THE CLOUD EMAIL SECURITY CHALLENGE:

CLOSING THE CYBERSECURITY SKILLS GAP THROUGH AUTOMATION

Email remains at the heart of the business communications landscape.

While nobody loves using it — see employees exchanging quips on their fruitless efforts to reach "Inbox Zero" and media headlines heralding newer, trendier apps as "email-killers" — email is still the most common form of communication in the business world. A recent study predicts that over one third of the population (or slightly more than 2.9 billion people!) will be using email by the end of 2019.

Given its integral role in the business world, it comes as no surprise that the adoption rate of email security technology is nearly 100%. Despite this universal investment in securing email, however, breaches are still occurring — and at increasing rates.

An FBI Public Safety Announcement issued on May 4, 2017 outlines the scope of the problem:

"The BEC/EAC scam continues to grow, evolve, and target small, medium, and large businesses. Between January 2015 and December 2016, there was a 2,370% increase in identified exposed losses. The scam has been reported in all 50 states and in 131 countries. Victim complaints filed with the IC3 and financial sources indicate fraudulent transfers have been sent to 103 countries."

Why Can't We Stop Getting Owned?

Increasingly sophisticated attacks are bypassing legacy email security tools.

Targeted phishing has become the single most effective attack type in the world today, and attackers' emphasis on social engineering tactics make the protection of cloud communication platforms a critical component of any cybersecurity strategy.

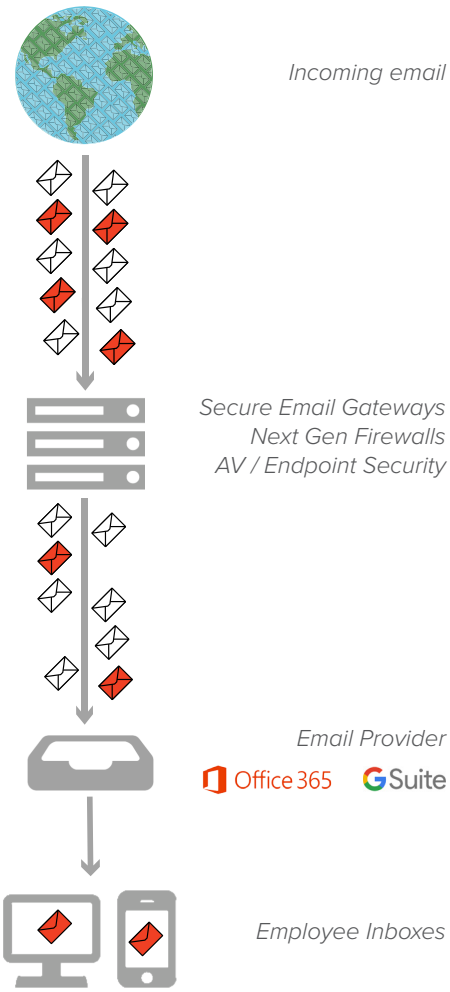
However, communications security at scale is complicated by hybridized cloud adoption and the integration of customized workload integrations with public SaaS communication platforms — Microsoft Office 365 and Google Apps (now G Suite) dominate this space in the email channel.

Legacy security vendors, historically focused on on-premise technology and point solutions for email, have struggled to adapt to these newer platforms. Single-point-in-time efforts to block threats at the perimeter through the use of a Secure Email Gateway are clearly insufficient, and offer no visibility, control, or protection against messages that have bypassed the SEG. In order to successfully protect the organization against highly targeted social engineering attacks, IT and Security teams must gain post-delivery visibility into, and control over, messages that have already landed in employee inboxes.

Employee training efforts aren't good enough to stop modern attacks.

Major data breaches are front-page news on an almost daily basis, and every employee understands that hackers are a real, persistent threat. However, cybersecurity trainings are typified by ill-attempted compliance tick-box initiatives that largely waste time and resources.

Depending solely on a perimeter-based email security strategy leaves organizations vulnerable to attacks that sucessfully bypass those controls.



The pervasiveness of email, the proliferation of self-owned devices, and the always-on-nature of modern work makes it impossible for people to be constantly vigilant. There's no way to transform people into hard targets for hackers; they're all soft.

The key to stopping targeted phishing attacks is not "more tools," but rather a shift in mindset. Bolstering detection capabilities is more effective when coupled with automated response capabilities and preventive controls that inform and guide behaviour, rather than prohibit users from working. For the average end-user, security should be front and center — but only when security is relevant.

Security teams can't detect, analyze, and respond to literally every suspicious email their organizations receive.

Enterprise IT and information security teams almost always find themselves pushing against resource limitations in the face of unending attacks and increasingly sophisticated criminals — but a deficit of qualified workers often referred to as the "cybersecurity skills gap" leaves many organizations unable to find and hire the people they need in a timely fashion (if at all).

This shortage of qualified professionals leads to a critical lack of visibility. Attackers often compromise an organization in just minutes, and exfiltrate data in a matter of days; increasingly, organizations don't know that they've been breached until they're notified by a third party. Security teams must spend their time understanding and preventing threats categorically, rather than being buried in the noise of day-to-day alerts. As information security and IT staff shifts to become a more analytical role, the ability to narrow the time between incident and remediation is key to preventing a major financial or data loss event.

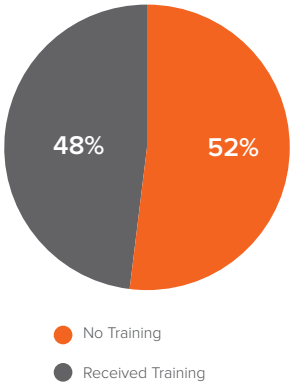
Automation is the only way to keep up.

Automation reduces the workload on IT and Security teams by programmatically identifying and addressing threats based on preset policies. Leveraging machine learning and automation can:

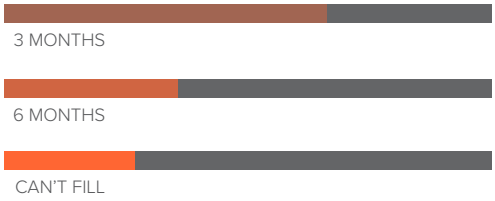
- Increase visibility of threats
- Reduce time to detect / respond
- Increase accuracy and detect patterns that humans might miss

By using automated data science techniques to assess trust during users' interaction within these platforms – rather than attempting to block malicious attacks at the perimeter – GreatHorn has established a modern, autonomic, confidence-enabling model for businesses that have or will shortly embrace cloud technologies for their core business applications.

Among all tracked breaches in 2015, the statistical difference between organizations who received training and those who didn't was only 4%.

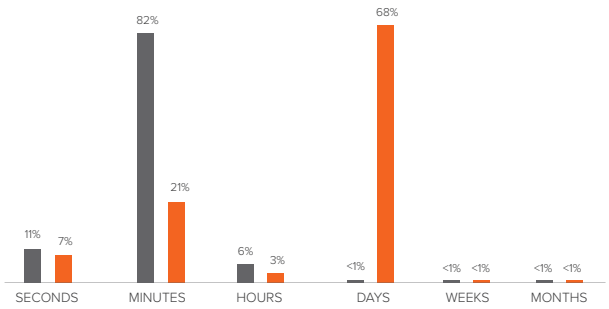


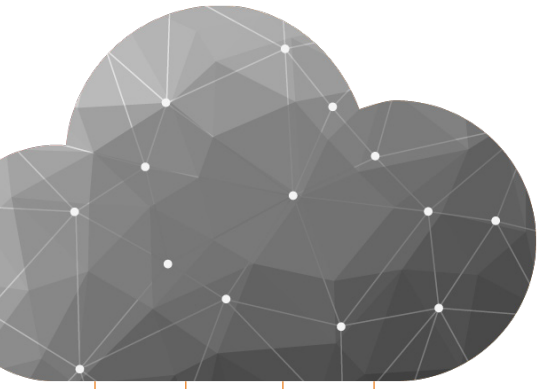
55% of security positions take at least three months to fill; 32% take six months or more, and over a quarter of all US-based enterprises can't fill their open positions at all.



Time is of the essence: often, attackers compromise an organization's defenses in minutes and exfiltrate data in just days.

TIME TO **COMPROMISE** AND **EXFILTRATION**





GreatHorn's Inbound Email Security platform detects and stops targeted phishing and social engineering attacks that operate by exploiting user trust.

GreatHorn's automated policy-driven engine leverages machine learning to analyze a growing data set comprised of millions of analyzed emails and over 3.5 terabytes of enterprise mailbox data. By natively integrating with cloud email providers like Google and Office 365, the platform is able to perform realtime analysis of message authenticity, based on both authentication data such as SPF, DKIM, and DMARC as well as contextual analysis of mail transmission pathways, sender IPs, domain "look-alike" attack vectors, and indicators of message or domain spoofing.

With hundreds of millions of emails analyzed every week, the breadth and scope of data with which GreatHorn detects threats enables our customers to benefit from the early identification of emerging attack trends, and increases threat intelligence over time.

114,545 MAILBOXES UNDER PROTECTION

373,803,448 UNIQUE EMAILS ANALYZED

231,800 THREATS REMEDIATED BY POLICY SINCE APRIL 2016

3.5TB OF DATA IN THE GDC

We analyzed a subset of GreatHorn customer data to build a risk profile based on what percentage of inbound mail can be expected to bear certain threat characteristics.

Threat Type	% of Received Mail
Direct Spoof	0.006
Display Name Spoof	0.002
Domain Lookalike	0.001
Keywords: - W2 - Wire Transfer	 0.001 0.001
Authentication Risks	0.005
TOTAL	**0.016%**

Using the numbers above, we can build a risk profile for, let's say, a Fortune 500 organization with 50,000 full time employees. Since the average office worker receives 460 emails / week*, that's a **threat surface of 23,000,000 emails**.

Regardless of how these threats were discovered — whether employees reported them to IT, or a Secure Email Gateway flagged them at the perimeter and alerted an admin, or if the company is running GreatHorn and the platform detected it at the moment it arrived — an estimated 0.016% of those 23,000,000 emails will bear some threat characteristics that will require review, investigation, and (if applicable), remediation.

That's **3,680 emails in a week.**

It takes a security admin **5 minutes, on average, to review an event**. Some events will be reviewed in a bit less time than that, but others will take much longer, especially if they require input from other departments / stakeholders.

The table below shows how much time this organization's security team would have to spend reviewing the threats that GreatHorn *automatically* analyzes and takes action on in a single week:

Threat Type	Number of Threats / Week	Estimated Investigation Time Without GH	Policy Action Taken (Immediate)
Direct Spoof	1,380	115 hours / ~5 days	• Quarantine message • Alert intended recipient
Display Name Spoof	460	38 hours / ~1.5 days	• Move message to "Possible Phishing" folder • Alert admin • Alert intended recipient
Domain Lookalike	230	19 hours	
Keywords: - W2 - Wire Transfer	230 230	19 hours 19 hours	• Add warning banner to message • Trigger end user training workflow
Authentication Risks	1,150	95 hours / ~4 days	• Alert admin
TOTAL	**3,680**	**305 hours / 12+ days**	

Integrated Threat Intelligence

Many suspicious messages can be detected and remediated automatically, but some will still require review by a security analyst. Understanding whether a specific message is an attack requires fully integrated threat intelligence, with significant amounts of data to identify threat patterns and help inform incident response actions.

GreatHorn's threat intelligence arms investigators with data that can't be seen in house, driving down time-to-detection and increasing efficiency; insights across the GreatHorn Data Cloud continuously increase with intelligence on both emergent and historical threats.

GreatHorn analyzes the relationships between the following data points and provides in situ threat intel directly within the platform:

- From: address
- From: domain
- Display name
- Reply-to address
- Return path
- IP address
- SPF / DKIM / DMARC
- Sender's historical relationship with the recipient
- Sender's historical relationship with the organization

The bottom line: even if you don't experience a large-scale breach, targeted phishing is still costing you — in money as well as time, resources, and risk.

GreatHorn reduces your workload for investigating phishing by 61 hours a week, which is the equivalent of 7 additional FTEs in IT / Security (if you were to hire employees dedicated solely to analyzing message-based threats).

In addition to saving time and enabling better allocation of human capital, leveraging automation and machine learning in security provides increased accuracy and detection capabilities.

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 Post-Delivery 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.

We are headquartered in Belmont, Massachusetts. To learn more and begin a 7-day trial of Inbound Email Security, please get in touch:

www.greathorn.com

info@greathorn.com

800-604-2566