REPUBLIC NATIONAL DISTRIBUTING COMPANY

National Distribution Company Bolsters IT Security with Trend Micro Threat Detection

RNDC Uses Trend Micro™ Deep Discovery to Proactively Detect, Analyze, Adapt and respond to targeted attacks and advanced threats

Republic National Distributing Company

Industry

Beverage Distribution

Region

Atlanta, US

Trend Solutions

- Trend Micro Deep Discovery
- Trend Micro™ Threat Mitigator

IT Environment

Centralized data center, with backup facility in another state

6,000 PCs and servers

95% virtualized in the data center (VMware)

Multilayered, multivendor security solutions

> "We immediately detected command and control servers had established connections through our new firewall. With Deep Discovery, we were able to identify the potential threats and then take steps to prevent it."
>
> John Dickson,
> Director, IT Infrastructure,
> Republic National Distributing Company,
> Atlanta, Georgia

Overview

Republic National Distributing Company (RNDC) is the second largest alcohol beverage distributor of premium wines and spirits in the U.S. with wholly-owned operations in 21 states. RNDC also operates in Arizona, Indiana, Kentucky, Ohio, Oklahoma, and South Carolina through venture partnerships. In total, RNDC employs more than 8,000 workers nationwide and is built on the strong foundations of long-term, well-established family owned companies. The earliest RNDC predecessor company traces back to a single distributorship that was founded back in 1898 in Pensacola, Florida.

Challenges

As a leading alcohol beverage distributor committed to keeping their operations flowing smoothly, RNDC focuses on deploying innovative IT solutions. In early 2013, RNDC decided to bolster its IT security and prevent advanced malicious attacks by deploying an application-based, next generation firewall to replace its traditional firewall. While implementing the next gen firewall with its added security, the vendor configured the solution based on its own best practices rather than RNDC's own best practices and business requirements.

Within hours of deploying the next generation solution, RNDC end-users were notified of malicious activity. While the new antivirus solution identified an attacker, it failed to identify the specific malware and wasn't able to eliminate it. When RNDC notified the firewall vendor of the malicious activity that had passed through the next generation firewall, the vendor's response was disappointing. They responded by saying that although the malware made it through the firewall, it was not sending information outside the network, so no damage was done.

This response did not satisfy the RNDC IT team, who had previously experienced severe issues with the Conficker virus in 2009 that resulted in a shut down of major operations for three weeks. Given this, RNDC wanted to know what the current threat was, and how to stop it cold. "This malicious activity was a major concern for us because we learned the hard way that the instant you allow malware to get into your network, the next exploit may result in a full-fledged attack," said John Dickson, Director of IT Infrastructure. "The Conficker virus in 2009 shut down our systems and drained us for over 5,000 hours of effort."

Solution

RNDC turned to Trend Micro, who had established a trusted relationship by mitigating the Conficker virus that had plagued RNDC's system in 2009. As a result of this relationship, Trend Micro Deep Discovery provided RNDC with a solution they could simply plug in to their network to instantly identify the malware and malicious activity their next generation firewall vendor had ignored. "Prior to Deep Discovery, the Conficker outbreak required a team of 30 engineers and helpdesk personnel to trace the issue at a cost of $500,000," said Dickson. "Every day, Deep Discovery alerts and stops 6-10 attacks–and delivered a return on investment within 1 year."

Trend Micro Deep Discovery instantly detected a botnet that had permeated the next-generation firewall. "We immediately saw that known command and control servers had been allowed to establish connections through our new firewall," said Dickson. "With Deep Discovery, we were able to identify the potential threat and then take steps to prevent it."

Once the botnet was identified, Trend Micro Deep Discovery collected a variety of information about the malicious botnet's activity. RNDC used that information to create a custom "block list" that prevented unwanted traffic from getting into their network. Deep Discovery uses the Trend Micro™ Smart Protection Network™ infrastructure to identify sources of traffic related to malicious activity.

With Deep Discovery's proactive threat detection, RNDC is now instantly alerted when malicious activity is detected anywhere on its network. "With Trend Micro's shared intelligence and malicious activity database, we don't have to wait for command and control servers to act to know if it is a viral attack," said Dickson.

> "Trend Micro Deep Discovery shines a light in the darkest corners of our network by looking for anomalous behavior instead of just viral definitions. It allows me to rest easy, knowing that Deep Discovery can handle the next attack."
>
> John Dickson,
> Director, IT Infrastructure,
> Republic National Distributing Company,
> Atlanta, Georgia

Benefits

Trend Micro Deep Discovery provides the granular visibility required to instantly alert RNDC's IT team of targeted attacks or other suspicious network activity, "When our firewall vendor was unable to identify malicious activity on our network, we called Trend Micro," stated Dickson. "Using Deep Discovery, Trend Micro's specialists found a known command-and-control issue in less than 2 hours."

Today, Deep Discovery monitors the activity on the RNDC network to prevent malicious activities before they can affect the company's business performance. "Trend Micro is a trusted partner with a very responsive team that adds value to their security solutions. We plan to turn to Trend Micro for additional IT protection in the future."

After deploying Deep Discovery, RNDC spends less IT time preventing and remediating threats, and more time boosting IT efficiency. "Trend Micro Deep Discovery shines a light in the darkest corners of our network by looking for anomalous behavior instead of just viral definitions," said Dickson. "It allows me to rest easy, knowing that Deep Discovery can handle the next attack, no matter where it comes from."

Deployment Environment

Centralized data center, with backup facility in another state

6,000 PCs and servers

95% virtualized in the data center (VMware)

Multilayered, multivendor security solutions