Keeping Personal Data Private with RSA Technologies

AT-A-GLANCE

Challenges
– As a global provider of HR and payroll services, ADP handles more social security data than any other company. It is imperative that it protects this information.
– ADP needed to understand cyberthreats and fraud attempts, inside and outside its environment.

Results
– A combination of RSA NetWitness® Logs and Packets, Adaptive Authentication and RSA SecurID® Access enable the ADP team to see attacks across the entire infrastructure.
– RSA Archer collates all security information and business processes to provide clear visibility of the organization’s security posture.

“RSA NetWitness Logs and Packets is used to defend ADP every single day. It gives us the ability to see attacks across our entire infrastructure.”

ROLAND CLOUTIER, GLOBAL CHIEF SECURITY OFFICER, ADP
ADP is a global provider of cloud-based Human Capital Management (HCM) solutions that unite HR, payroll, talent, time, tax, and benefits administration; and a leader in business outsourcing services, analytics and compliance expertise. The company’s experience, deep insights, and cutting-edge technology aim to transform human resources from a back-office administrative function to a strategic business advantage. With 610,000 clients worldwide, ADP helps organizations of all sizes to unlock their business potential.

ABOUT RSA
RSA’s Intelligence Driven Security solutions help organizations reduce the risks of operating in a digital world. Through visibility, analysis, and action, RSA solutions give customers the ability to detect, investigate and respond to advanced threats; confirm and manage identities; and ultimately, prevent IP theft, fraud and cybercrime. For more information on RSA, please visit www.rsa.com.

CONTACT US
To learn more about how RSA products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller — or visit us at www.rsa.com

Please tell us about yourself and your organization
My name is Roland Cloutier, and I am ADP’s Global Chief Security Officer. ADP is a human capital management company. We’re a technology and services organization that ensures our clients can manage their most valuable assets, their people. From the time that an employee of our client is recruited to the time that they retire, we provide all the human resources programs, including benefits management and retirement management.

How mission-critical is security for your business?
We manage some of the most sensitive information for our clients, and the most protected information of their employees. We have more social security numbers in our platforms than anyone outside the social security administration. We move an average of about $1.7 trillion a year in payroll, and we have the benefits and bank account information for millions of employees around the globe. So security is everything at ADP.

How do you work with RSA?
RSA is a big component of ADP’s trusted platform security initiative. This covers the defensive technologies for both our go-to-market hosting operations as well as our enterprise platforms.

Does RSA support your authentication strategy?
We use the authentication technologies in our hosting environments to protect not just our cloud platforms but also our fraud defensive programs. We use the authentication data in our analytics to look for fraudulent activities. We use RSA SecurID Access when we need critical insurance on multi-factor authentication, whether it’s for VPN, access, or advanced protection of data sets within our own environment. We have about 50,000 or 60,000 people using it on our platform, and it is considered our best defense for understanding who’s at the other end of the wire.

How do you protect your infrastructure?
We use technologies like RSA NetWitness Logs and Packets to help us understand threat traffic within our environment. We use RSA’s GRC platform for governance risk and compliance, RSA Archer, which acts as the central workflow for all of our converged security areas. So it doesn’t matter whether it’s incident response, cyber operations, or operational risk management: all the information and business processes flow through Archer.

Tell us about your use of RSA NetWitness Logs and Packets.
RSA NetWitness Logs and Packets is used to defend ADP every single day. It gives us the ability to see attacks across our entire infrastructure.

It is predominantly used in our cyber and fraud areas to look at data coming from multiple parts of our business and articulate that into a threat story. So, for instance, we might take information from our cyber defense technology, our firewalls and IDS and other things of that nature. But we also bring in information from our business processes, our transactions; things where we know how they should operate. We create contextual alerts for analytics that we couldn’t do with standard security technology. RSA NetWitness Logs and Packets allows us to really understand whether a business process is good or bad, and whether there’s a potential threat to it. On the fraud side we use it in much the same way. We take transaction data, information out of our authentication platforms, and data from external entities, and we allow the analytics platform to say whether it’s a fraudulent attempt to access or move money.

What advice would you offer to others about best practice?
First and foremost, set the standard for data logging and ensure that everybody understands what that means. If you don’t, it’s going to be very difficult to collect the appropriate information.

Next, start thinking about the scope: what you will do and not do. I think it’s important to make a decision on whether you will use RSA NetWitness Logs and Packets to do just reporting, or for cyber threat intelligence, or for everything. Once you define your scope you'll be able to better identify the architecture you need, or that you'll need to grow into over the following years.

And finally, I would say make sure you’re enriching your data. The problem is that most people look at the box they live in: their company and what’s coming at them. But if you’re not looking beyond that, looking at the industry you’re serving, or the markets that you’re in, or who’s attacking other people, how are you going to be able to meet the oncoming threat? So use enrichment through intelligence sharing, through feeds, through whatever makes sense to your business.

To view the full video interview, go to http://www.emc.com/link