CASE STUDY

Center for American Progress (CAP) Deploys LogRhythm to Thwart Would-be Hackers

LogRhythm

Political think tank uses LogRhythm to derive actionable insight that improves security and operations.

Center for American Progress

Customer
Center for American Progress (CAP)
Washington, D.C.
CAP works to find progressive and pragmatic solutions to significant domestic and international problems and develop government policy proposals.

Challenges
Numerous hacking and security breach attempts, IT operational issues.

Solution
LogRhythm appliance collects, correlates, analyzes and reports on events from the desktop to the data center.

Early Results
Benefits so far from the early stages of deployment:

- Actionable insight enables the technical team members to be more efficient and effective in their jobs
- Ability to spot situations before they turn into security or operational problems
- Cost savings due to operational efficiencies

> "What sold me on LogRhythm was ... the simple, straightforward way we can get real insight to our network. Everyone in IT can use it to be more effective."
>
> **Steve Heibein**
> VP Technology
> Center for American Progress

Steve Heibein and Nick Levay are accustomed to working with subject matter experts who provide deep analysis and meaningful insight. Heibein is Vice President of Technology and Levay the Manager of Information Security and Operation at the Center for American Progress (CAP), a leading political think tank. CAP works to find progressive and pragmatic solutions to significant domestic and international problems and develop government policy proposals. The organization boasts dozens of experts who cover vital topics such as the economy, national security, energy and the environment.

Not long ago, CAP added one more "subject matter expert" whose job it is to provide deep analysis and meaningful insight about what is happening on the organization's computer network in order to thwart hacking attempts. This expert isn't a person, though; it's a computer application from LogRhythm that delivers valuable, timely and actionable insights into security, availability, performance and audit-related IT issues in real-time.

Background

Given its high profile and influence in the U.S. and abroad, CAP's IT infrastructure is often the target of outside attacks and attempted security breaches. CAP chose LogRhythm to monitor, correlate and alert on events that could indicate an attack is underway or a system has already been breached.

CAP's multi-vendor environment infrastructure includes 12 physical and 60 to 70 virtual servers at a co-location center, as well as about two dozen in-house servers. The organization has servers from numerous vendors, including HP, Sun and Dell; security and firewall gateways from Cisco and Juniper; and Windows-based PCs and Mac desktops. The servers run different versions of Windows and "a lot of Linux," according to Levay.

The IT department has a team of just 14 people, who manage the data center operations, provide desktop support for about 300 users, and support an extensive Web presence. Heibein says, "We have 'big organization' needs, even though we aren't a big organization staffed with lots of support people. The data we watch over is pretty important, and we have crafty attackers trying to get to it."

The Challenges

Network security is a top concern for CAP's IT team. "We get a fair number of brute force attacks," says Levay. "We have servers that get something like 60 to

70 thousand attempted logins a day by machines trying to guess our passwords." The organization also gets a large number of drive-by attacks on its websites where hackers are looking for vulnerabilities.

"Spear phishing" is another serious problem for CAP. "Hackers are always looking to compromise our desktops and user resources," says Levay. "Once they get into the network, they burrow themselves in and attempt to hide by mimicking normal user activity. Then they try to exfiltrate information."

"We were losing against these attacks," admits Levay. "Sifting through logs from different locations and trying to correlate the information was definitely taking too much time."

The team also faces the standard operational issues—common events like users getting locked out of their accounts because they've forgotten a password, or software errors stemming from an Active Directory replication problem. Significant time is spent in a reactive mode, diagnosing problems and trying to figure out what happened and why.

The multi-vendor environment doesn't make things any easier. "On our security gateways, we have a good way of diving into our traffic logs, but we didn't have a way of doing this across multiple vendors' products. And, we didn't have a way of aggregating our Windows logs so we could see a big picture rise out of everything," says Levay.

The Solution

CAP's IT team knew it needed a tool to automate the collection, correlation and analysis of event data from the devices spanning the desktop to the data center. They compared and evaluated several commercial and open source security information and event management (SIEM) products; LogRhythm was a standout from the very beginning. "In a feature-by-feature comparison, LogRhythm was basically the leader or among the leaders in almost every feature," says Heibein.

As the lead evaluator, Levay was particularly impressed with LogRhythm's ability to handle data "just about any way I can throw at it." The software pulls in Windows logs, syslog, and Netflow information from any and all of CAP's devices. "In addition, LogRhythm has an agent architecture but it doesn't require an agent architecture for most of the information I'm concerned with," says Levay.

"The log aggregation tool—how quickly you can drill down to the actual information you're looking for—that's one of the places where LogRhythm really shines," according to Levay. "We can load up the client, start an investigation based on some piece of information or some user we're looking at, and in no time we can drill down into the data to see what's happening."

"We looked at a lot of products," says Heibein, "but what sold me on LogRhythm was when Nick demonstrated the simple, straightforward way we can get real insight to our network. Everyone in IT can use it to be more effective. LogRhythm gets the information out of the realm of a subject matter expert and into the hands of more of the staff."

With LogRhythm, the staff can get answers to complex questions that would have been time-prohibitive before. These answers reveal abnormal behavior that could indicate a security breach or an operations problem. For example, Levay can ask to see the logs for all TCP sessions that lasted more than an hour but downloaded less than a megabyte of information. This odd query is born out of an attack that CAP suffered a few months ago.

"The hackers try so hard to stay under the radar that they try to mimic our legitimate users' patterns," says Heibein. "LogRhythm helps us discern very subtle differences between a hacker's activities and those of a regular user. If one of our employees left a connection open for an hour, we'd expect to see him dumping real big data. The pattern that LogRhythm reveals is unusual for a real person but it might work out fine for a bot."

> "We looked at a lot of products," says Heibein, "but what sold me on LogRhythm was when Nick demonstrated the simple, straightforward way we can get real insight to our network. Everyone in IT can use it to be more effective. LogRhythm gets the information out of the realm of a subject matter expert and into the hands of more of the staff."

Price and ease-of-use were important criteria in the selection process. LogRhythm led the pack on both fronts. "The other vendors don't have the features that LogRhythm has at the same price point," says Levay. "Other solutions require you to strap on components that come standard with LogRhythm. You might have to pay an extra 60 or 70 thousand dollars to get a correlation engine. The way LogRhythm is put together definitely made a difference that led us to choose this product."

The Results

On the first day that CAP had LogRhythm running, the IT team was able to see previously undetected problems with their Windows configuration. Levay says he began turning to the LogRhythm dashboard in situations where he normally would go out and log into individual machines. "On day one we realized immediate visibility improvements," says Levay. "There were things we didn't see before." For instance, he was really surprised to see how many pages people print. "This is something we never saw before. We have now changed all our printers to default to double-sided print to save money."

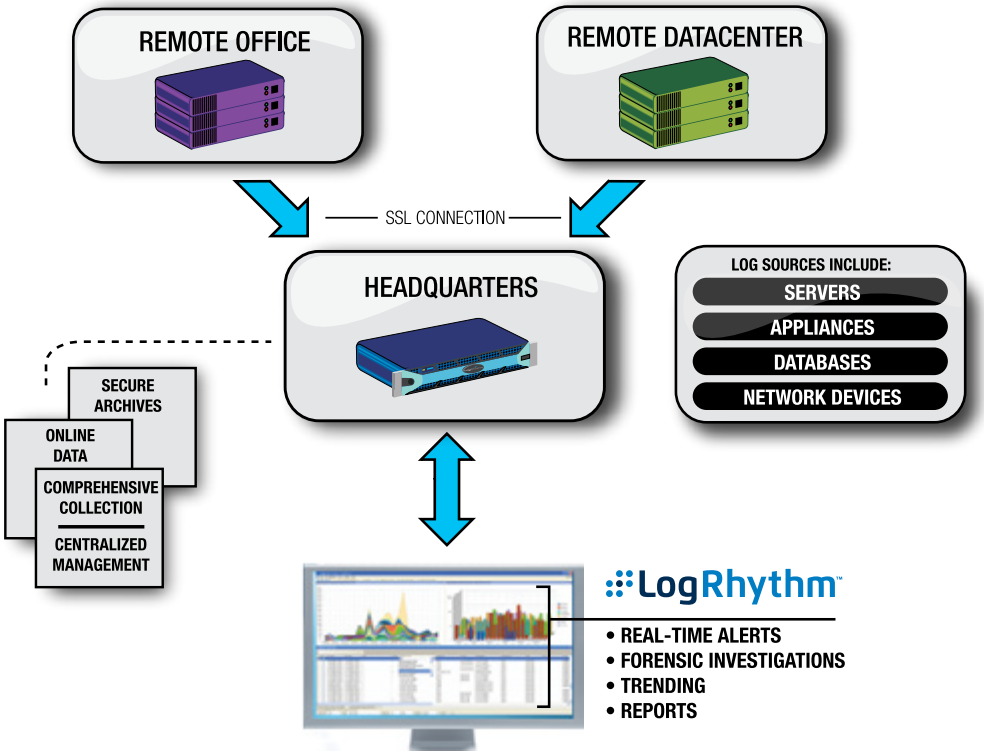
Another shock was the sheer number of authentication failures and the volume of password-guessing. "We knew we were under attack, but we had no idea how pervasive the problem is," Heibein admits. Now they can plan better defenses for their sensitive systems.

What's more, Heibein believes LogRhythm could help CAP determine the extent of a breach if it happens again. "We were hacked one time, and we didn't know what information the thieves got. Without knowing, we had to send out thousands of letters to people saying, 'We know they got into this range of machines and it may include social security numbers.' We didn't know for sure if that information was compromised, but we had to notify in order to be compliant with state and federal laws. If something like this happens again, we expect that LogRhythm could tell us exactly where a hacker went on our systems. This would cut down on our notifications." Better yet, LogRhythm can help prevent or mitigate future breaches by alerting when suspicious events are happening.

Looking Ahead

Based on what he's seen so far, Levay believes they are going to see big benefits. The team is expecting to see even bigger benefits after they bring in the logs from the web applications, and deploy file integrity monitoring and endpoint monitoring & control on the desktops.

"There's so much capability here that we haven't gotten to yet, but we intend to," says Heibein. "It's easy to get to that 80/20 point quickly, but LogRhythm is a very deep product if you want to keep growing. It's a sophisticated product, but at the same time, it's easy to use." Heibein and Levay are happy to have purchased this deep-thinking and analytical "subject matter expert."



LogRhythm Provides Global Insights into CAP's Entire Network