlanta

"Trend Micro makes my job easier while I am delivering the best service back to the organization, back to our donors, our volunteers, and in a larger sense, back to the community."

Orinzal Williams, Executive Director of IT, United Way of Atlanta

RESULT

Multitasking got easier for the IT team following implementation of Smart Protection for Endpoints. Before deploying the security suite, IT faced from eight to 20 security issues a week, any one of which could spread malware or a Trojan like CryptoLocker to files on the server. It took all hands on deck to run solutions to combat a serious security issue. With Smart Protection for Endpoints, IT receives an alert that the firewall has automatically quarantined a machine. "Now we have one isolated issue to check and nothing else that has to be done – no issue on the server or on other machines. The threat probably didn't even take hold on the original machine," said Williams.

"Smart Protection for Endpoints does a great job of blocking unwanted traffic. It flags bad websites and stops malware entering from spam emails. It also flags personal email, which covers a huge hole and is a big win for us," said Williams. He estimates that 50 threats – mostly malware from web traffic – have been blocked by Smart Protection for Endpoints since its implementation four months ago. The software is so efficient that the server never gets above 10% utilization. "The system remains efficient even when we have scheduled scans," said Williams.

Smart Protection for Endpoints alerts, reports, and preprogrammed compliance features ensure a small IT team can operate efficiently to protect donor information at United Way of Greater Atlanta. "I don't want to see us spending a lot of money on internal operations. I want the money to help the community. Since deploying Smart Protection for Endpoints, we know we are delivering the best service without increasing our workload," said Williams. "I can say with confidence to our board that the combination of Deep Security and Smart Protection for Endpoints ensures we are taking all the necessary steps to make our environment secure," he added.

Williams has not had to call in a support ticket for Smart Protection for Endpoints. However, he's confident that if an issue developed he would receive exemplary service. In all the time he's used Deep Security, he's only called in five tickets, and only one of those required an escalation. He received a call back on the escalation within the hour. "Trend Micro worked with us on the problem after hours until we got it resolved," said Williams. "The fact that I've only had five tickets is a testament to the quality of Trend Micro software," he added.

WHAT'S NEXT?

"We are still trying to figure out what actions we need to take for the cloud," said Williams. The organization migrated to Office 365 almost a year ago, so most file sharing now takes place through OneDrive. Currently, they rely on the Smart Protection for Endpoints DLP module and built-in Microsoft protection on Office 365 to protect data in cloud applications. As Williams investigates a more layered defense for cloud apps, he will certainly look into Trend Micro solutions and consider their applicability for United Way of Greater Atlanta.

FOR MORE INFORMATION

For more information, please visit **www.trendmicro.com/switch**

TREND MICRO™

Securing Your Journey to the Cloud