Leading Human Capital Management Firm Enhances Security with Threat Intelligence

ADP integrates advanced malware analysis and global threat intelligence with its security platform to better serve clients.

EXECUTIVE SUMMARY

ADP

- Human Capital Management
- Roseland, New Jersey
- 52,000 Employees

CHALLENGE

- Reduce increasing number of malware attacks.
- Automate malware defense process.
- Integrate malware analysis with security platform.

SOLUTION

- Malware analysis technology, services, and intelligence in a single solution
- Global threat intelligence on all industries served by the company
- Expert knowledge of support team for greater security protection

BUSINESS RESULTS

- Integration of malware analysis and threat intelligence in a single monitoring platform
- Twenty times more malware analysis and introspection daily
- Faster, more accurate faster decision making for preventative action

Challenge

As a comprehensive global provider of cloud-based human capital management solutions, ADP provides HR, payroll, talent, tax, and benefits administration solutions to more than 625,000 companies in more than 100 countries. ADP is not only a Fortune 500 company itself, but it also provides services to 80 percent of the other Fortune 500 companies and more than 90 of the Fortune 100 organizations. In 2014, the company paid more than 36 million people around the world and moved $1.5 trillion in client tax, direct deposit, and related funds within the United States alone.

Needless to say, security and privacy are paramount to ADP, and they are the cornerstone of maintaining client trust and reducing risk. Roland Cloutier, ADP's chief security officer, says that security, risk, and privacy are synonymous with what the company calls business operations protection. "It's simply part of how we design our business," says Cloutier. "We use the latest industry-recognized tools, tactics, techniques, and procedures to identify any risks and vulnerabilities that could affect our business processes." Cloutier adds, "If I cannot ensure the continuity of the services that we deliver our clients, it would be devastating to those businesses and the economies they serve."

The current cybersecurity landscape in ADP's business is broad and complex. "In each business sector, there are different threats and threat vectors," notes Cloutier. "We see attacks against different platforms trying to access protected information, including the identity information of our consumers."

"Our focus is to understand who accesses our platforms and why. We want to root out fraudulent types of access or cyberattacks and ensure the sustainability and the uptimes of those platforms," says Cloutier. " That's why we looked at Cisco® AMP Threat Grid."

> “It’s this integrated defense system that helps us defend ADP around the clock.”
> **— Roland Cloutier, Chief Security Officer, ADP**

Solution

ADP’s security platform includes a combination of more than a dozen technologies that collectively help the company create an operating model that its security team can use to review the defensive posture of its environment. This helps ADP quickly identify malicious traffic, understand the overall threat, and then prevent it from executing within the company. “We had a great system in place, but we were experiencing more attacks and had less time to address them. We started reviewing components of our ecosystem that could be automated, and Threat Grid quickly came into view, because of our increased focus on our malware defense processes,” says Cloutier.

After a thorough evaluation process, ADP made the decision to move forward with AMP Threat Grid based on several key criteria. “The first reason we chose Threat Grid was because of its effectiveness,” says Cloutier. “The technology, services, and intelligence capabilities that Threat Grid delivers in a single package were beyond anything that we had before.” Other deciding factors included the deep technical intelligence available in the solution and expertise from the AMP Threat Grid team. “It didn't matter what we threw at the team during the evaluation process,” says Cloutier. “It didn’t matter what industry a threat was coming from or what threat process was involved. The Threat Grid team had a depth of knowledge that helped us continually improve our overall protective operation.”

Today, ADP uses AMP Threat Grid in two ways. First, the company automatically extracts specific parts of its network traffic and evaluates whether or not the traffic is threatening. Secondly, the company integrated the solution’s broad deep-intelligence platform with its analytical system in its security intelligence platform using the AMP Threat Grid API. “We have an intelligence-led approach to security,” says Cloutier. “Therefore, threat intelligence is part of our decision support infrastructure, and it's a core component in how we make our decisions every day. This intelligence helps us create faster alerts and make quicker decisions.”

Using AMP Threat Grid context-rich threat intelligence, ADP can now understand what might attack the company in the future—and why. It also helps the company understand what it needs to do to create the best defense in the most cost effective manner.

Cloutier adds, “In a single product set, Threat Grid helped us automate our malware defense program and extend our intelligence program. Threat Grid is now implemented as a core component of our trusted security platform. It is our automated malware defense and prevention mechanism that looks at key network traffic elements and decides whether or not they're malicious.”

Results

Cisco has been a long-term, trusted partner and an integral part of the ADP total security ecosystem from a security, risk management, and privacy perspective. Now AMP Threat Grid is part of this as well.

“Threat Grid has taken what was a manual process and allowed us to use a cloud-based service with better decision-making capabilities,” says Cloutier. “This means we can do 10 or 20 times more malware inspection on a daily basis than we could before with people doing it. This automated defense solution has greatly increased our ability to do things like reverse malware engineering and deciphering of malicious code.”

PRODUCT LIST

- Cisco AMP Threat Grid
- Cisco Advanced Malware Protection (AMP) for Networks
- Cisco Next-Generation Intrusion Prevention System (NGIPS)
- Cisco Cyber Threat Defense
- Cisco AnyConnect® Secure Mobility Solution
- Cisco Incident Response Services

Cloutier notes the company's vast infrastructure, which includes security technologies, IT technologies, transactions within its cloud business platforms, and security intelligence providers, sees nearly eight billion events daily. "Whether it's our intrusion detection platforms, deep packet inspection technologies, or even unstructured data protection environments, all of those are now integrated together into a single monitoring platform that feeds into our global threat monitoring." Cloutier also notes that because AMP Threat Grid is cued up and connected through APIs, ADP is alerted when one of its defense systems detects a potential threat. "Once a threat is detected, we run some significant analytics to help us define what malware needs attention. It's this integrated defense system that helps us defend ADP around the clock."

For Cloutier, the greatest benefits of AMP Threat Grid are its speed and accuracy. "From a speed perspective, we've greatly increased our ability to look at threatening traffic and make very fast decisions. In addition, Threat Grid's threat intelligence allows us to look beyond the walls of ADP into the markets and industries we serve. This allows us to look at specific threat information for specific types of data and take proactive, preventative action."

Cisco and the AMP Threat Grid team use their global expertise, technical depth, and knowledge to help ADP optimize its security platform and protect the company every day, notes Cloutier: "It's that type of deep technical partnership that we expect out of our relationship with Cisco and Threat Grid. Our investment in Cisco has been a smart one. We have been able to leverage our existing platforms and strategies along with Cisco's technologies and expertise to accelerate the delivery of the services that we bring back to our own company."

For More Information

To learn more about Cisco AMP Threat Grid, visit www.cisco.com/go/amptg or watch the ADP video case study here.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C36-735059-00 07/15