Government Department Boosts Network Immune System with RSA® NetWitness®

**AT-A-GLANCE**

**Key Requirements**
- Centralize management of security over half a million geographically dispersed access points
- Ensure ability to identify and respond in real time to malicious attacks
- Support both central and department-level security priorities

**Solution**
- RSA NetWitness enables forensic investigation of events from any perspective
- Network-wide visibility enables faster detection and resolution of real time threats
- Integration with other security-intelligence feeds gives team deeper insight and reporting capabilities

**Results**
- Intelligence on queries and blacklisted IP addresses can be transmitted quickly across entire network
- Rapid adoption by all operating divisions underlines usability and effectiveness of solution
- Increased agility to respond to advanced malicious code security events

“Industry opinion and the unique features and functionality of RSA NetWitness, added to the fact that three of our operating divisions were already using it with demonstrable success, persuaded us to put our trust in the solution.”

KEVIN CHAREST, DIRECTOR & PROGRAM MANAGER CSIRC, HHS

The United States Department of Health and Human Services (HHS) is the principal agency for protecting the health of all Americans. It is made up of the Office of the Secretary and 11 operating divisions, such as the Food and Drug Administration (FDA), the Centers for Disease Control (CDC), and the Centers for Medicare and Medicaid. HHS employs more than 100,000 people across the agency.

**KEY REQUIREMENTS**

Few organizations can claim to be as complex as HHS. Its large budgets, wide-ranging fields of influence, and multiple operating divisions – not to mention thousands of staff – mean the task of managing and protecting the IT network that holds everything together is a particularly challenging one. With each employee often using more than one device, HHS estimates that it needs to secure as many as half a million IP addresses across its network.

“Being made up of different operating divisions means we’ve often had quite a fragmented approach to security,” explains Kevin Charest, Director & Program Manager CSIRC, HHS. “Each operating division has its own internal team, resources, and processes, so our central security team often struggled to gain the detailed visibility we needed to allocate resources quickly in the event of an incident or threat.”

With malicious attacks an unfortunate fact of life for all government organizations, and advanced persistent threats on the rise, Charest and his team wanted a more robust system to keep ‘bad actors’ out of HHS’s network. “In the past, we could only be reactive, responding to an attack when it had already entered our network,” comments Wally Wilhoite, federal lead of the digital forensics team at HHS. “We needed to respond faster, regardless of the type of attack or where it occurred across our divisions.”

The team at HHS’s Computer Security Incident Response Center (CSIRC) set out to identify a full-packet-capture network-security solution that would enable it to more effectively carry out forensics post-event as well as to identify emerging threats in real time. It was essential...
that the central team have full visibility and control across the network, while providing an easy-to-deploy and user-friendly solution at a department level. “We can’t force the operating divisions to adopt our preferred technologies so we needed to encourage them to do so by suggesting the most effective and appealing solutions,” Charest adds.

**SOLUTION**

After carrying out extensive research into the solutions available, HHS identified RSA NetWitness as the most compelling. “Industry opinion and the unique features and functionality of RSA NetWitness, along with the fact that three of our operating divisions were already using the technology with demonstrable success, persuaded us to put our trust in the solution,” explains Charest.

HHS chose to purchase the RSA NetWitness platform, along with software modules Investigator for interactive network forensics, Live Enhanced for threat-intelligence feeds, and Informer for automated reporting and alerting. The Spectrum module, for automated malware analysis, was also purchased for activation once the initial roll out was completed.

One of the key features for the HHS team was the scalability of the solution, which would stand up to the challenge of a large initial deployment and ongoing growth. Wilhoite adds: “Not only was the technology capable of supporting our heavy demand, but RSA provided great support to make sure it all went in without a hitch. The team proposed a network design and helped us implement it, showing a commitment and level of consultancy that we weren’t offered by other vendors.”

Implementation also involved making sure the RSA NetWitness platform was fully integrated with HHS’s existing security information and event management (SIEM) system. This ensured that any alerts and feeds from RSA NetWitness could be displayed to the central security team in the same consolidated dashboard with those of the SIEM platform.

“The ability of RSA’s solution to deploy easily at a local divisional level while passing all the metadata we needed into this single point for centralized management at the CSIRC was also very important for us,” continues Wilhoite. “No other solution we looked at could achieve this within our resource and budget constraints.”

Deployment began at the CSIRC site in Atlanta, with roll out to half of the operating divisions completed in less than six months. The response from the operating divisions has been very positive, and HHS expects deployment across all sites to be completed within 18 months of the first CSIRC implementation. Charest observes: “Some people thought I was committing career suicide when I set such an ambitious timescale for this project, but thankfully RSA NetWitness hasn’t let me down.”

The introduction of the solution has enabled HHS and its operating divisions to implement a range of new proactive security practices, including:

- Running automated queries and checks for known threats and in response to alerts from the Department of Homeland Security
- Carrying out in-depth forensic analysis in real time when APTs and other malicious activities are spotted
- Recording and storing network traffic over time, so backward-looking analysis can be carried out for more complete incident response than was ever possible before

**RESULTS**

“Our visibility across our network – both locally and at a department level – has without question significantly increased since implementing RSA NetWitness,” reflects Charest. “We were often blind to coordinated threats before, but standardizing on the RSA NetWitness solution not only gives us the visibility to spot anomalies, but also the capabilities to resolve them before they do any damage.”
HHS can now use powerful forensics tools to mine data correlated from multiple sources, particularly the RSA NetWitness and SIEM feeds, to pinpoint exactly where an incident has occurred, within minutes. Additional security resources can then be deployed exactly when and where they are needed, to keep HHS’s network and data secure. Being able to run in-depth reports and analysis quickly, on-demand, also means that the organization is better equipped to verify any compliance requests faster.

With the solution’s automated alerting capability, the teams at the CSIRC and within the operating divisions can also proactively look out for traffic anomalies and rapidly take action if needed. “The ability to combine both local and central control means that in the event of an incident we can resolve it at the initial point of contact and quickly issue an alert across the wider network so that we’re prepared if a similar attack strikes another operating division,” explains Wilhoite. “For divisions that may only have a one-person security team, this automated, proactive approach makes an enormous difference.”

The CSIRC team has been pleased with the enthusiasm shown by the operating divisions for the solution. “They won’t use it if they don’t feel the technology is good enough, so the widespread adoption is an affirmation that we chose the right solution,” concludes Charest.

Indeed, the organization has set up a common framework for discussing uses of the solution and sharing best practices across departments. It expects that additional benefits and new use cases will evolve as the solution is rolled out further and users continue to share their successes.