LACEWORK

CASE STUDY

Wavefront secures devops environments at scale with Lacework

WAVEFRONT by vmware

Challenges

- Securing an environment that continually changes and where threats and vulnerabilities are difficult to track
- Knowing if there is a zero-day vulnerability in the system

Solutions

- Lacework focuses on changes in behavior as an indicator of a zero-day event
- Lacework is a tool that proves SOC compliance in a dynamic cloud environment

Results

- Improved visibility into the overall security posture at any given time
- Reduced need for domain experts

> "My argument with infosec is always the same. If I take Lacework out, what's the alternative? There isn't one."
>
> MATTHEW ZEIER, SENIOR MANAGER OF TECHNICAL OPERATIONS, VMWARE

The company and its business

Wavefront, a VMware company, is a cloud-based platform for observability and analytics used by developers to view application performance in real time. It is widely used by DevOps teams for resource and performance optimization of cloud native applications and systems. Wavefront is ideally suited for applications that rely on containers and microservices, and it fully integrates with all the technologies in an environment, including those in very large, complex enterprises. With Wavefront, developers and SRES can instantly assess the impact of new code and quickly spot anomalous activity.

The security challenge

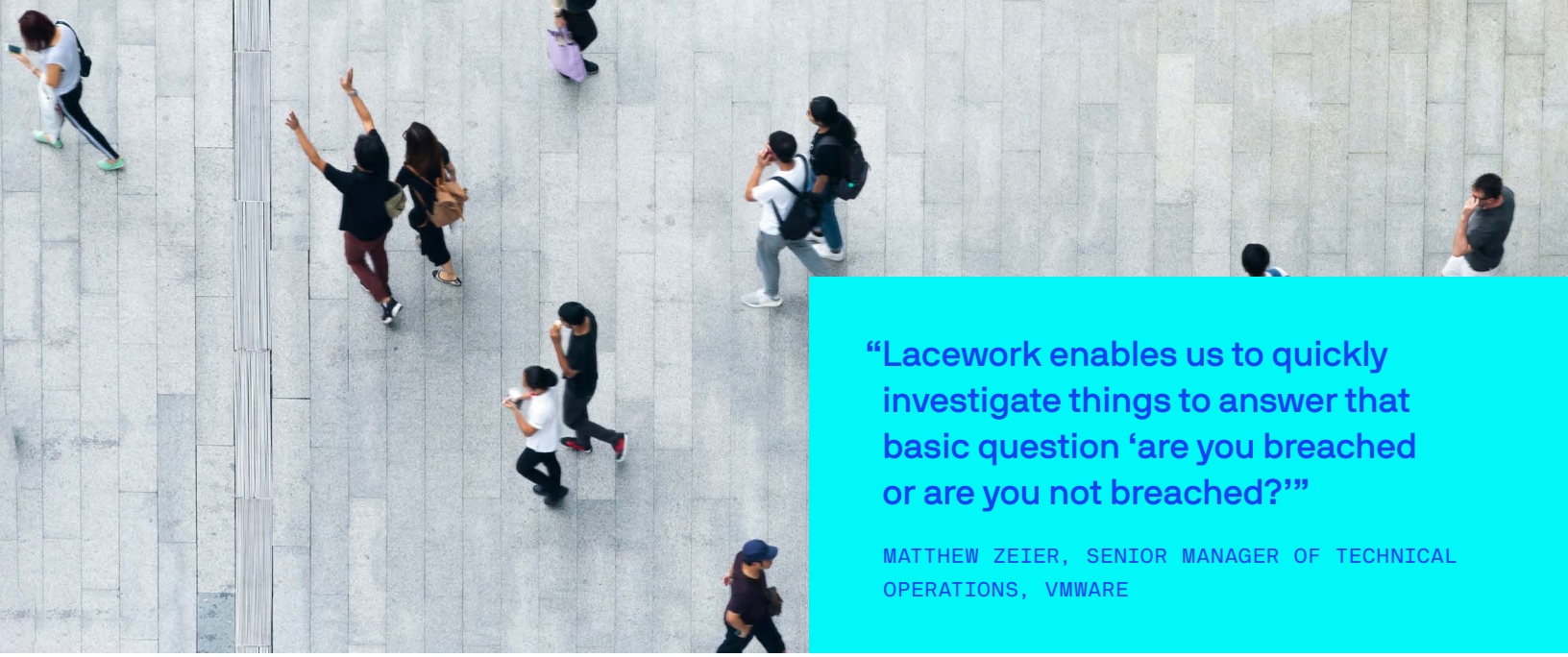
Wavefront operates in the public cloud using containerized services that at any given time support thousands of workloads across tens of thousands of hosts. It is an environment that continually changes and where threats and vulnerabilities are difficult to track. "The problem I must solve," says Matthew Zeier, Senior Manager of Technical Operations at VMware, "is to be able to tell our CEO with some confidence that we're not compromised. I need to know if there is a zero-day vulnerability in my system right now.

Choosing Lacework

In addressing these security challenges, Wavefront began a typical checklist of security solutions handed to them by the corporate information security team. As often happens, their approach is if you're operating in the cloud, you have to do these things which may not sound rational, but you have to do them because they say so. "I pushed back on some of those things, and we compromised," Zeier explains. "They required one solution that sends me a giant CSV file once a month. Fine, except in our environment, after a month most of those issues have disappeared. I can't investigate them anymore."

At an AWS re:Invent conference, Zeier learned about the Lacework approach of focusing on changes in behavior as an indicator of a zero-day event. Lacework continuously searches and provides real time alerts on significant changes. Zeier says, "By and large Lacework doesn't make a judgment call. It just tells me this is different, and then I can go investigate."

Zeier liked that approach. "The next month we signed up with Evident.IO, Threat Stack, and Lacework," he says. "Within three months we stopped using Evident.IO. At the end of the first year, we stopped using Threat Stack. Every year we re-up with Lacework. My argument with infosec is always the same. If I take Lacework out, what's the alternative? There isn't one."



> "Lacework enables us to quickly investigate things to answer that basic question 'are you breached or are you not breached?'"
>
> MATTHEW ZEIER, SENIOR MANAGER OF TECHNICAL OPERATIONS, VMWARE

Greater visibility for everyone

Lacework offers several advantages when it comes to keeping operations secure. For one thing, it enables security teams to quickly investigate unusual events. Zeier explains it in this way: "An application like Tenable is looking at a database of knowns and it's looking at versions or compliance against standards. It doesn't know beyond that. Lacework sees everything. We are aware of any change in behavior, and we can immediately assess a change to see if it's legit or a threat." Lacework also improves visibility into the overall security posture at any given time. "I'm very aware of my security posture, mostly because of the feedback that Lacework gives me." Zeier says. "Once a quarter we go into an operational review with senior management and I'm making the case that they care about availability. They also care about some numeric value that indicates our health and security. I can show that."

Lacework also helps demonstrate compliance. "We leverage the CIS benchmark screen," Zeier explains. "We know our security groups have not been manually changed because we can trace back specific values. Lacework is a tool that's helping prove that we are SOC compliant." On several occasions, that granular visibility into code activity has pinpointed code problems in some of Amazon's own services. But its core capability is answering those critical security questions. Zeier says, "Lacework enables us to quickly investigate things to answer that basic question 'are you breached or are you not breached?'"