

Web Reputation Checks Keep Employees from Risky Sites

The Trend Micro™ Smart Protection Network™ infrastructure stops threats in the cloud to enhance on-site performance.

“Today, when I look at the numbers, it is astounding. Smart Protection Network is stopping attempted accesses to hundreds of bad sites per day. One month, the number of blocked accesses reached 50,000.”

— Kurt Nikolas, Security Analyst Consultant for Ceridian

EXECUTIVE SUMMARY

Customer Name: Ceridian Corporation

Industry: Business Services

Location: Minneapolis, Minnesota

Web Site: www.ceridian.com

Number of Employees: Almost 10,000 globally

CHALLENGE:

- Allow employees to make use of the web without introducing risks to the business
- Minimize windows of vulnerability for zero-day threats
- Optimize the distribution of new signatures to keep endpoint security as up to date as possible
- Reduce the complexity of endpoint security, to enable administration by a small team of security professionals.

SOLUTION:

- Deploy Trend Micro™ Enterprise Security for Endpoints, with automatic update distributions
- Enable Trend Micro Smart Protection Network features

BUSINESS RESULTS:

- Real-time protection, with threats blocked in the cloud
- 30–40% decrease in infection rates with introduction of web reputation checks
- 33–50% faster distribution of new signatures
- Blocking up to 50,000 attempted accesses of risky sites per month, with very few false positives

Challenge

In 1992, Ceridian Corporation emerged from a successful restructuring of its predecessor, Control Data Corporation. However, the company's history goes back to 1932 when IBM established an organization to focus on delivering business services. Today, more than 20 million employees working for more than 100,000 companies around the world rely on Ceridian to help them improve their productivity, save money, and minimize financial risks.

As a global company, Ceridian faces many of the same business challenges as its customers, including the cost-effective management of effective security solutions. The company relies on its expert IT resources to select and deploy security solutions that can block threats without introducing complexity to the business.

The challenge has always been to maximize protection of its digital assets while allowing employees responsible access to the Internet. “I am the main administrator taking care of a 10,000 node network of endpoints,” explained Kurt Nikolas, a security analyst for Ceridian. “It is almost unbelievable, but there are still many people that click on links in phishing emails or try to access malware-propagating web sites. Our security solution has to be constantly prepared to prevent infections that can come about from these actions.”

Solution

For almost a decade, Ceridian has relied on Trend Micro Enterprise Security to protect its infrastructure. When increasing malicious activity on the Internet raised concerns about threats and vulnerabilities, a Trend Micro innovation gave them an easy solution.

Trend Micro Enterprise Security products and services are powered by the Trend Micro Smart Protection Network infrastructure that delivers advanced protection from the cloud. Threats are blocked in real-time, before they reach the Ceridian network and computers.

“As soon as the web reputation features of Smart Protection Network were enabled on Ceridian endpoints, there was a 30 to 40% drop in infection rate,” said Nikolas. “Today, when I look at the numbers, it is astounding. Smart Protection Network is stopping attempted accesses to hundreds of bad sites per day. One month, the number of blocked access attempts reached 50,000. Keeping employees off of risky sites really gives us peace of mind.”

Recent enhancements to Smart Protection Network have also been introduced at Ceridian. “We usually only hear from users when they have complaints, but when we upgraded to the latest Trend Micro release, with web reputation caching, employees noticed how web pages now come up faster,” said Nikolas. “

The configuration of internal Smart Protection Servers has also improved performance for downloading updated pattern files. Nikolas said, “Smart Protection Servers improve the efficiency of automatic updates, and we can now leave on logging features even during update downloads, without overloading servers or impacting employee productivity.

“As a result, we have increased the frequency of our updates from hourly to every 15 minutes for increased protection. And updates now get distributed to all of our endpoints 33–50% faster. Smart Protection Servers have been a tremendous time saver for getting updates out to all of the endpoints.”

Results

Decreased infection rates and improved management efficiencies have both benefitted Ceridian’s global operations. Smart Protection Network is also helping Ceridian move from on-premise, traditional security to a private cloud approach. Ceridian has set up local Smart Protection Servers to host web reputation information in a private cloud.

The private cloud improves performance and privacy; fewer queries go out over the WAN. The public cloud is still available to protect mobile users that are off network.

“Web reputation, and now locally hosted web reputation, have given us a two-fold improvement in both protection and service levels,” said Nikolas. “The virtual users on our slower VPN connections experience less latency than do users on the company networks, and everyone is protected from thousands of risky URLs each month. This Smart Protection Network defense has proven to preempt infections and exposures from malicious web sites, making it a foundational component in our endpoint security.”

With continual gathering of threat intelligence, Smart Protection Network speeds time to protection.

“In September of this year, there was a zero-day virus that hit many businesses around the world,” said Nikolas. “I know IT teams at other companies using different security solutions. With Trend Micro security and Smart Protection Network, I was the first one to have a fix in place.

“We were remediating the threat within six hours. It was completely managed that day, with new signatures downloaded to all of our computers. This was many hours faster than other security competitors.”

The in-the-cloud protection gives Ceridian’s IT administrators a set-it-and-forget-it approach to security. “I don’t have to figure out the source of threats or worry about keeping security up to date—with Smart Protection Network, it is all taken care of dynamically and on the fly.

“It is astounding how many things Smart Protection Network blocks before reaching us, with very few false positives. Out of 50,000 blocked sites, for example, I whitelisted only three. That is a pretty good rate!”

“Smart Protection Servers improve the efficiency of automatic updates... As a result, we have increased the frequency of our updates from hourly to every 15 minutes for increased protection. And updates now get distributed to all of our endpoints 33–50% faster.”

— Kurt Nikolas, Security Analyst Consultant for Ceridian

DEPLOYMENT ENVIRONMENT

PCs: 6,000+

Servers: 1000+

Locations: Dozens of offices in the U.S., plus many sites in Canada, U.K., and Europe

Trend Micro Enterprise Security for Endpoints

Company Profile

Ceridian is a leading global business services company that provides solutions that take the guesswork out of impacting an organization’s bottom line. From human resources and benefits to productivity and payroll services, Ceridian helps organizations maximize their human, financial, and technology resources. As a leader in payroll outsourcing, gift cards and corporate spending, the company is the driving force in payment innovation. Whether partnering with customers to save money, grow their business, enhance operations, or minimize financial risks, Ceridian provides the insights and solutions that ensure success.

Trend Micro Security

- **Trend Micro Enterprise Security for Endpoints**

<http://us.trendmicro.com/us/products/enterprise/security-for-endpoints/index.html>

Trend Micro Enabling Technology

- **Trend Micro Smart Protection Network**

<http://us.trendmicro.com/us/trendwatch/core-technologies/smart-protection-network/>



© 2011 Trend Micro Incorporated. All rights reserved. All Trend Micro company, product and service names and slogans are trademarks or registered trademarks of Trend Micro Incorporated. Other names and marks are the property of their respective owners.
CS_Ceridian_ESE_SPN_March2011
www.trendmicro.com