GreatHorn

GreatHorn Case Study

Early Growth Leaps Past Email Security Problems with GreatHorn

At a firm serving Silicon Valley businesses, there isn't time for unnecessary complexity in email security.

AT-A-GLANCE

Company

Early Growth Financial Services, Palo Alto, CA

Website

www.earlygrowthfinancialservices.com

Industry

Small and Midsize Business Services

Challenge

Quarantine phishing and spoofing attacks; cut down on admins' time reviewing and remediating suspicious messages

Environment

- Google Workspace
- Remote workforce
- High volume of phishing and spoofing attacks
- Limited IT team bandwidth
- 100+ employees
- 300+ clients

Why GreatHorn?

- Easy implementation: no changing of mail exchanger (MX) records required
- Seamless integration with Google Workspace
- Ease-of-use for admins: an intuitive dashboard that made adoption a no-brainer
- Automatic quarantine, eliminating "the human factor"
- Fast, simple review and remediation

Early Growth Financial Services (Early Growth) is an outsourced financial services firm that provides financial support to small and mid-sized businesses. Headquartered in the Bay Area, Early Growth has over 300 clients across the United States. In 2013, it was ranked No. 5 in the Silicon Valley Business Journal's list of the Fastest Growing Private Companies.

Email Security Challenges

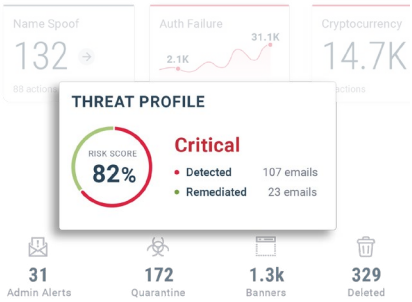
Early Growth Financial Services (Early Growth) used Google Workspace as their cloud-native email platform. The security team at Early Growth had built internal workflows to assist in the manual delivery of user-reporting phish for the team to log into the Google Workspace interface and individually block domains and email addresses. However, users were reporting suspicious emails at a rate of two emails per employee per day. With hundreds of suspicious messages reported per day, the process became too cumbersome to manage.

In addition, some well-intentioned users were still responding to malicious emails, despite employee security training efforts. The most potentially damaging attacks were spoofing emails impersonating the company's CEO, asking for wire transfers and gift cards. Security personnel were manually blocking domains and senders, a cumbersome process fraught with the knowledge that the next round of attacks might elude those filters and do damage to the company, its employees or its clients.

"Our CFO and I were looking at solutions and we knew there had to be a way to fix this," said Stephanie McCain, Director of Human Resources at Early Growth. *"We stumbled onto GreatHorn and it was everything we were looking for."*

"Rather than spending hours blocking these bad emails, with GreatHorn it's as easy as logging into the administrator panel and selecting to delete, approve or deny the emails."

– Stephanie McCain,
Director of Human Resources



"GreatHorn is a product that is easy to use and easy to understand ... I trust it completely."

– Stephanie McCain,
Director of Human Resources

Review of Email Security Providers

In 2017, Early Growth researched third-party email security providers, looking for a solution that could easily connect and support security functionality for their native email platform. The core evaluation criteria included:

- Easy install using native API integration with Google Workspace
- Identification and automatic quarantine of malicious emails
- Remove employees from difficult, security-related decisions when interacting with email

Secure Email Gateway (SEG) solutions were immediately removed from the evaluation list, due to changes in mail exchanger (MX) records that would add more work to the initial deployment phase. In addition, because the initial integration appeared cumbersome, the cost of the software and the resource constraints eliminated them from the evaluation process.

"All the larger vendors were either extremely costly or wanted us to do a lot of the work up front by changing all these records and by doing a lot of employee education," McCain said. "I was looking for a email security solution that is going to save me time, not add more work."

During the evaluation process of email security solutions, Early Growth requested demonstrations from multiple email security providers. Other providers' complex dashboards required staff education to use effectively. When the staff reviewed the demo of GreatHorn's Cloud Email Security Platform, they made the decision to immediately purchase the solution.

Results with the GreatHorn Email Security Platform

Early Growth was impressed with the ease of integration and deployment of the GreatHorn solution into their Google Workspace environment. "The deployment was important to our organization, because we didn't have the bandwidth for a tedious process. We needed to solve our problems immediately and that's exactly what we experienced with GreatHorn," McCain said.

After deploying the GreatHorn Email Security Platform, Early Growth was able to eliminate the manual processes previously utilized for managing malicious emails within their environment. Replacing those processes with the automated GreatHorn solution has saved her security team hundreds of work hours, McCain estimates. Work handling malicious emails was reduced by 90%, down to a 15-minute-a-day task that one person can handle, she said.

"Rather than spending hours blocking these bad emails, with GreatHorn it's as easy as logging into the administrator panel and selecting to delete, approve or deny the emails. It's a life saver and has taken a tedious job and turned it into something that is manageable," McCain said.

The GreatHorn Email Security Platform provided an interface that was simple to use, allowing the team to access everything they needed in a dashboard that is intuitive and actionable.

"GreatHorn is a product that is easy to use and easy to understand," McCain said. "I trust it completely."