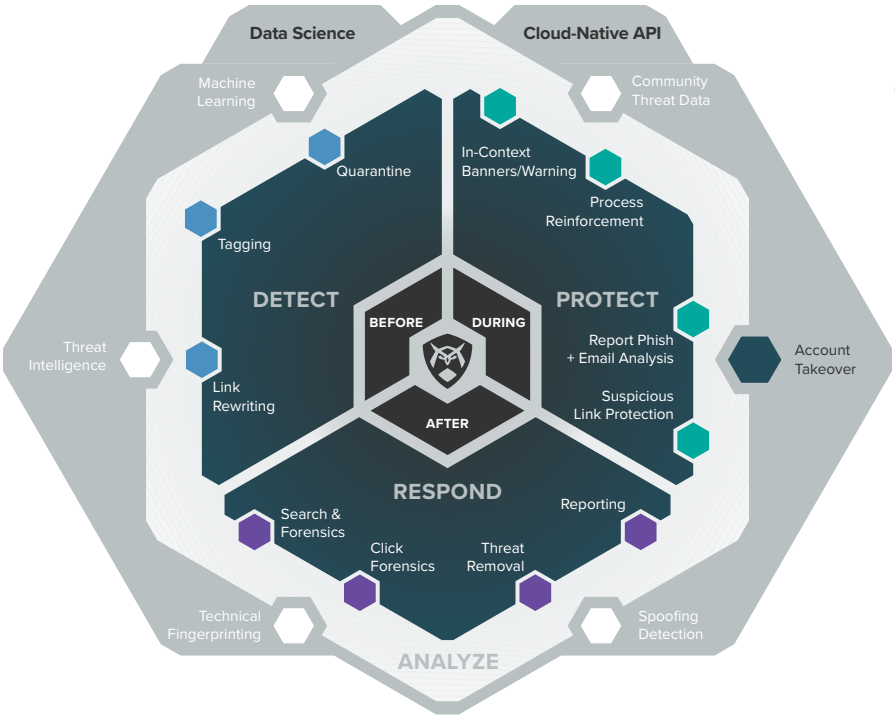


GreatHorn Email Security

Manage risk throughout the email security lifecycle – from threat identification to response

Cloud-Native Platform

Native cloud-email API integration provides visibility, control, and analysis without changes to mail routing or MX records—with just a 5-minute implementation time

Multi-Layered Protection

Multiple layers of defense protect organizations against advanced email threats before, during, and after a phishing attack, providing tools and automation to keep employees safe

Accurate Threat Analysis

A powerful analysis engine combines data science, technical fingerprints, and organization context to identify impersonations, credential theft, and business email compromise attempts

Context-Specific Warnings

In-the-moment alerts, banners, and phish reporting help employees make better decisions, improve business process adherence, and reduce fraud risk

Search & Remediation

Integrated search, forensics, and remediation tools reduce time to response from hours/days to minutes, minimizing threat exposure, and simplifying the response process

Enterprise Controls

Robust management interface enables security teams to customize configuration based on their unique risk profile and tolerance using either the dashboard or 3rd-party security tools

Email security as a risk management function

For decades, email security has relied too heavily on a threat prevention strategy – resulting in slow remediation, continued employee phish engagement, and a game of quarantine catch and release.

With GreatHorn, you'll get protection throughout the email security lifecycle – by identifying and removing more threats, warning users in real-time of potential risks, and quickly remediating attacks from employee mailboxes.

Supporting the email security lifecycle

ANALYZE

GreatHorn's advanced threat analysis engine automatically and continuously analyzes hundreds of data points – through data science, machine learning techniques, technical analysis, as well as threat intelligence and community threat data – to determine the risk of any given email.

As a result, we can more accurately identify more brand and executive impersonations, credential theft, and account takeover attacks.

DETECT

Combined with our analysis engine, GreatHorn's detection capabilities automatically identify, tag, remove, and flag threats – as well as rewrite links for continuous analysis – before users ever see them based on your organization's risk tolerance.

Security teams have the ability to visualize all the different vectors that make up email risk and determine automatically how to treat it – from the quarantine of confirmed threats to visual tags and warnings on suspicious ones.

PROTECT

GreatHorn provides context-specific warnings to employees, enabling security teams to drastically reduce false positives without increasing exposure.

These "in-the-moment" employee engagement tools include dynamic, context-specific warning banners, process reinforcement reminders, previews of suspicious link destinations, email warnings, and a client-side plug-in that not only allows employees to "Report Phish", but also gives them stoplight-level threat analysis of any given email.

GreatHorn gives employees the right context, at the right time, so they can make the right decisions and enhance an organization's security posture.

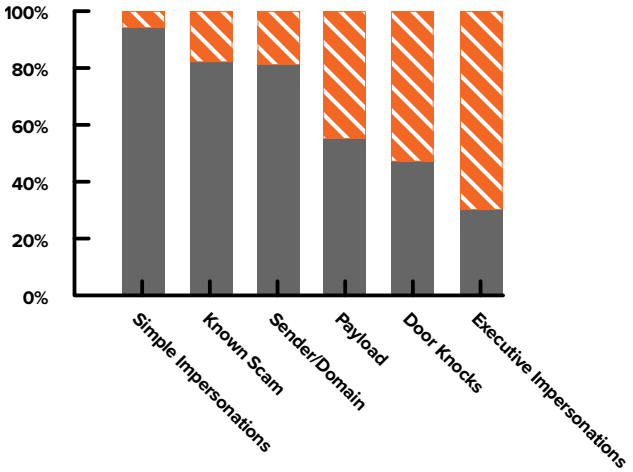
RESPOND

GreatHorn's robust response tools help security teams identify the scope of an attack and remove all incidents of the threat in seconds – no scripting required. Administrators have access to full-click tracking for suspicious and malicious URLs, post-delivery blocking capabilities, and enhanced detection of new threats—even zero-day threats that have not yet been added to real-time blacklists or publicly available antivirus tools.

The result is a platform that automatically protects organizations from advanced email threats and gives them the insight, visibility, and control to stop the damage from business email compromise.

CLOUD-NATIVE ARCHITECTURE

GreatHorn's cloud-native architecture connects directly into cloud email platforms via their API, enabling greater visibility and control, as well as a five-minute deployment to get up and running immediately. Intra-organizational email is analyzed automatically and identically to external email without any special set up. Upon initial deployment, GreatHorn can ingest already delivered mail to identify latent threats sitting in inboxes, as well as calibrate relationship analytics, communication patterns, and technical fingerprints.



3-Month Case Study:
Global 1000 Company Using a Leading Gateway

Threats identified by both Gateway and GreatHorn

Threats identified by GreatHorn, but missed by Gateway