GreatHorn

CASE STUDY

DevOps Company Strengthens Security Resilience

"Security-first" mindset drives a cloud email security strategy that includes comprehensive protection before, during, and after an attack.

At-a-Glance

INDUSTRY

Based in San Francisco, the DevOps company enables teams to run and secure cloud-computing infrastructure.

CHALLENGE

Protect employees from targeted phishing without impacting mail flow or business operations.

ENVIRONMENT

> Google G Suite
> Fast-paced business, reliant on email performance
> Distributed workforce across multiple locations
> Cloud-first IT strategy

WHY GREATHORN?

> Simple and fast cloud-based set up and management
> No interruptions to mail delivery
> Simple and effective email remediation capabilities

In 2017, the company was in the early stages of its trajectory and knew that their risk profile would quickly outstrip their ability to manage and mitigate phishing and other email attacks.

Cybercriminals were targeting both the leadership team and junior sales engineers. *"Not only do we receive credential theft and money laundering attacks, we also see tailored messages designed to extract confidential data, often around our customer infrastructure,"* said the senior security engineer. *"While we are an extremely security conscious organization, we needed a way to technically validate the legitimacy of every email message."*

THE SEARCH IS ON FOR A COMPREHENSIVE CLOUD EMAIL SECURITY SOLUTION

After participating in several pilots with email security providers, the security team found that the solutions failed to address targeted attacks. With a heavy reliance on threat intelligence and metadata analysis, the tested email security solutions failed to give the company a holistic view of its email risk profile.

"When you look at just the metadata without looking at the broader context of messaging at the company at large, you're missing a good 20-30 percent of attacks," explained the senior security engineer. He continued, *"Understanding targeted phishing requires you to take a step back and look at how it all connects. For example, the communication patterns and the relationships that are formed when you send and receive messages. By examining these relationships, this is how you can actually distinguish attack patterns."*

A fellow CISO suggested to the company that they look at GreatHorn as a potential solution. Unlike the options he had been evaluating, GreatHorn identified the targeted types of threats the company worried about most, automatically adjusting its analysis based on the company's email interactions both at the macro and the individual level.

CLOUD EMAIL SECURITY THAT OFFERS PROTECTION BEFORE, DURING, AND AFTER AN EMAIL ATTACK

The DevOps company embodies a security-first mindset. They've adopted "safe, sane, and pragmatic" processes that "don't get in the way of employees being able to do their jobs." So, the security team wanted to find a solution that capitalized on the trust and accountability that the company had already instilled in its employees, a way to tap into their inherent knowledge to bolster security.

"We needed a way to prove the legitimacy of any given email message without compromising the privacy of our employees. GreatHorn gave us exactly that. If you like a tool that you don't have to babysit, GreatHorn's an obvious choice. I would strongly recommend GreatHorn. The value is real. It's scalable. GreatHorn will help you move faster, no matter the size of your team."

You can't protect what you don't know. GreatHorn has given us a deep understanding of our risk profile and an incredible level of awareness into our overall security posture.

- The company's senior security engineer

GREATHORN PROVIDES THE COMPANY WITH MULTIPLE LAYERS OF DEFENSE:

1. Proactive threat detection that protects the company from both volumetric and targeted phishing attempts

2. Real-world, in-message warnings to educate and alert employees of suspicious emails

3. Simple, effective, and thorough email remediation capabilities. Security teams can quickly mitigate any malicious messages that may have landed in employee mailboxes

The company's senior security engineer said, *"Most email security solutions rely on a premise of dogmatic, authoritative control that runs counter to our corporate culture. We need to be able to trust our employees and give them accountability to do their jobs and keep the company safe. But they can't do that if they don't have the right information to make good email security decisions."*

"You can't protect what you don't know. GreatHorn has given us a deep understanding of our risk profile and an incredible level of awareness into our overall security posture. We now know what kinds of information our employees are being asked to provide and which users are at the highest risk, and we can tie that back to our business processes and training to reduce risk even further."

Before GreatHorn, the security team had two options when they were experiencing an active email incident: struggle with their native email provider's API to manually find and remove the emails or build a custom script to intercept them.

"We've gone from an initial turnaround time of 48 hours at best to detect and respond to business email compromise to having instant alerts on our phones and desktops, catching the events in near real-time and preventing them from escalating. Using GreatHorn, we can now mitigate phishing attacks in five or so minutes."