CUSTOMER SUCCESS STORY

Infor Offers Comprehensive Cloud Security to Multiple Industries with Amazon Web Services and Trend Micro Deep Security

Website
www.infor.com

Region
Global

Sector
IT Services

Employees
12,500

Trend Micro Solutions

- Deep Security

Business Benefits

- Simplifies management of multiple security tools
- Plug-and-play implementation in the AWS cloud
- Ensures compliance and ends rogue IT
- Three to four times faster compliance audits
- Adds strategic value to security operations team

Lessons from a CISO: How to Securely Scale Teams, Workloads, and Budgets

OVERVIEW

Headquartered in New York, Infor is a leading provider of business application software, serving about 75,000 customers in 200 countries, provinces, and territories globally. In 2014, it launched Infor CloudSuiteTM, a group of industry-specific application suites, on Amazon Web Services (AWS). Infor powers many of the world's largest companies in the public cloud, offering applications purpose-built for specific industries to handle everything from the front office to mission-critical core functions.

Among Infor's first rollouts on AWS were CloudSuite Automotive, Aerospace & Defense and Hospitality. On its heels came CloudSuite Corporate, a next-generation back office system that fulfills financial, supply management and procurement, human capital management, and enterprise performance management needs. Today, Infor CloudSuite serves 3,500 customers and 45 million users in the AWS cloud. Users access the environment from 6,300 sites globally. When fully rolled out, CloudSuite will serve a wide range of industries, including high-tech, pharmaceuticals, city governments, financial services, retail, and manufacturing.

CHALLENGES

With AWS, Infor saw an opportunity to end some of the challenges of large-scale security in an on-premises environment. The security operations team used to spend a great deal of time managing and installing hardware. Their security tools did not all speak the same language, which made applying security to releases a resource-intensive task—one that jeopardized DevOps timelines. The Infor security operations team had trouble managing the exceptions that various application and operations teams required.

"We had so many siloed communications happening within those teams that my security team would end up repeating many of the requirements - we couldn't use a single policy, a single standard, or a single wiki," said Jim Hoover, Vice President and Chief Information Security Officer (CISO) at Infor.

A lack of standards also impacted overall visibility into the company's security posture. If someone bypassed standard protocols and put a server in a closet or under a desk, the unauthorized hardware could elude detection for a long period of time. A lack of visibility across the environment not only left room for error, it left room for Infor to be out of compliance or, at best, to experience a slow and painful audit procedure.

> "CISOs are able to make better decisions that drive business growth by understanding how AWS and Trend Micro work together to enhance workload security and visibility."
>
> Jim Hoover
> Vice President, Chief Information Security Officer, Infor

> "Our security and operations teams are providing more value than ever before due, in part, to the proven capabilities of Trend Micro Deep Security and the AWS Cloud."
>
> Jim Hoover
> Vice President, Chief Information Security Officer, Infor

> "With Deep Security, our security engineers can help DevOps teams respond to security events as they happen."
>
> Jim Hoover
> Vice President, Chief Information Security Officer, Infor

TREND MICRO™

Securing Your Journey to the Cloud

CHALLENGES *Continued*

In the cloud, security is a shared responsibility. AWS is responsible for the security of the physical and network infrastructure to the hypervisor layer, but Infor must protect their operating systems, applications, and data. AWS promised to relieve the Infor security team of hardware installation and upgrade duties with tools that would streamline security tasks. AWS also met a vast array of compliance and regulatory requirements, and had the right certifications and attestations to satisfy auditors.

To fulfill its part of the shared responsibility, Infor needed a security solution that improved visibility into CloudSuite environments. The solution needed to integrate seamlessly with AWS tools to improve host security and keep pace with Infor's continuous integration DevOps environment. The ideal security solution also needed to help Infor prove compliance with a variety of regulations.

WHY TREND MICRO

Before it could launch CloudSuite in the AWS cloud, Infor needed to find a security partner to protect the hosted CloudSuite offering. Infor was evaluating two security providers when AWS recommended Trend Micro™ Deep Security™. An AWS Advanced Technology Partner since 2012, Trend Micro offered security solutions that integrated directly with AWS for effortless, plug-and-play functionality.

SOLUTION

In April 2014, Infor purchased Deep Security as a Service licenses for 1,000 servers with additional licenses added once the initial deployment was up and running. Deep Security as a Service was built to augment cloud provider security and optimized for the AWS infrastructure as well as most common operating systems. "The advantage of Deep Security is it brings multiple tools into one – anti-malware, firewall, host-based intrusion protection, and web reputation. We're really happy we chose it," said Hoover.

By offering a single pane of glass for monitoring security events, Deep Security heightens visibility for the Infor security operations team. The team receives alerts of suspicious behavior or malicious activity. They know when something is out of compliance and can rein it in quickly. "If someone stands up an unapproved server in AWS, Deep Security puts that on the portal right in front of me, so I can see there is a new system that's not managed by Trend Micro," said Hoover.

Deep Security as a Service relieves security operations teams of many time-consuming, repetitive tasks. It secures cloud workloads in minutes and provides automatic protection for new AWS instances. It addresses major compliance requirements and provides auditable reports that document attack prevention and policy compliance. Trend Micro handles the heavy lifting, such as managing product and kernel updates, and setting up and maintaining the security database.

RESULTS

Deep Security replaces four or five different tools that Infor used to use to provide security services. "The best part is we get one portal to look at," said Hoover. Between the portal and a weekly report, Hoover's team has everything they need to find out who provisioned a server without Deep Security on it and why. The visibility keeps Infor compliant and makes audits three to four times faster than they used to be. Also, the practice of putting something into AWS without approval has mostly stopped. Not only is rogue IT now impossible to hide, but employees no longer need it, because Infor can stand up a secure system in minutes, often for immediate use.

Tight integration and automation between AWS and Deep Security add to Infor's security posture and ensure fine-grained control. "Our teams now think securely, which improves the likelihood that implementations will be secure," said Hoover. "They have one standard, one set of policies, one set of directions that are posted in one place on a wiki and followed by everyone." In this new standards-based environment, Deep Security automatically extends security to Infor's continuous integration pipeline. "With Deep Security, our security engineers can help DevOps teams respond to security events as they happen," said Hoover.

It used to take as much as 48 hours to decide how to respond to new threats. Now Deep Security and AWS work together so DevOps and Security (DevSecOps) can team up to find vulnerabilities and automatically get patches and new software versions out into the environment quickly without disrupting business. With this new agility, the security operations team is positioned to add value at the strategic level.

"Security used to be thought of as an inhibitor to development, but not anymore. Our teams understand that security is built into the environment and that the security team isn't going to hold or stop releases. The security team is helping to steer the effectiveness of cloud operations," said Hoover.

While the CISO benefits directly from better visibility into the network, all leaders within the enterprise benefit from cultural shifts brought on by the unprecedented visibility of AWS and Deep Security. Hoover outlines the benefits for each role: "CISO's benefit from seeing what's being provisioned and judging how well it is managed; CIO's can perform network segmentation at an incredible level and respond more quickly than ever before to the needs of the organization; COO's gain the rhythm, effectiveness, and efficiencies associated with doing an audit improve dramatically. Finally, the CFO can see exactly what environments are being stood up for each business and tag resources for automatic shutdown."

FOR MORE INFORMATION

For more information, please check out **www.trendmicro.com/aws**

NOTE: At the 2015 AWS re:Invent conference, Trend Micro sponsored the presentation, "Lessons from a CISO: How to Securely Scale Teams, Workloads and Budgets." Jim Hoover, Infor Vice President and Chief Information Security Officer, discussed Infor's journey to the AWS Cloud. Matt Yanchyshyn, senior manager and solutions architect at AWS, offered perspective on best practices employed by Infor. Adam Boyle, Trend Micro Director of Product Management, chaired the discussion. This success story draws from that discussion. View recorded session **here**.