How a leading research university uses cloud security to protect its users, data and open culture.

Organization snapshot

Organization: University of Oklahoma (OU)

Headquarters: Norman, OK

Users: 36,000 - Cloudlock
       6,000 - Umbrella

Objective: OU’s campus-wide move to Office 365 required a new security approach to protect its highly sensitive and heavily regulated data in the cloud and on premise.

Solution:
Cisco Cloudlock
Cisco Umbrella

Impact:
• Quickly remediated a set of compromised accounts
• Significantly decreased malware infections
• Increased blocked threats by thousands per hour
• Secured users, data, and apps in the cloud
• Cut security administration and remediation time

“The all around experience with Cloudlock has been terrific. From DLP to UEBA, we’ve gotten the visibility we need into our cloud environments and have been able to extend our security policy to those locations.”

Aaron Baillio
Managing Director, Security Operations and Architecture
University of Oklahoma
The objective

Security in the multi-cloud era

Once known primarily for its national championships in multiple sports, the University of Oklahoma (OU) has developed into a world-renowned research institute that’s as accomplished off the field as it is on it. With nearly 1 million square feet dedicated to public and private sector collaborations on its Research Campus, OU has achieved the Carnegie Foundation’s highest tier of research activity classification.

“The mission of the university is to promote the exchange of ideas, and that requires open protocols and the right mix of cloud and on-premise access,” says Aaron Baillio, who manages security operations and architecture at OU. “Our users are increasingly active in the cloud via Dropbox, Amazon Web Services (AWS), Salesforce, among other applications.”

When the university moved to Office 365, OU grew concerned about the possibility of account compromises. OU recognized a need for more visibility into its cloud environment in order to protect its highly sensitive research data, as well as HIPAA and PHI data. “Our research data is a competitive advantage. Loss of this data would not only pose a risk to our reputation but could cost the university thousands of dollars and lead to loss of contracts or future research opportunities,” says Baillio.
The solution

Protecting sensitive research data and student accounts

For visibility into data and applications in the cloud by user and device, the university explored cloud access security broker (CASB) solutions.

“We turned to Cisco Cloudlock because they offered strong security, extensive experience in higher education, pricing agreeable to academic budgets, and more customization options than competitors, plus an API approach that covers on and off-network activity,” says Baillio. “Cloudlock helps ensure regulatory compliance in cloud apps like Dropbox, in which it prevents us from accidentally posting HIPPA or other personal health information. It answered our need for data leak prevention while ensuring compliance with the many regulations governing the data in our cloud environment.”

To address the increase in malware, OU initially considered several web filtering solutions, but realized that they lacked the capabilities and threat intelligence that Umbrella could provide.

“We liked the fact Cisco Umbrella utilizes real data captured from a large percentage of global DNS traffic and also draws from Cisco’s Talos threat intelligence. Our student accounts are especially vulnerable to malicious links that could lead to malware and ransomware but now Umbrella enables us to block these destinations before a connection is ever established,” he says.

After implementing Cloudlock, OU next added Umbrella as a first line of defense against internet threats like ransomware, malware and phishing attacks. OU also implemented Umbrella virtual appliances with AD integration to add visibility into user activity.

“\n
“We liked the fact Cisco Umbrella utilizes real data captured from a large percentage of global DNS traffic and also draws from Cisco’s Talos threat intelligence.”

Aaron Baillio
Managing Director, Security Operations and Architecture
University of Oklahoma

© 2018 Cisco and/or its affiliates. All rights reserved.
The results

Actionable insight into cloud activity and threat traffic

“Cloudlock gave us visibility about our users and data in the cloud that immediately led us to lock nearly 200 compromised accounts, which was a quick win for UEBA and IT,” says Baillio. “Within days, the alert pattern made it clear that we were looking at repeated compromise activity rather than a few one-off incidents.”

By quickly identifying anomalous user activity that is indicative of a compromise, Cloudlock has allowed OU to pinpoint its source and confidently block and reset affected accounts to keep it from spreading. “Cloudlock enables quicker investigations and remediation, so fewer users lose access and require help desk support,” says Baillio.

The deployment of Cisco Umbrella has helped the university to defend against ransomware.

“When we were attacked by Locky ransomware, Palo Alto Networks firewalls took four days to detect it, while antivirus software did not catch it for a week,” Baillio says. “Since deploying Umbrella’s blanket protection against outbound traffic and attacks, we’ve been able to block more than 1,000 threats per hour, and—while a sister university not using Umbrella continues to suffer repeated attacks on network share files—ransomware has become an institutional non-issue on the OU Norman campus.”

OU’s steadily improving BitSight score, which factors in command-and-control traffic coming from IP space, reflects a substantial decrease in malware; a pre-Umbrella score of F has jumped to a post-implementation C, and continues to rise.

“Overall we’ve gained enhanced security with key insights to inform better policymaking and architecture, so we can now start publishing policy around data management based on type, sensitivity, and location,” says Baillio. “We can block malicious activity, protect devices, isolate and quarantine the most compromised machines, and safely control sensitive data across all cloud platforms regardless of licensing agreement.”

“Cloudlock gave us visibility about our users and data in the cloud that immediately led us to lock nearly 200 compromised accounts, which was a quick win for UEBA and IT.”

Aaron Baillio
Managing Director, Security Operations and Architecture
University of Oklahoma