IT Risk Management

SEP STREAMLINES SECURITY

Client Profile

A leader in local news and information in 10 states.

Challenges

As a large entity with multiple locations throughout the United States, the client faced numerous challenges when solidifying its security posture. First, its internal Antivirus environment was operating on three separate consoles—each with an individual database, IT team and location. Additionally, many employees operate remotely and with no process for unified updates, several versions of antivirus software were in play. The often-outdated virus protection exposed the company to elevated risk and vulnerability.

To make matters worse, the client had no disaster recovery program in place, so if a security threat did arise, all active data and projects could be lost. These logistical constraints caused numerous disruptions to the overall management of the environment and forced company leaders to take a closer look at the security of their network.

Solution

After performing an exhaustive security audit, CBI recommended implementing Symantec Endpoint Protection (SEP) 12.1 to protect the client's network against malware threats. After consolidating the three consoles and their databases into one high performance agent for optimal management, the software seamlessly integrated essential security tools. Insight, which powers the product, reduced file scanning time by 70 percent by identifying files that had never been infected and removing them from the scanning process unless an alteration is sensed.

Group Update Providers (GUP) were also strategically implemented to run automatic checks of the antivirus protection being used across the network. Through the use of GUPs, all machines—including those operating remotely—will be updated during their programmed heartbeat intervals, ensuring optimal security.

Additionally, SEP 12.1 is equipped with SONAR; a high-level protection software that identifies new security threats before they are able to compromise the network. CBI was also able to set up a function inside the software that automatically sends reports to the department managing the environment, warning them of impending threats to the network. To ensure that the client was prepared for a security breach, CBI created a disaster recovery program, mirroring all work that was created within the production environment inside a separate disaster recovery environment for easy restoration.

Results

The results of the console consolidation and software migration had an immediate and measurable impact. As a result of SEP 12.1 deployment, the company was able to cut down on virus infiltration, alleviating threats that were discovered during the initial audit.

Due to the faster scan time, which typically slows down the functionality of a machine, overall productivity and efficiency drastically increased. The new disaster recovery measures ensure that, should any problems arise in the newly secured environment, all work would be preserved in a safe network from which it can be restored.

Additionally, the monitoring and reporting function integrated by CBI provided the client's IT team with valuable insight and faster reaction time in the event of a security breach.

OVERVIEW

Industry
Media

Solution
Endpoint Protection

CBI Generated Results

- Mitigation of virus infiltration
- Improved productivity and efficiency
- Enhanced monitoring for faster incident resolution