PARTNERS HEALTHCARE

Boosting visibility and insights with RSA Security Analytics, Archer and SecurID®

AT-A-GLANCE

Challenges

- Partners HealthCare holds patient data, intellectual property and employee personal information, all of which must be protected
- Security is an increasingly important priority for the board, so clear visibility and reporting on security status is essential
- The organization needed to boost automation and standardize processes to enhance its security posture and compliance

Results

- RSA SecurID enables customizable risk profiling to ensure that over 65,000 employees can access Partners systems remotely, without compromising security
- RSA Archer provides enterprise-wide GRC support, integrating input from SOC and other feeds, and enabling the team to create standard processes and workflows
- RSA Security Analytics provides clear visibility across all network traffic, allowing the team to identify correlations across the business

“Analytics are critical. [RSA Security Analytics] can help us determine standard behavior, and what’s one standard deviation away, or two standard deviations away, so that we have better visibility into what potential attackers are doing.”

JIGAR KADAKIA, CHIEF INFORMATION SECURITY AND PRIVACY OFFICER, PARTNERS HEALTHCARE
Partners HealthCare is a not-for-profit health care system that is committed to patient care, research, teaching, and service to the community locally and globally. Collaboration among its institutions and health care professionals is central to its efforts. Founded in 1994 by Brigham and Women’s Hospital and Massachusetts General Hospital, Partners HealthCare includes community and specialty hospitals, a managed care organization, a physician network, community health centers, home care and other health-related entities.

Please tell us about yourself and your organization
I’m Jigar Kadakia, Chief Information Security and Privacy Officer for Partners HealthCare. We’re a large academic medical center, with various associated hospitals. We also operate a clinic in Africa and have a number of practitioners and clinicians practicing internationally.

How mission critical is security to your organization?
Security is an important component of the overall strategy within Partners HealthCare. First and foremost our goal is to protect patients’ health, but it’s important to protect their privacy as well as we handle their sensitive records and clinical information.

We have a lot of other types of information to protect, including intellectual property and research data from our academic activities, and the personal details of over 75,000 employees.

The large number of recent breaches involving well-known public companies means security has become a board-level discussion for us. A sub-committee of the board meets quarterly to talk about security, cyber security and privacy, and we issue regular updates to the board and other key executives. So it’s critical, and it’s a high priority within the organization.

What’s your security strategy?
We have a long-term security strategy. It’s been a multi-year plan with multiple components, starting from process procedures, moving on to enhancing and automating processes, and then adding technology to further automate processes and expand our security reach.

So we have a number of in-house operation centers set up, including a security operations center (SOC) as well as a network operations centre that recently implemented to enhance our knowledge of what’s happening within our environment. We have a large research community as well as a large employee base and a number of affiliate doctors that interact with our environment, so we have to have a better grasp of what’s happening not only within the hospitals but also our physician practices, the research community and other components of our business.

What are your top priorities?
Firstly, we’re looking to achieve better automation overall, so we can have automated events and alerts and address things in an automated fashion. Incident response is really important, not only from a reporting and standpoint with the HIPAA rule, but also it’s important internally with regards to malware and viruses and getting those things remediated quickly.

Secondly, we want better visibility within the environment, so we have better view into what’s going in and coming out of our environment. And lastly, just moving forward, doing a great job of protecting our data.

Which RSA solutions have you implemented?
We have deployed RSA SecurID® to enable remote authentication for physicians and researchers working off-site, and we have around 65,000 regular users. We leverage the soft token capabilities, helping our international researchers and physicians connect to our systems in a secure manner.

We really value the ability to create risk profiles of our community and our user population and then use those risk scores to help evaluate to whom we’re giving remote access. So if you’re an unknown IP address from France for example, you may not be allowed into our network. Being able to customize the risk portion of the SecurID tool in this way has been a huge enabler for us.

We’re looking to integrate Archer as our enterprise-wide GRC platform, and integrating the SOC modules so that we can have a better grasp and visibility of events and incidents, as well as automated workflows to address the long term remediation of incidents. We’re also planning to leverage Archer for incident response management, as well as risk management processing specifically around our enterprise risk assessments and our third party risk assessments.

Security Analytics will bring us the visibility of inter-network traffic, meaning east-west traffic versus the traditional north-south traffic that most organizations have good visibility into. This will give us the opportunity to correlate across multiple areas within our environment.

What role do analytics play in your environment?
Analytics are critical. Everyone talks about data warehouses, data analytics and so on, but it’s important to understand known behavior and unknown behavior to identify when there’s a deviation. The analytical component can help us determine standard behavior, and what’s one standard deviation away, or two standard deviations away, so that we have better visibility into what potential attackers are doing.
Can you share any learnings or best practices?
I think the most important things overall is having a solid foundation of policies and procedures that not only are understandable but have the support of leadership. In addition to that I think it’s key to have strong processes in which the business can be engaged, so users see it as not just a security process but an overall business process.
The biggest pitfall to avoid is trying to do too much at the same time, and thinking that one solution or technology is going to solve all your problems. Technology can help automate and create efficiencies but it may not solve every problem that you face, so there’s got to be some type of custom process that’s unique to your environment. too much at the same time, and thinking that one solution or technology is going to solve all your problems. Technology can help automate and create efficiencies but it may not solve every problem that you face, so there’s got to be some type of custom process that's unique to your environment.

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