GreatHorn

CASE STUDY

Hersha Hospitality Management Closes Email Security Gap

Hotel Management Firm Protects Customer and Employee PII from Phishing Attacks by Automating Email Security and Remediation with GreatHorn

At-a-Glance

HEADQUARTERS

Harrisburg, PA

WEBSITE

www.hhmhospitality.com

INDUSTRY

Travel/Hospitality

CHALLENGE

Protect employees from targeted phishing and other types of malware-based attacks with the least business impact causing email delays or downtime.

ENVIRONMENT

> Fast-paced business, reliant on email performance
> High exposure to PII in general and credit card data in particular
> Distributed workforce across multiple locations
> Cloud-first IT strategy
> Email platform: Google G Suite

WHY GREATHORN?

> Simple and fast cloud-based set up and management
> No interruption to mail delivery
> Ability to more accurately identify and prevent payload-free phishing attacks
> Quick and easy remediation for zero-day attacks

COMPANY OVERVIEW

HHM

Hersha Hospitality Management (HHM), part of the Hersha Group, is a 5,000-person industry-leading hotel management firm that provides turnkey management from accounting services and revenue management to IT services and support for more than 125 hotels and resort complexes across the United States.

SECURITY FOR PII AND PCI COMPLIANCE

Cybercriminals have increasingly targeted the hospitality industry because they handle sensitive data such as personally identifiable information (PII). Many hotel brands have reported large-scale data breaches through a variety of threat vectors such as point-of-sale (POS) exploits, targeted spear phishing, and malware-based attacks.

HHM's Vice President of IT Jason Shane and IT Security Engineer Yoel Alvarez knew they needed to implement a modern cybersecurity strategy that could protect HHM from advanced email threats. Since credit cards are the primary payment method in the hospitality industry, the team is particularly proactive about ensuring compliance with the payment card industry data security standards (PCI DSS). The team conducted an initiative to identify the greatest threat vectors to PCI compliance in the hospitality industry, and found email to be one of the most insecure.

SECURITY AWARENESS TRAINING IS NOT ENOUGH

HHM uses Google's G Suite for business productivity and communications. However, while G Suite provides many advantages, its email security capabilities can't adequately protect against the sophistication of today's targeted phishing attacks.

And yet with the company's geographically dispersed operations, email remains a critical platform for certain types of communication such as new HR policies and procedures, guidance from the executive team to regional managers, business changes and more. In addition, customers often use email to communicate with hotel staff and will provide sensitive credit card information via email. All in all, HHM processes about half a million incoming and intra-organizational emails each week.

"Email is one of the biggest targets for hackers. If just one of these attacks successfully made it through to our finance system, for example, the damage would be huge," explained IT Security Engineer Yoel Alvarez. "We can't afford a single breach."

To minimize that possibility, HHM invested heavily in cybersecurity awareness training to educate employees on what phishing attacks were, how they worked, and how to flag them for remediation. However, across the hospitality industry, employee bases fluctuate pretty significantly.

Describes Alvarez: "We were constantly training. But we knew that not all our employees were giving this the attention it deserved. We needed a tool that could provide an upper layer of defense so that we could protect those users in a different way."

HHM's cloud-first strategy immediately disqualified email security solutions that interrupted mail flow by changing mail routing and MX records. They also wanted to avoid the mail disruption caused by relying on a single point of failure such as a secure email gateway–a point driven home during a proof of concept with a secure email gateway vendor when the system went down and lost email for 45 minutes.

AUTOMATING EMAIL SECURITY

While searching for alternatives, Alvarez found GreatHorn. Architected and built for the cloud, GreatHorn's solution combines advanced threat intelligence and deep relationship analytics to identify both widespread known attacks as well as highly targeted or zero-day attacks.

Because the product sees all email within the organization, it has an evolving understanding of HHM's unique communication patterns, making it much easier to see phishing attacks that have no obvious known malicious threat.

In addition to identifying threats other products can't, GreatHorn also provides HHM's end users with context around emails that are suspicious but don't quite meet the threshold of an obvious threat. For example, if an email references a W2, it might add a banner to the email to remind the user that HHM's business processes don't allow for W2s to be sent via email. That additional warning effectively serves as in-context security awareness training and often provides the necessary context the user needs to reconsider responding with sensitive information.

Shane said, "It's refreshing to work with a vendor that looks at security as a continuous improvement cycle rather than a binary good / bad determination. We can tune the system based on our business processes and risk tolerance, and then GreatHorn automatically optimizes our protection based on our own patterns of communication. This combination makes GreatHorn so much more effective than other options."

The platform uses native cloud email APIs to integrate at the mailbox level (without requiring MX changes), so security teams can quickly and easily remove suspicious emails post delivery if necessary.

Alvarez said, "We needed a robust solution that could protect us from zero-day attacks as well as phishing campaigns that were growing in frequency and sophistication. GreatHorn not only identifies more threats than other products, it also provides us with easy remediation capabilities in the rare event that it misses something. We can conduct a quick search within the console to figure out if an attack is limited or widespread, and then remove all at once from users' inboxes even after they've been delivered."

THE RESULTS

Shane and Alvarez believe that GreatHorn has taken the pressure off of employees to act as a "human firewall" and allows them to communicate with colleagues and clients confidently.

"GreatHorn is obviously just one part of our larger security strategy, but it's a critical one because of how easy email is to abuse," said Shane. "With GreatHorn, we get a multi-layered approach to email security – not just prevention of known threats and targeted phishing attacks, but also in-the-moment user awareness training and incredibly effective remediation tools. As a result, my security team spends less time on email threat management and more time on other critical security areas."

> "
>
> With GreatHorn, my security team spends less time on email threat management and more time on other critical security areas.
>
> Jason Shane, Vice President, IT

Continued Alvarez, "We were one of GreatHorn's first customers because they were the only ones who provided cloud-based answer to phishing. From the beginning, GreatHorn has provided a very unique approach to a tough problem, and they've continued to build on that advantage as they matured the product to the enterprise-class solution it is today. On top of that, the team at GreatHorn is extraordinary. I know from every interaction that they're listening and committed to our success."