MEDHOST Takes a Security-First Approach to Healthcare Services and Solutions

Website
www.medhost.com

Region
North America, United States

Sector
Healthcare, Information Technology

Employees
400

Trend Micro Solutions
- Deep Security
- Smart Protection Suite: OfficeScan, Control Manager, Integrated Data Loss Prevention (iDLP), Web Security Gateway

IT Environment
Amazon Web Services (AWS), Microsoft Azure, VMware, hybrid cloud architecture, multi-cloud, Citrix, Linux, various Windows operating systems

Business Benefits
- Potential threats blocked with web reputation across several hundred users on network
- Secures applications upon development for faster time to market
- Patches vulnerabilities immediately and efficiently
- Reduces overhead with agentless security solution
- Increases productivity with centralized management of workloads in the data center and in the cloud
- Ensures continuous protection with minimum disruption

Trend Micro Simplifies Security Management and Provides Greater Visibility Into Threats

OVERVIEW

For more than 30 years, MEDHOST has been a leader in healthcare technology and solutions, meeting existing and emerging needs of its customers in advance of market demand. Today, nearly 1,100 North American acute care and specialty hospitals utilize MEDHOST's solutions and services to improve clinical delivery and financial and operational performance. "Every day we come to work, we know we're helping Americans receive care and helping hospitals efficiently and safely manage their facilities," said Todd Forgie, Vice President of IT and Managed Services at MEDHOST.

A staff of 60 IT professionals takes on the management of client environments in a hosted environment and internal core services, including all the security tools for about 1,500 endpoints and 700 pure-play mobile devices. Security is at the core of all MEDHOST activities, from product development and customer support to management of day-to-day operations and hosting a hospital information system. "Security has to be front and center for us, because it is a big part of ensuring our customers' success," said Forgie.

MEDHOST has the same compliance and risk issues as any other major enterprise, in addition to a federal mandate to protect patient privacy. "However, the most important security issue for us is our responsibility to prevent the breach of private health information of the people in our communities," said Forgie.

CHALLENGES

In the wrong hands, health records open opportunities for medical fraud and identity theft, which makes them highly lucrative targets. "With the monetization of health records on the dark web, we're seeing organized crime, nation states, and activists going after healthcare organizations like ours," said Forgie. "We're not just a single hospital trying to protect its health information. We keep hundreds of hospitals' protected health information in the cloud. That creates specific security needs that other security shops don't have to contend with," he added.

As healthcare becomes a bigger target, it's essential for MEDHOST to ensure that weekend surfing from home on a work laptop can't infect the network on a Monday morning. It's also important for IT to know where employees are saving sensitive information, so they can set appropriate policies to ensure its safety.

MEDHOST delivers data from its private cloud as well as from hybrid and public cloud settings. "We see cloud delivery as a necessity in today's marketplace. As hospitals consolidate, they are

"Almost all information security shops are outgunned every single day. We need a partner like Trend Micro to give us the firepower to fight back."

Todd Forgie,
Vice President of IT and Managed Services, MEDHOST

"In the first three to four months of use, OfficeScan web reputation blocked potential threats across several hundred users on our network. It significantly reduced resource consumption on the desktop support space."

William Crank,
Chief Information Security Officer, MEDHOST

"With Trend Micro Deep Security, I can look at my public cloud instances as well as what we are managing in our data center under a single pane of glass. That level of visibility is the best circumstance you can have."

William Crank,
Chief Information Security Officer, MEDHOST

looking to achieve the economies of scale that cloud delivery can provide," said Forgie. "It's our job to wrap the right security process, governance, and capabilities around cloud delivery to allow innovation in this space," he added. To find the best security for its infrastructure, MEDHOST decided to look for one security provider to meet all of its needs.

WHY TREND MICRO

Not long ago, MEDHOST provided security through several vendors, including Trend Micro. This arrangement proved inadequate from a cost containment and management standpoint, and eventually led MEDHOST to select a single vendor. "Trend Micro picked up outbreaks that other solutions could possibly miss. We liked how its single console helped us manage threats with limited resources," said William Crank, Chief Information Security Officer (CISO) at MEDHOST. "We decided to go pure-play with Trend Micro and we have not looked back," he added.

SOLUTION

MEDHOST uses the Trend Micro's Smart Protection Suite to protect endpoints. "Antivirus and anti-malware take care of commodity-based threats that come into the network through email and web surfing, while behavioral monitoring and web security provide more advanced protections and allow us to extend security beyond the borders of our network," said Crank.

The Integrated Data Loss Prevention (DLP) module gives MEDHOST visibility into where network users are saving and storing information. "It pulls back the covers and allows us to manage our clients' information and our information much better," he added. We use the solution to put risk-based policy in place to make sure users are not storing sensitive data in cloud-based applications like Dropbox and Box."

In addition to the Smart Protection Suite, Trend Micro Deep Security gives MEDHOST the capabilities it needs to operate a virtualized data center and to safely move workloads to the cloud. MEDHOST partners with VMware for its virtualization needs, and with Microsoft Azure and AWS for its public cloud needs. "Deep Security basically shims into the hypervisor and reduces the CPU cycles and memory usage on the guest VMs (virtual machines)," said Crank. It also takes data center security controls to the cloud with log management, integrity monitoring, antivirus and anti-malware protection and virtual patching, and by providing a firewall and intrusion protection at the guest OS level. "Deep Security is at the forefront when it comes to providing the majority of controls we need for compliance and risk mitigation in the cloud," he added.

"With Trend Micro Deep Security, I can look at my cloud instances as well as what we are managing in our data center from a single pane of glass. That level of visibility is the best circumstance you can have for a hybrid deployment like ours," said Crank. Equally important is the level of automation Deep Security brings to orchestration. "As we spin up new VMs, we can provision them and know they are protected by Deep Security, with minimal interaction on our part," he added.

RESULTS

In today's landscape, MEDHOST has to react to threats faster than ever before. "Trend Micro's virtual patching capability in Deep Security lets us react quickly to a zero-day outbreak instead of working on a patching scheme that may take a week or a month to get in place," said Forgie.

"Trend Micro builds recommendation scanning into virtual patching, so we can turn off rules for vulnerabilities that do not apply to a particular VM and reduce performance overhead on that VM. Using this toolset to run our environment more efficiently allows us to be secured at the level where our risk appetite is," said Crank.

The engineering team is experiencing new levels of productivity thanks to Deep Security automation and simplified management. "We don't have to look at a screen all day waiting for things to happen, because we know Trend Micro tools are monitoring the house," said Crank. "In the first three to four months of use, OfficeScan web reputation blocked potential threats across several hundred users on our network. It significantly reduced resource consumption on the desktop support space," he added.

"Almost every shop in the healthcare field is increasing its investment in security, and we're no different. With Trend Micro, we leveraged our investments in security technologies and partners to get the most bang for our buck–a strong strategic partner, a return on our investment, and a culture of responsiveness like ours," said Forgie. "We invested early in private cloud, self-provisioning, automation, and orchestration. Being able to do this without the overhead or maintenance associated with a security agent has been a huge benefit to us," he added.

"In the last few years, we've really moved the needle on security. Trend Micro increases our competence and lets our customers see us as a trusted partner," said Crank.

WHAT'S NEXT?

"We have a hard exterior defensive posture and good firewalls and network maps in place. We have next-generation intrusion detection and are doing a good job of securing endpoints and servers. Our next challenge is to put additional behavior-based tools in place that allow us to know when systems or users aren't behaving as expected," said Forgie.

MORE INFORMATION

For more information, please go to **www.trendmicro.com**

TREND MICRO™

Securing Your Journey to the Cloud