CYLANCE™

CASE STUDY HEALTHCARE

Hospital Takes on Cybersecurity

INDUSTRY
Healthcare

ENVIRONMENT
- Top 25 healthcare system
- Over 9,000 employees
- Virtual desktop infrastructure deployment
- 12,500 nodes protected

CHALLENGES
- Meeting regulatory compliance requirements
- Protecting patient information
- Relieving virtual desktop infrastructure resources overtaxed by legacy antivirus
- Alleviating the negative impact of antivirus on employee productivity
- Lowering the high number of antivirus-related help desk calls
- Eliminating the high number of false positive incidents
- Decreasing costly computer re-imaging due to malware

SOLUTION
Deploy CylancePROTECT® Enterprise-wide to contain potentially unwanted programs, reduce the total cost of antivirus protection, and stop threats BEFORE they cause costly harm to critical systems

The Company

A Top 25 healthcare system that is also one of the largest healthcare systems in Oklahoma.

The Situation

Tasked with providing improved service availability and cost reductions for the company, the IT leadership decided to implement virtual desktop infrastructure (VDI). During their initial rollout of 8,000 virtual machines, it was quickly realized that the company's legacy antivirus solution, which was provided by a Tier One AV, was a drain on system resources and wouldn't support the performance objectives of the VDI deployment. The IT and security teams needed endpoint protection for compliance purposes and wanted a lightweight, next-generation solution that would be free of antivirus system resource drain. The team also wanted a solution that would be transparent to employees while still mitigating the threats posed by ransomware, zero-day attacks, and other exploits.

The Process

After conducting extensive research, the information security team narrowed their endpoint protection options to Cylance® and SentinelOne. Both potential solutions were brought into the healthcare system's lab for a thorough evaluation.

Cylance and SentinelOne provided very lightweight agents that were easy to deploy. However, during the initial deployment of SentinelOne, the agent

"CylancePROTECT has really helped us clean up our infrastructure and made our VDI deployment a success! It has saved a huge amount of time and money. Also, people don't even realize it's there, which makes my life so much better." **— Senior Information Security Engineer**

9,000
EMPLOYEES

12,500
ENDPOINTS
PROTECTED

needed to be updated with the latest signatures. SentinelOne's agent used virus repository lookups, ReversingLabs, government sources, and other trusted AV signatures to feed its matrix of algorithms that make up its behavioral analysis engine residing in the cloud. The SentinelOne agent on the endpoint performed a check-in once every minute to capture any new behavioral signatures.

"We were very concerned that if their signatures didn't stop something and it executed, then it would be too late for effective remediation," said the company's Senior Information Security Engineer. "Every year signature-based AVs are getting less and less effective, and at the end of the day, SentinelOne uses signatures. In addition, we were concerned that if an endpoint was offline for a period of time, then the level of protection from SentinelOne would diminish because of its inability to check-in and update."

Unlike SentinelOne, Cylance didn't rely on signatures from third parties in order to deliver endpoint protection. Cylance utilized a far more reliable and effective methodology, based on artificial intelligence, which analyzed hundreds of thousands of file attributes to identify and eliminate malicious code before it executed. Cylance demonstrated a very high level of endpoint protection, for all endpoints (online and offline), and eliminated some highly complex threat vectors, including a sophisticated PowerShell script attack.

"Not only did CylancePROTECT deliver outstanding endpoint protection, but the Cylance Consulting team provided tremendous support throughout the process of selecting and deploying their advanced endpoint protection solution," said the Senior Information Security Engineer.

The Results

After deploying CylancePROTECT, the information security team realized substantial benefits, including:

- The immediate quarantine of nearly 1,000 items, including adware and PUPS, that were missed by their Tier One AV product
- A dramatic reduction in antivirus-related help desk calls, which cost $22 per call
- The elimination of machines being offline for re-imaging, which cost $400 per machine
- A significant reduction in network traffic from the elimination of adware
- The complete elimination of ransomware executions
- The elimination of the need to maintain repositories at other hospitals for DAT file updates
- The extension of laptop service life and increased battery life of one to two hours
- The elimination of 64 pages of exceptions requiring security team intervention

The information security team was able to dramatically reduce the total cost of ownership of endpoint protection by eliminating the burden of legacy antivirus on end-users' machines, resulting in a dramatic reduction in help desk calls, eliminating the need for re-imaging due to malware, a significant reduction in network traffic, and the elimination of exceptions that needed to be worked by the information security team.

By deploying CylancePROTECT, the information security team achieved its goal of attaining true endpoint protection that is transparent to the user while enabling a successful transition to VDI.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

CYLANCE™

20170302-0420