GreatHorn

GreatHorn Case Study

# Rigid Bits Leverages GreatHorn for Email Security That Helps the Client Work

## AT-A-GLANCE

### Company

Rigid Bits LLC
Longmont, CO

### Website

www.rigidbits.com

### Industry

Cybersecurity Consulting

### Challenge

Find an email security solution that Rigid Bits can both use for itself and recommend, that won't impede client business

### Environment

Clients of Rigid Bits use both Microsoft 365 and Google Workspace

### Why GreatHorn?

- Security tools that empower Rigid Bits clients to take action on their own, without relying on Rigid Bits
- Warnings on suspicious emails that educate and protect at the same time
- Efficient remediation of threatening emails
- Early awareness in business email compromise situations
- Easy implementation that is seamless for end users

Rigid Bits, a cybersecurity consulting firm, wanted an email security provider it could use to protect its own systems and users, and also recommend to clients as an integrated part of the cybersecurity solutions it designs for them.

## Rule #1: Empower the Client

Rigid Bits' highest priority in selecting an email security provider was not to get in the way of clients' businesses. Rigid Bits is not an IT service provider. They wanted to empower clients to take action on their own, without relying on Rigid Bits.

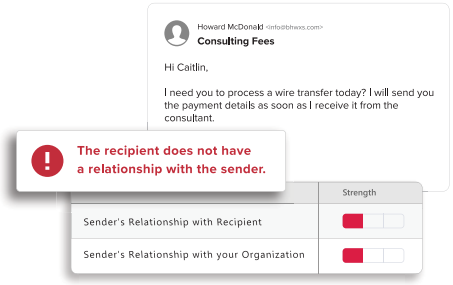
With GreatHorn, Rigid Bits is recommending email security that puts full access into the clients' own hands. The client's own admins have the ability to change policies, remediate threatening messages and review, retrieve and gain insight into filtered messages.

*"GreatHorn gives us a way to empower our clients to take action on email based threats, allowing us to maintain an advisory role as cybersecurity consultants, since we are not IT service providers. We're able to still give people tools to help secure the email attack vector,"* said Ryan Smith, Director of Sales and Customer Success at Rigid Bits. *"We're not touching anything that could impede their ability to work efficiently."*

## Better Filtering and Insights

Right away, Rigid Bits clients found that GreatHorn was providing better email security, over providers they had used in the past. GreatHorn was simply catching things other email security providers weren't.

If a phishing email made it through to users, GreatHorn also stood out in its ability to provide insight into the extent to which users had interacted with the threatening message. Clients told Rigid Bits they had better peace of mind from being able to see exactly who had clicked on what. The knowledge enabled them to remediate efficiently and effectively, without having to worry about threats and exposure that they might have missed.




*"GreatHorn gives us a way to empower our clients to take action on email based threats, allowing us to maintain an advisory role as cybersecurity consultants, since we are not IT service providers."*

– Ryan Smith,
Director of Sales and
Customer Success

*"Most people I talk to are having some kind of clunky, really inefficient way to remediate phishing emails,"* Smith said. *"Just the ability to know that, if they find a malicious email, they can remove it from everyone's inbox with just a few clicks, that's huge to them. Before, a lot of our clients were just hoping people wouldn't see those emails."*

Thorough insight into what was happening with each phishing email has also allowed Rigid Bits' clients to demonstrate the ROI of the GreatHorn solution, by showing leadership exactly what their email security tools are catching and preventing.

## Visibility Into Business Email Compromise

GreatHorn's ability to provide insight into threatening emails has given Rigid Bits' clients early warning when a business email compromise has occurred.

Often, the goal of a phishing campaign targeting an organization isn't necessarily about gaining direct access to sensitive systems. Takeover of an employee account can provide a foothold for cybercriminals seeking access, or looking to accomplish other objectives, like fraud and extortion. Often, it's a way for a criminal to impersonate a trusted sender, thereby infiltrating firms and individuals in the initial victim's address book.

When a user's email is compromised, by whatever means, GreatHorn is able to identify the change in emailing behavior and flag it as suspicious for administrators. That early warning has helped Rigid Bits' clients stop damage from spreading to their own clients and partners.

*"Before, someone suffering a Business Email Compromise (or BEC) would have to wait until someone was nice enough to email them to let them know they got hacked. GreatHorn can actually tell them,"* Smith said. *"Having a way to be more proactive in detecting a BEC resonates with the people we work with, because of the nature of their businesses and because they are worried about their reputations and can now take action more quickly."*