TECHSTARS **CASE STUDY**

techstars

Industry: Venture Capital

Website: techstars.com

ABOUT TECHSTARS

Techstars is one of the world's respected and effective startup accelerator programs, making entrepreneurship accessible by opening doors to capital, mentorship, marketing, business development, customer acquisition, and talent recruitment for some of the world's fastest growing and most exciting startups and entrepreneurs.

THE CHALLENGE

Working with thousands of the world's most promising startups, especially as they seek to raise capital from both angel investors and venture capital firms, brings with it a challenge: protecting against fraud in an organization where requests for wire transfer details and sensitive financial information are ingrained in the business.

"We've seen the sophistication of attacks grow over the course of the past few years, which reflects a broader trend: the bad guys are getting smarter about how they go after their targets, and like many organizations that regularly work with investors and entrepreneurs, we're a target," notes Jed Christiansen, who heads up all of Techstars' core IT systems.

"As a Google Apps client, we know that we have a tremendous amount of platform-level security from Google directly, but also that we have a shared responsibility for protecting against fraud that relies on deception of our users, and that's especially challenging given that the roster of companies and individuals with whom we communicate changes so rapidly."

"Spend time in a Techstars office, and you'll likely hear someone say, "Do More Faster" – one of our favorite phrases. GreatHorn's fully automated policy engine keeps us secure while allowing us to focus on delivering value to our companies, entrepreneurs, and communities."

– Jed Christiansen

Director of Technology

THE SOLUTION

GreatHorn was brought online for Techstars in 2015, and its ability to detect one of the most sophisticated types of inbound email attack was quickly put to the test.

"While we were still in a proof-of-concept phase, one of our senior executives' email was spoofed via a look-alike domain – the criminals knew how to write a convincing email, and they set up a clone of techstars.com, but with a single character changed in the domain name," Jed explained. "GreatHorn's unique ability to detect these kinds of attacks was both the first and remains the most accurate system for stopping this kind of threat before it leads to an embarrassing situation. Combined with their security automation, user behavior analysis, and detailed forensics, their system has significantly reduced our risk profile."

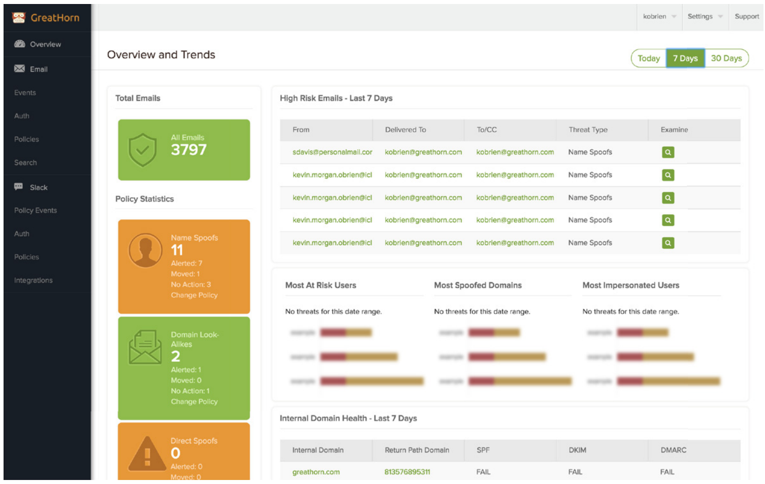
COMMUNICATE CONFIDENTLY

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.



Overview and Trends

Total Emails

All Emails 3797

Policy Statistics

Name Spoofs 11
Alerted: 7
Moved: 1
No Action: 3
Change Policy

Domain Look-Alikes 2
Alerted: 1
Moved: 0
No Action: 1
Change Policy

Direct Spoofs 0
Alerted: 0
Moved: 0

High Risk Emails - Last 7 Days

From	Delivered To	To/CC	Threat Type	Examine
sdavis@personalmail.cor	kobrien@greathorn.com	kobrien@greathorn.com	Name Spoofs	🔍
kevin.morgan.obrien@icl	kobrien@greathorn.com	kobrien@greathorn.com	Name Spoofs	🔍
kevin.morgan.obrien@icl	kobrien@greathorn.com	kobrien@greathorn.com	Name Spoofs	🔍
kevin.morgan.obrien@icl	kobrien@greathorn.com	kobrien@greathorn.com	Name Spoofs	🔍
kevin.morgan.obrien@icl	kobrien@greathorn.com	kobrien@greathorn.com	Name Spoofs	🔍

Most At Risk Users

No threats for this date range.

Most Spoofed Domains

No threats for this date range.

Most Impersonated Users

No threats for this date range.

Internal Domain Health - Last 7 Days

Internal Domain	Return Path Domain	SPF	DKIM	DMARC
greathorn.com	813576895311	FAIL	FAIL	FAIL

> "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.