Red Hat

Emory University conquers sudo threat with Red Hat

EMORY UNIVERSITY

Emory University's security team alerted the IT team of a security vulnerability that needed to be remediated quickly. An event such as this would have been very disruptive to the team's regular operational and project work, not to mention the hours required to manually remediate the patch across more than 500 Red Hat Enterprise Linux servers as well as the potential data breach. Emory used Red Hat Ansible Automation Platform to write a playbook and automate remediating all hosts. What would have taken up to two weeks to remediate across all servers took collectively four hours.

Software

Red Hat® Ansible® Automation Platform

Red Hat Enterprise Linux®

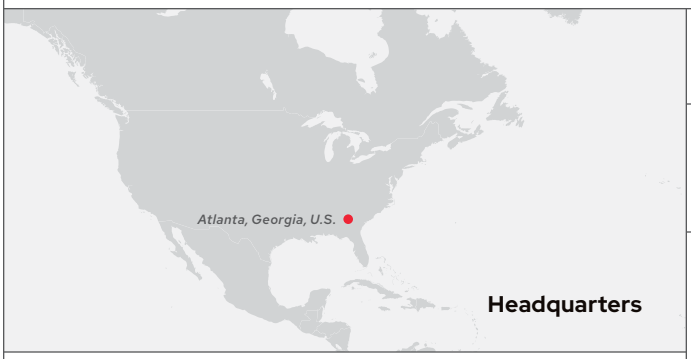
Services

Red Hat Training

Red Hat Professional Services

Partner

Amazon Web Services



Headquarters

"People didn't think we could patch Linux servers every 30 days, but with Red Hat Ansible Automation Platform it's possible and it's necessary."

Steve Siegelman
Manager of Systems Engineering
Office of Information Technology
Emory University

Education

15,400
university faculty and staff

Benefits

- Completed patch updates in hours, not weeks
- Freed valuable resources to focus on higher-value projects
- Improved agility in face of unique COVID-19 challenges

Protecting research and education

Emory University is one of the most prestigious colleges in the U.S., with 15,000 students at its metro Atlanta campuses, research ties with institutions around the globe, and the operator of Georgia's largest healthcare system.

With such a high profile, Emory is a natural target for cyberattackers looking to exploit and gain access to confidential information through its digital footprint. Once there is an entry through a vulnerability, the concern is the attacker would surreptitiously move throughout the network taking intellectual property and slipping away undetected. Educational institutions are also a primary target for ransomware and other cyber extortion techniques.

The school's Office of Information Technology (OIT) is tasked with maintaining systems for students, staff, faculty, researchers, and other stakeholders to ensure that networks and data are protected from unauthorized access and potential security breaches. This is why there was such an alarm in January 2021 when OIT's security team found a vulnerability within Emory's Red Hat Enterprise Linux systems affecting the program's sudo utility.

"When you don't have to handle repetitive tasks that could be taken care of by Ansible Automation Platform, that frees people to work on other more critical projects."

Steve Siegelman
Manager of Systems Engineering
Office of Information Technology
Emory University

"Vulnerabilities are graded by our security team so that we know how quickly it has to be remediated," said Steve Siegelman, Manager of Systems Engineering at Emory's OIT. "Our policy is that those that are more serious need to be remediated within 30 days, others that aren't as critical can be fixed in 60 to 90 days. This particular one needed us to drop everything and get it patched."

Identifying vulnerabilities and organizing a response

Siegelman and his team are somewhat used to "doing the invisible work," keeping the backend systems functioning to allow for the front-facing apps and programs to shine and operate reliably. They rely on Red Hat Ansible Automation Platform as a single automation solution that helps Emory's various IT teams collaborate. The platform brings together Red Hat Ansible Engine, Red Hat Ansible Tower, and Red Hat Ansible Network Automation, along with new capabilities including Certified Content Collections, Automation Hub, and Red Hat Insights for Red Hat Ansible Automation Platform in a single subscription. These new capabilities are designed to create a more consistent automation experience and help teams like Emory's solve big challenges.

When they found the sudo threat, however, it was their turn to take the point against a dangerous vulnerability.

Anyone who got access to the system could easily elevate their credentials and gain administrative privileges, which could lead to a potentially devastating security breach if it were exploited. The vulnerability stretched over several university departments and business units. A breach like this could have expanded across the university.

"Since we're central IT, handling much of the administrative systems and doing a lot of sensitive computing on our side, we took this problem pretty seriously," said Siegelman.

Automation to accelerate remediation

Completed patch updates in hours not weeks

Creating the patch for this potential breach was not difficult, but the hard part was the application of the patch.

With more than 500 servers using Red Hat Enterprise Linux under their charge, OIT knew they had a difficult road ahead if they had to install the patch manually, which would have put the university's infrastructure in danger. The solution was to use an Ansible Playbook to apply the patches automatically to each server. What would have taken up to two weeks to remediate across all servers took collectively four hours.

"We were in a time crunch. We saw that we had this great tool in Ansible Automation Platform that could easily handle a project of this scope," said Siegelman. "It did the job; we couldn't have made this fix in a timely manner without automation."

> "We couldn't have made this fix in a timely manner without automation."
>
> **Steve Siegelman**
> Manager of Systems Engineering
> Office of Information Technology
> Emory University

Freed valuable resource to focus on higher value projects

Emory's journey to Ansible Automation Platform began a few years before as the university looked for a tool that would automate apps and IT infrastructure. "Ansible Automation Platform was the easiest choice," said Siegelman. "The training was thorough and our goals to get our systems standardized and stable and make sure we're automating everything we could were met."

Ansible Automation Platform was first applied to Emory's financial systems before it was rolled out to the student and HR systems. "Automation has been a huge feature for us. We're pressed to do more with the same number of staff like many other organizations. And when you don't have to handle repetitive tasks that could be taken care of by Ansible Automation Platform, that frees people to work on other more critical projects," said Siegelman.

Improved agility in face of unique COVID-19 challenges

Much of Emory's infrastructure is on-premise, but the school is also migrating many programs and applications to the cloud. By using Ansible Automation Platform to automate those jobs that can be automated, more hands-on work can be put into Emory's cloud migration project.

Another example of the system's flexibility was in March 2020 when Emory, like nearly every school and organization, was forced to close its buildings and send students and staff to work from home. The university needed controls in place with tracking to clear those who needed to be on campus during the lockdown.

OIT realized it needed database servers to be quickly deployed in order to handle this new task of tracking essential employees, organizing who they were and their health screenings and training.

The selected staff had to fill out questionnaires that were then fed into the system and they received a certification that allowed them on campus. Setting this up on the servers manually would have taken a few days. "With Ansible Automation Platform it was done in a matter of minutes," said Siegelman. "It showed what automation on the backend could do."

Automation as cultural transformation

The need for automation is critical to Emory's plans moving forward, especially as it transitions to the cloud. "We have some legacy systems that are a mix of old and new builds, and we're putting a great deal of effort into our AWS platform," said Siegelman. "With these different systems, Ansible Automation Platform allows us to have repeatable processes that are standardized. No matter if the platform is in the cloud or on premises, everything looks in place."

The OIT has been able to use automation to patch servers and do server configurations and it expects to do more as it continues the move to the cloud. Enterprise resource planning (ERP) upgrades would have taken many hours as the server was built, and the Emory-required customizations were made regarding security, standards and logins. Using Ansible Automation Platform has changed how OIT staff think about their tasks.

"We're thinking about what we can automate first," said Siegelman. "There's a new security tool we're pushing into our existing servers using Windows and Linux systems with Ansible Automation Platform and it does the job effortlessly. With a little bit of provisioning, it will be automatically included on anything new we deploy."

Another implementation came about when upgrades were needed on Emory's PeopleSoft ERP infrastructure. OIT setup Ansible Tower along with a Red Hat Satellite server to orchestrate and create monthly packets of patches for automatic server updates. "People didn't think we could patch Linux servers every 30 days, but with Red Hat Ansible Automation Platform it's possible and it's necessary."

About Emory University

Emory University is known for its demanding academics, outstanding undergraduate experience, highly ranked professional schools and state-of-the-art research facilities. Emory encompasses nine academic divisions as well as the Carter Center, the Yerkes National Primate Research Center, the Michael C. Carlos Museum, and Emory Healthcare, Georgia's largest and most comprehensive healthcare system.

Red Hat Innovators in the Open

About Red Hat Innovators in the Open

Innovation is the core of open source. Red Hat customers use open source technologies to change not only their own organizations, but also entire industries and markets. Red Hat Innovators in the Open proudly showcases how our customers use enterprise open source solutions to solve their toughest business challenges. Want to share your story? Learn more.

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers develop cloud-native applications, integrate existing and new IT applications, and automate and manage complex environments. A trusted adviser to the Fortune 500, Red Hat provides award-winning support, training, and consulting services that bring the benefits of open innovation to any industry. Red Hat is a connective hub in a global network of enterprises, partners, and communities, helping organizations grow, transform, and prepare for the digital future.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com

redhat.com
#F29867_0821