charity: water

Industry: Nonprofit
Website: charitywater.org

ABOUT CHARITY: WATER

charity: water is dedicated to solving the water crisis in their lifetime. 100% of their public donations go directly to funding clean water projects around the world. Their work provides rural communities with access to clean water, and in doing so, dramatically improves education, income and health for the people they serve.

THE CHALLENGE

The charity: water team understands the challenge - and importance - of keeping their valuable information secure: information about their team is largely public, they deal with financial transactions on a daily basis, and they are globally distributed, with team members around the world.

"Safeguarding our team against spear phishing attacks and email fraud means being able to focus our time on our work to help change lives, especially those of women and children in rural communities. We've been on the receiving end of attempted cyberattacks, and it's incredibly important to us that we both protect our data and resources as well as not let these criminals reduce our efficiency or get in the way of our work," notes Sabrina Pourmand, Vice President of Key Relationships for the nonprofit.

"We devote 100% of public donations to communities in need. Our reputation, our work, our partners and ultimately our supporters rely on us. GreatHorn is a critical part of our cybersecurity infrastructure, because they help us operate safely and efficiently without falling victim to inbound communication fraud."

– Sabrina Pourmand

Vice President of Key Relationships

THE SOLUTION

GreatHorn's cloud-native approach to detecting inbound threats - disrupting them through their fully automated policy-driven remediation engine, and defending the entire team from threats 24/7/365 - was easy to implement and quickly became a valuable tool for the charity: water team.

Ian Cook, Head of IT for the nonprofit, pointed to this ease of deployment when describing their experience. "GreatHorn was up and running for us in minutes. They've built a truly powerful security system that's integrated at the platform level, and with their Policy Engine, we can filter through the noise and find exactly what threats we receive, from impersonation attempts to suspicious attempts to execute wire transfers, in real time and without interrupting our typical mail flow. Having a complete solution, rather than piecing one together from multiple systems, made the process of protecting charity: water a straightforward one."

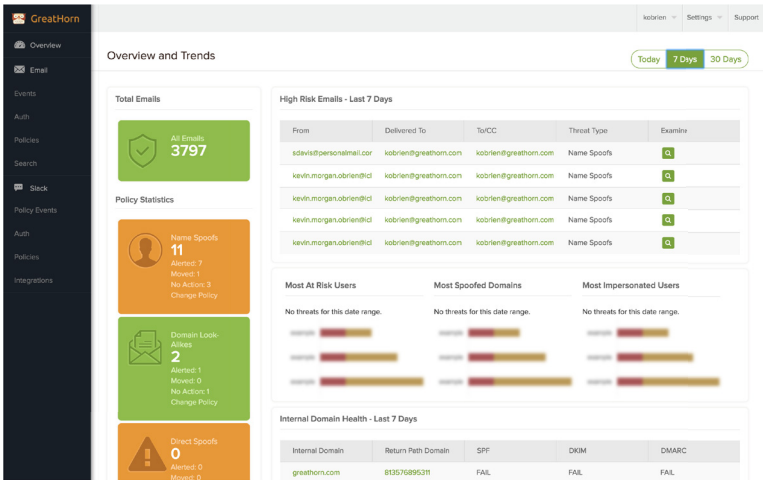
COMMUNICATE CONFIDENTLY

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.