GreatHorn

DATA SHEET

GREATHORN EMAIL SECURITY

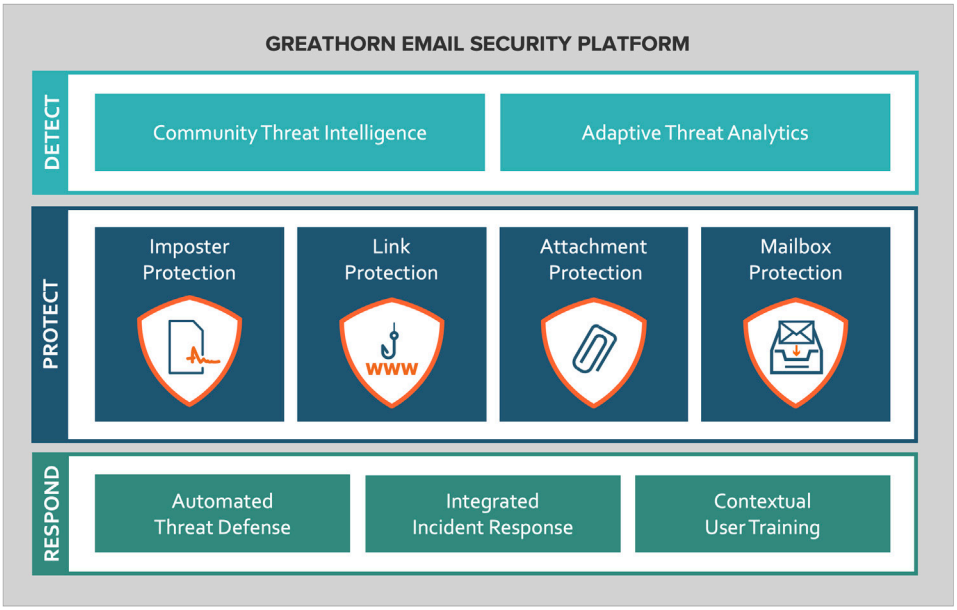
SIMPLIFIED EMAIL PROTECTION — FROM DELIVERY TO DELETION

Executive impersonations and business services spoofing have increased exponentially as criminals see rising success from such sophisticated spear phishing tactics. The result? 1 in 5 security professionals conduct significant remediation actions weekly *despite* the presence of existing email security solutions.

Unlike such legacy tools, GreatHorn Email Security combines adaptive threat detection, automated threat defense, and integrated incident response into a single, comprehensive platform.

Architected specifically for cloud email, GreatHorn naturally adapts to your organization's communication patterns to combat both targeted phishing attacks and widespread threats such as malware and malicious links - all while reducing time spent on day-to-day management and incident response time.

This is enterprise email security - simplified.



KEY BENEFITS

- > Highly effective, tunable threat detection
- > Less time managing quarantine + minimal disruption to business
- > Integrated, rapid incident response and faster time to remediation
- > Reduced risk through in-context user training
- > Improved business process adherence and reduced risk of fraud
- > 5-minute implementation - no gateway to manage, no major DNS changes
- > No interruption to existing email flow - and no risk that email won't be delivered
- > Visibility into both internal & external email

SUPPORTING THE LIFECYCLE OF EMAIL SECURITY

Advanced email threats masquerade as "regular" email - often without attachments or known malicious links, making them difficult for employees to spot. This complexity also means that no email security tool can be 100 percent effective without severely impacting business operations.

That's why GreatHorn supports every stage of the email security lifecycle. GreatHorn detects and eliminates malicious threats upon delivery, provides tools and context for security personnel and end users to evaluate suspicious emails, and makes it easy to remove threats from inboxes at any time.

REQUEST A DEMO

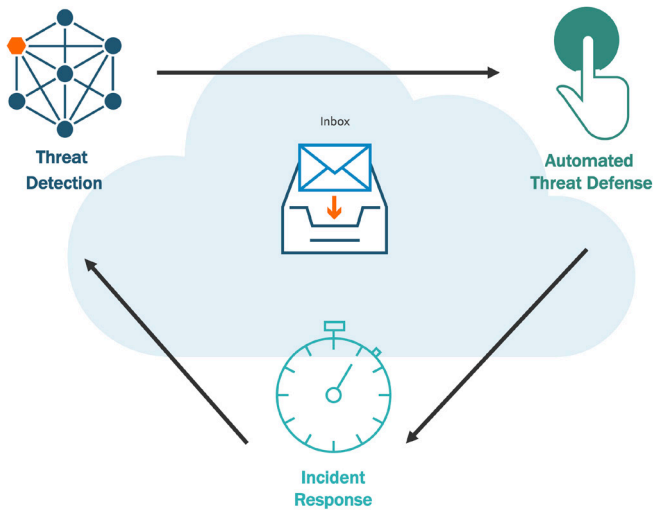
GREATHORN.COM/DEMO

ADAPTIVE THREAT DETECTION

Legacy "one-size-fits-all" email security approaches won't stop targeted threats. GreatHorn combines traditional threat intelligence with both individual- and organization-specific data to more accurately assess risk. By adapting to constantly evolving communication patterns, GreatHorn continuously improves detection of targeted phishing, traditional malware, and fast-moving, emergent threats.

Here are just some of the considerations in our analysis:

- > Deep relationship analytics
- > Advanced spoofing detection to catch impersonations
- > Technical fingerprinting
- > Social fingerprinting
- > Sender reputation
- > Communication pattern analysis
- > Content analysis
- > Threat intelligence



AUTOMATED THREAT DEFENSE

When it comes to threat defense, "blocking" should be ***an*** option—not the ***only*** option. GreatHorn's API connection to Microsoft Office 365 and Google G Suite offers a wide range of threat defense actions that can be adjusted for an organization's risk tolerance and profile - from in-context user training, policy reminders, link rewriting and preview, move to folder, and of course quarantine / delete.

In addition to quarantining high-risk emails and protecting all links both during delivery and at time-of-click, GreatHorn provides users with the context, warnings, and reminders they need to make good decisions about moderate-risk emails. As a result, organizations get better protection without negatively impacting business operations and agility.

INTEGRATED INCIDENT RESPONSE

As threats have increased in sophistication and impact, organizations can no longer afford to rely on a detect / quarantine model that assumes a 100 percent "catch-rate."

By integrating incident response directly into the platform, GreatHorn minimizes exposure time by enabling organizations to quickly, easily, and definitively eliminate threats from end user mailboxes - regardless of when the threat was delivered.

GreatHorn's multi-factor search, forensic analysis, and user reporting makes it easy to understand the scope of threat exposure, as well as eliminate future risk from that threat.

COMPREHENSIVE EMAIL SECURITY. NO EXCEPTIONS.

From time of implementation, our turnkey modules provide immediate protection from today's most dangerous threats. Each module provides out-of-the-box protection using threat-specific detection and defense actions that automatically adapt to your organization over time.

Imposter Protection: Protect against impersonations, look-alike domains, service impersonations, and business email compromise with GreatHorn's advanced impersonation and spoofing detection.

Link Protection: Safeguard employees against credential theft attempts and malicious URLs with fully automated URL sandboxing, administrative tracking, and credential theft threat isolation.

Attachment Protection: Isolate and remove known, emerging, and suspected threats identified through multi-vector email analysis, proprietary community threat intelligence, and industry-leading threat intelligence.

Mailbox Protection: Actively engage end users in email security efforts with a mailbox-level plug-in that enables users to report phish and spam, manage personal block lists, and get access to easy-to-understand risk and link analysis for any given email.

ABOUT GREATHORN

GreatHorn simplifies email security by automating the cycle of email security – through continuous threat detection, defense, and incident response. Office 365 and G Suite customers using GreatHorn not only gain enterprise-class protection against both sophisticated phishing attacks and traditional threats, they also reduce complexity, manual remediation time, and negative impact on business operations.

By combining deep relationship analytics with continuously evolving user and organizational profiling, GreatHorn's cloud-native email security platform provides adaptive, anomaly-based threat detection that secures email from malware, ransomware, executive impersonations, credential theft attempts, business services spoofing, and other attacks. Contact GreatHorn at info@greathorn.com or by visiting greathorn.com.

AICPA Service Organization Control Reports
AICPA
SOC 2
Formerly SAS 70 Reports