CASE STUDY

Nylas quickly protects against the Log4j vulnerability using Lacework

Nylas

Challenges

- Check for critical Log4j vulnerability
- Protect cloud environments and customer data

Solutions

- Scanned thousands of hosts within one hour after Log4j was disclosed
- Monitored for suspicious activity and anomalies while vendors patched their services

Results

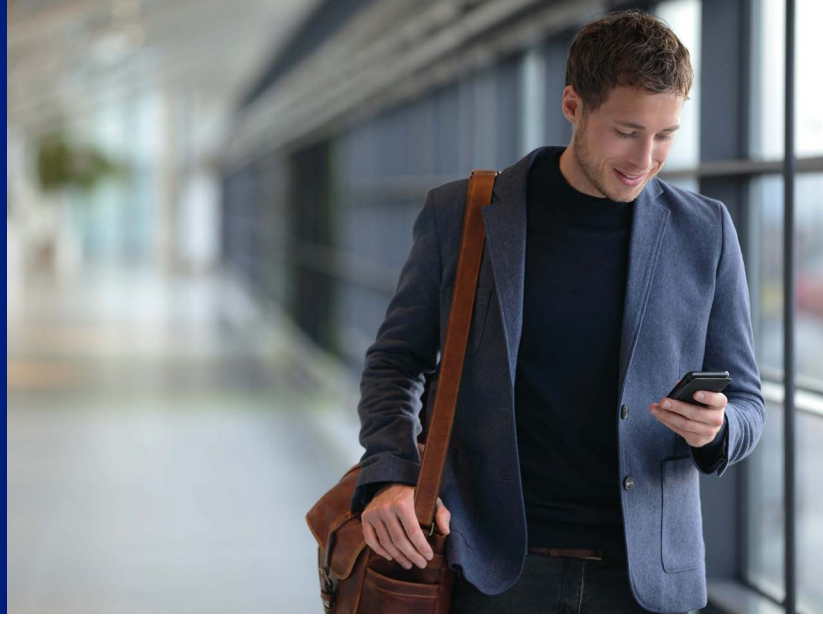
- Confirmed that their exposure to Log4j was limited and quickly relayed that information to customers
- Achieved continuous and complete visibility with event monitoring and anomaly detection

"With the help of Lacework, we rapidly identified instances of the Log4j vulnerability and continuously monitored our environment for any exploitation activity. In less than one hour, we were able to scan our entire cloud infrastructure, including thousands of servers, to assess our exposure to Log4j. We quickly determined that our codebase and our customers were not affected and were able to maintain transparency and open communication with our customers in real-time."

DAVID TING, CHIEF INFORMATION SECURITY OFFICER, NYLAS

> "Lacework allowed us to quickly determine that the library was not present across all of our hosts, which was enormously helpful. It saved us a huge amount of time."

AUSTIN GREGORY, INFORMATION SECURITY ENGINEERING MANAGER, NYLAS



When the Log4j vulnerability (CVE-2021-44228) was first disclosed in December 2021, security teams of all sizes, across all industries, immediately jumped into action. Responding to security incidents is a difficult, dynamic process, but with the right level of visibility across your cloud environment and with a team armed with the right insights, you can more confidently respond. The team at Nylas shares how they leveraged Lacework to handle and quickly respond to the Log4j event.

Nylas is a communications API platform that helps hundreds of thousands of developers around the world quickly and securely build email, scheduling, and work automation features directly into their applications. They have a multicloud environment, operating on both Amazon Web Services (AWS) and Google Cloud, and they use a mixture of containerized and non-containerized services, including Amazon Elastic Compute Cloud (EC2) hosts, Amazon Elastic Kubernetes Service (EKS) clusters, and Google Kubernetes Engine (GKE) clusters. In addition, they employ a number of managed services like Amazon Simple Storage Service (S3) buckets, Amazon Simple Queue Service (SQS), and Google Cloud PubSub.

Austin Gregory, the Information Security Engineering Manager at Nylas, works on functions including incident response and vulnerability and compliance management. At a high level, the InfoSec team is responsible for protecting Nylas's cloud environments and their customer data, so as soon as the Log4j vulnerability was disclosed, Austin's team got down to work.

Scanning for vulnerable systems

After hearing about the Log4j vulnerability, Austin initially felt relieved that Nylas doesn't use Java. But it soon became clear that the problem had a much wider impact. "Because the vulnerability is so easy to exploit remotely, and the exploit code was circling the internet, we quickly became aware that we needed to do a lot more than just check whether Nylas was using Java in our production code," says Austin. "It also mattered whether any of our critical vendors or dependencies were using it too." For instance, even though they don't deploy any Java code on their hosts, the Java virtual machine (JVM) may be present if there's another dependency that requires it.

Luckily, just like Nylas, Lacework was working swiftly behind the scenes to support their customers. Since Lacework scans for Common Vulnerabilities and Exposures (CVEs) on Nylas's hosts, says Austin, "Scanning for instances of the JVM, and specifically the vulnerable library, was incredibly easy because Lacework introduced support for this specific CVE soon after the vulnerability was publicly disclosed." In addition, Austin says, "Lacework allowed us to quickly determine that the library was not present across all of our hosts, which was enormously helpful. It saved us a huge amount of time."

Nylas's InfoSec team also appreciated that Lacework's CVE support didn't require any action on their part. "The Lacework team sent us an email saying that they had added support for the Log4j CVE and our next scans would show this vulnerability as a critical finding if the library was present," Austin recalls. "The very next scan that was run showed that we didn't have the vulnerability."

Continuous monitoring for exploit activity

As with any zero day vulnerability, it's critical to quickly uncover vulnerable systems, but also monitor for active signs of compromise. The Lacework agent turned out to be a key factor in helping Austin's team save time while carrying out necessary security measures. "We already had the Lacework agent deployed on all of our hosts, so we were really happy that Lacework was able to add the support so quickly," says Austin. "Scanning those thousands of hosts would have otherwise taken several days or even weeks, but we were able to do it in an hour with Lacework."

With the scan providing assurance, Austin's team could direct resources to other important tasks. "We were able to shift our attention towards critical vendors, like our subprocessors, to see if we were exposed through them," Austin says. Due to the huge reach of the Log4j vulnerability, some of those vendors were indeed exposed. But while vendors were patching their services, Nylas continued to rely on Lacework to monitor their environment for potential exploit activity. "We were able to use Lacework's event monitoring and anomaly detection to look for any suspicious activity or anomalies that could indicate whether we were compromised, or if there was an attacker trying to access data," says Austin. "Being able to not only detect vulnerabilities, but also watch for exploit activity — and having them constantly running — saved us a lot of stress and allowed us to get a handle on the issue really quickly."

In general, Austin seeks out solutions that give him the most visibility in the least amount of time. "Lacework combines an agentless and agent-based approach to collect data about our environment in the most efficient way possible. The agent allows us to quickly detect when something is wrong because we get constant information right in the Lacework dashboard," says Austin. "If you only rely on a snapshot, you're going to miss important activity and information. We want as much detail as possible to aid in investigations, and Lacework gives us that."

Achieving visibility and compliance

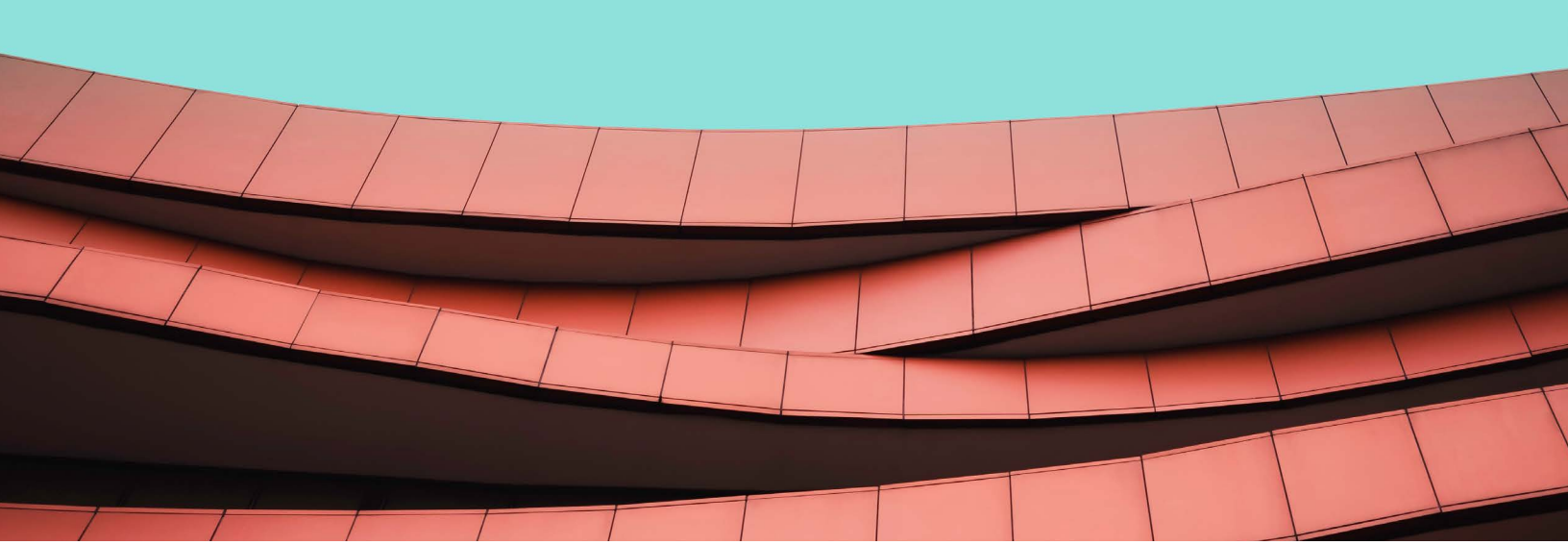
In addition to helping them address concerns around Log4j, Lacework has long been an important part of the security practice at Nylas. Initially, Nylas started using Lacework to get a holistic view of their security posture. With multiple clouds, many different technologies, and the incorporation of Docker and Kubernetes, they needed a solution that worked across both clouds to ensure secure configuration and alert them to unusual activity in the event logs. They found that solution in Lacework.

Lacework has proved to be invaluable for Austin's team due to its unique combination of capabilities that work across Nylas's complex environment. "Lacework continuously monitors for Center for Internet Security (CIS) Benchmark violations, and I consider those benchmarks to be a gold standard when it comes to secure configuration in the cloud," says Austin. "On top of that, it works for both of the clouds that we're using, which is rare." He also appreciates that Lacework can monitor for file integrity, CVE exposure, and any vulnerabilities that are published. Additionally, he says, "It works not only with the virtual machines (VMs) that we have deployed, but also with the Kubernetes clusters. We're able to deploy Lacework across our entire environment and get a comprehensive view of our configuration. The unique anomaly detection from Lacework's Polygraph technology, paired with the CIS functionality, is just incredible. I haven't seen another tool that does it all like that."

While Nylas is compliant with a number of standards, and Lacework helps ensure that the controls they've implemented for those frameworks are being enforced, the CIS functionality that Lacework offers has been a particular advantage. Austin estimates that CIS Benchmark violations have decreased by at least 60% with the use of Lacework. "At its core, what Lacework is really doing is giving us vital information about those CIS Benchmarks," Austin says.

"We were able to use Lacework's event monitoring and anomaly detection to look for any suspicious activity or anomalies that could indicate whether we were compromised, or if there was an attacker trying to access data."

AUSTIN GREGORY,INFORMATION SECURITY ENGINEERING MANAGER, NYLAS



Facilitating communication

Multiple teams at Nylas have benefited from the information that Lacework provides. “As soon as something pops up, we get alerts in our Slack channel,” says Austin. “Then we’re able to look into it and see if it’s something that we need to be concerned about, and decide which team we should relay that information to.” From there, they work to figure out what was changed and why, as well as how to fix it and how to prevent it from occurring in the future. “We’re able to use information from Lacework to talk to the engineering team really quickly after something happens,” Austin says. “That speed really helps. It’s harder to figure out what went wrong when you’re talking about something that happened a week in the past versus something that happened only an hour ago.”

For Nylas, Lacework has been an essential tool to help relay information, quickly and in real time, to their customers. With Log4j, customers almost immediately started reaching out to ask about Nylas’s exposure status and plans to address the vulnerability. “Because of Lacework,” says Austin, “we were able to very quickly tell our customers that our direct exposure was very limited, since we comprehensively scanned our entire environment for instances of Log4j and we don’t have it deployed anywhere.” Not only did they use Lacework to scan their environment, but they could relay that information directly to their customers right away. “The information Lacework provided was super beneficial,” says Austin. “It helped our customers a lot with their peace of mind.” Whether it’s Log4j or whatever comes next, Nylas trusts that Lacework is here to help keep them – and their customers – secure and informed.

Nylas

Nylas is a communications API platform that helps hundreds of thousands of developers around the world quickly and securely build email, scheduling, and work automation features directly into their applications.