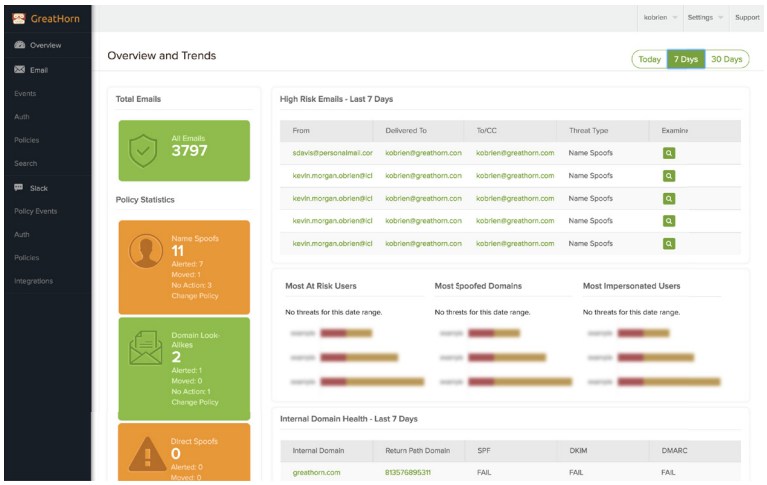
## Communicate confidently.

90% of breaches begin with a targeted email attack, and business email compromise attacks have caused $3.1B in damages since 2014. Cloud providers and legacy tools will not detect or stop these advanced social engineering attacks.

GreatHorn's Inbound Email Security platform is the leading cloud-native, fully automated solution for detecting and preventing these threats from tricking users and damaging organizations.

GreatHorn allows enterprises to securely communicate via Google Apps, Office 365, and other cloud communication platforms by detecting and stopping the social engineering threats that legacy tools miss.

Unlike perimeter-based tools, cumbersome training, or difficult-to-manage gateways, GreatHorn provides automatic feedback and response to these attacks, including business email compromise, CEO spoofing, fraudulent wire transfers, PII and IP theft, and other forms of deceptive message-based threat.




"GreatHorn's cloud-based email analytics suite gives us the insights we need to identify and mitigate threats to our employees and enterprise, and are essential to our overall security approach."

*-Nick Vigier, Director of Security, DigitalOcean*

---

### Cloud-Native

GreatHorn is natively integrated with the world's most popular cloud email platforms - including Google Apps and Office 365 - and provides seamless protection across all devices, clients, and networks.

### Rapid Deployment

Deploying GreatHorn takes 15 minutes, and doesn't compromise your organization's existing security and compliance programs by requiring you to change MX records or BCC / copy mail to an untrusted server. You'll start seeing data within minutes of deployment.

### Fully Automated

GreatHorn's unique Policy Engine allows you to identify and remediate potential threats 24/7, 365 days a year, instantly removing threats from user mailboxes and alerting security staff, and is compatible with Secure Email Gateways - no additional technology required.

### Continuous Protection

With hundreds of millions of emails analyzed every week, the breadth and scope of data with which GreatHorn detects threats and removes false positives is unmatched; insights across the GreatHorn Data Cloud continuously increase threat intelligence.

GreatHorn

# Inbound Email Security

| | SEG | Mail Auth Tools | Plugin Tools | GreatHorn |
|---|---|---|---|---|
| **PLATFORM** | | | | |
| Continuous monitoring over all email at the mailbox level | ◑ | ○ | ○ | ● |
| No performance/delivery risk | ○ | ○ | ● | ● |
| No MX changes required | ○ | ○ | ◑ | ● |
| Cloud-native Google Apps / Office 365 support | ◑ | ◑ | ◑ | ● |
| Painless deployment (<1 hour) | ○ | ○ | ○ | ● |
| Full data privacy support (no risk of exposure via vendor) | ○ | ○ | ● | ● |
| No user behavior changes required | ○ | ● | ○ | ● |
| No mail client plugins required | ● | ● | ○ | ● |
| Agentless deployment | ◑ | ◑ | ○ | ● |
| Integration with IT workflow tools | ● | ◑ | ● | ● |
| **DETECTION** | | | | |
| String-based DLP | ● | ○ | ○ | ● |
| RegEx-based DLP | ● | ○ | ○ | ● |
| Automated Display Name Spoof threat detection | ◑ | ○ | ○ | ● |
| Automated Domain Lookalike threat detection | ◑ | ◑ | ○ | ● |
| Automated Header Manipulation / Direct Spoof threat detection | ◑ | ◑ | ○ | ● |
| Automated Suspicious Link threat detection | ● | ○ | ◑ | ● |
| Attachment Analysis | ● | ○ | ◑ | ● |
| SPF authentication analysis across ALL received mail | ● | ● | ○ | ● |
| DKIM authentication analysis across ALL received mail | ● | ● | ○ | ● |
| DMARC authentication analysis across ALL received mail | ◑ | ● | ○ | ● |
| Automation fingerprinting and metadata threat detection built on global intelligence | ◑ | ◑ | ○ | ● |
| Emergent threat detection – authentication metadata changes | ○ | ○ | ○ | ● |
| Automated threat correlation across industries / market segments | ○ | ○ | ○ | ● |
| **RESPONSE** | | | | |
| Customizable action framework | ◑ | ○ | ○ | ● |
| Preset policies based on common patterns | ◑ | ○ | ○ | ● |
| Comprehensive risk remediation actions | ○ | ○ | ○ | ● |
| Folder/Label/Category-based control, post-delivery | ○ | ○ | ○ | ● |
| In-email warnings (banners) alerting users to potential risks | ○ | ○ | ○ | ● |
| In-email warnings (banners) alerting users to policy violations | ○ | ○ | ○ | ● |
| Out-of-band email notifications alerting users to received threats | ○ | ○ | ○ | ● |
| Algorithmic tuning based on user behavior and response | ○ | ○ | ○ | ● |
| End-user alerting compatible with all mail clients, including mobile | ○ | ○ | ○ | ● |