Cybersecurity INSIDERS RECOMMENDED

PRODUCT REVIEW

GreatHorn Cloud Email Security Platform

GreatHorn

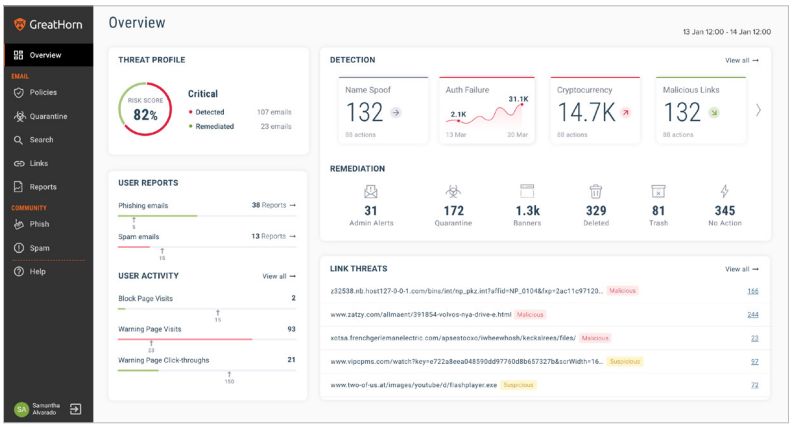
Today, we are reviewing the GreatHorn Cloud Email Security Platform, an email security solution to protect organizations against phishing attacks and advanced communication threats. Phishing attacks have been growing dramatically in the wake of the COVID-19 pandemic and the resulting massive increase in employees working from home.

SOLUTION OVERVIEW

How does GreatHorn address these security risks?

GreatHorn accurately identifies risk areas, threat patterns, and zero-day phishing attacks using a fact-based detection model that combines artificial intelligence and machine learning. This enables organizations to respond to attacks within seconds across the attack kill chain to mitigate the risk of advanced phishing and business email compromise.

Before we dig deeper into GreatHorn's email security platform, let's address the common misconception that existing email infrastructures, such as secure email gateways and the native security controls embedded in email platforms, are sufficient to protect an organization against phishing and other advanced threats.



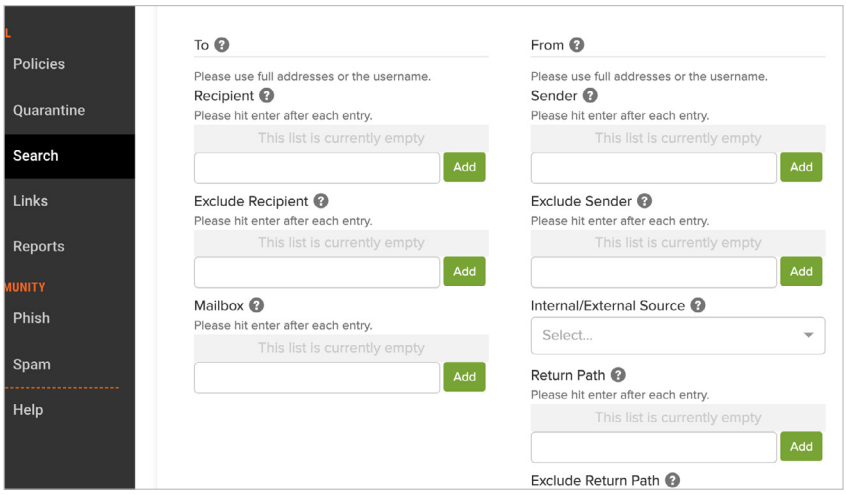
Intuitive dashboard to provide key email health stats

Let's begin with Secure Email Gateways (SEGs). SEGs were built for on-premises email servers, changing the MX records to reroute email (this introduces risk to organizations as SEGs can have intermittent downtime). In addition, SEGs have difficulty identifying advanced phishing attacks as they lack advanced capabilities to look into relationship patterns and other anomalies across the entire email envelope.

Native cloud email security platforms, such as Office 365 and Google Workspace, offer advanced SPAM and email filtering capabilities but lack the advanced threat capabilities to detect and remediate today's sophisticated phishing attacks.

What distinguishes the GreatHorn email solution is the degree to which it leverages machine learning and artificial intelligence. This enables the platform to quickly and automatically learn what the legitimate communication patterns to each sender and recipient look like, and in turn, detect anomalous emails, attachments, and links that deviate from normalcy and typify suspicious emails.

Through this intelligent approach, GreatHorn does not simply focus on "known bad." The platform provides visibility across every threat vector within the email environment allowing organizations to provide the appropriate corresponding layer(s) of security control based on their risk.



Intuitive dashboard email search close up

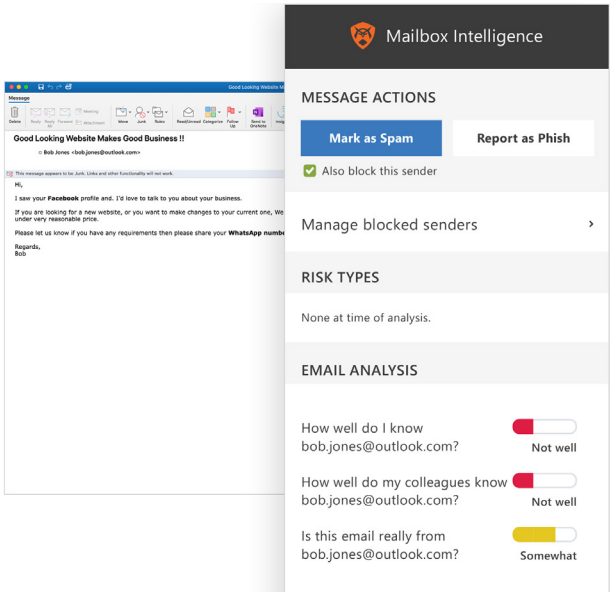
On average, an organization will see 0.8% of all their email as high-risk attacks that should be quarantined. In addition, GreatHorn also provide layers to protect against the medium and low risk (suspicious) emails, including relationship strength, spoofing likelihood, domain name reputation, content analysis, communication patterns, and more. GreatHorn's fact-based policy engine leverages artificial intelligence, data science, machine learning, and community threat intelligence to identify current and emerging risk. This provides clients with a more comprehensive email security protocol to mitigate risk.

GREATHORN CLOUD EMAIL SECURITY PLATFORM BENEFITS

1. **Search and remediate phishing attacks within minutes**
2. **Administer comprehensive policies and controls based on an organization's risk profile**
3. **Provide layered controls, including end-user education to mitigate risks**

GreatHorn also provides robust Account Takeover Protection using biometric authentication to verify employee identities, thereby reducing exposure from any compromised accounts, as well as machine learning techniques to capture an employee's unique typing pattern on both desktop and mobile devices. This feature analyzes the dynamics of an employee's keystrokes, such as speed, pressure, and timing between key press and release. This is the only email security solution on the market to offer this capability.

One of the key factors in protecting email communications is user education. The solution displays customizable banners to contain specific instructions and context to warn employees of a specific email threat. Link protection enables quarantining of links or preview of suspicious link pages, including blocking credential theft sites. A bonus feature called Mailbox Intelligence provides a client-side plug-in that offers employees digestible insights as they interact with emails, using stoplight visibility into any sender and domain trustworthiness, relationship strength, and suspicious link warnings to help users evaluate risk within every email.



GreatHorn Reporter enables easy tagging by users

IMPLEMENTATION, DEPLOYMENT, PROVISIONING, CONFIGURATION, AND MANAGEMENT

GreatHorn provides the email security platform in the cloud with granular API integration into corporate systems. Deployment is a breeze and can be completed typically in less than an hour.

The platform is offered on a subscription basis with an annual term.



Search and remediation video

AWARDS & RECOGNITION

SC Media 2020 Trust Award Finalist
www.greathorn.com/company/press-releases/greathorn-selected-as-sc-media-2020-trust-award-finalist/

ABOUT GREATHORN

GreatHorn safeguards cloud email from advanced threats, (e.g., impersonations, credential theft, malware, and social engineering attacks) by protecting organizations before, during, and after an email attack.

Through its proactive threat detection engine, end-user education, and robust remediation capabilities, GreatHorn frees security teams from time-consuming email security management to enable them to respond to genuine threats faster.



1-800-604-2566
info@greathorn.com
www.greathorn.com

CUSTOMER SATISFACTION

"We've gone from detecting and responding to business email compromise within 48 hours at best, to having instant alerts, able to catch these events in real time. In a recent example, we mitigated a BEC attack within five minutes. We couldn't have done that without GreatHorn."

– Jeff Kohrman, Former Global Security Leader at HashiCorp

"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."

– VP of IT at HHM