FORTRA™

DATASHEET (CLEARSWIFT)

Filling the Gaps in Microsoft 365

Leading Cloud Data Management Company Deploys Fortra's Cloud Email Protection and Stops Executive Impersonation in its Tracks

Executive Summary

Blink, and they might have missed it: Security leaders at a major cloud data management company recently identified a shift in their security posture after experiencing a spike in email attacks targeting their executive team with exquisite precision. As it happens, the company's existing email security controls were unable to detect and disrupt the attacks because the solutions were designed to search for malicious payloads. Instead, these emails appeared to employ executive impersonation and social engineering tactics that are are highly effective at bypassing this kind of content analysis. The Senior Director of Information Security and his team knew they had a choice: Act quickly, or risk a dangerous compromise to the organization. By leveraging Cloud Email Protection, the team was able to eliminate the attack risk, bring trust back into the organization's email communications, and reduce the resources assigned to mitigate the problem. Today, this leading cloud data management company's executives, employees and partners all enjoy the confidence that comes with knowing they can communicate productively—without fear of compromise.

The Modern, Sophisticated, Identity-Based Attack Epidemic

Over the past few years, the InfoSec team logged a steady rise in the number of targeted email attacks escalated by their executive team after successfully circumventing the security solutions InfoSec had in place. Understandably, the executive team's concerns and frustrations mounted with each new attack, unable to understand why a seemingly simple problem could not be solved quickly. In investigating the problem, the InfoSec team found that the attacks were highly sophisticated, socially engineered, impostor-based schemes specifically designed to bypass existing controls. "Many of these attacks fit the profile of the executive asking for urgent contact, moving the conversation from email to another channel to launch subsequent social engineering attacks.

COMPANY SNAPSHOT

INDUSTRY

- Cloud Data Management

ENVIRONMENT

- 3600+ employees worldwide
- Microsoft 365 with Exchange Online Protection & Advanced Threat Protection

BUSINESS & TECHNOLOGY CHALLENGES

- Deteriorating executive and employee productivity due to daily missed credential phishing, executive, and partner spoofing-based email attacks
- High-risk for compromise, having thwarted several compromise attempts that leveraged successfully phished credentials

SOLUTION

- Cloud Email Protection

BENEFITS

- Enabled productive communication between executives, employees, partners, and customers without fear of a data breach
- Reduced time spent & number of incident investigations needed
- Re-established trust between executives and the Information Security team, resulting in increased investment in security programs
- Fortified investment in M365 while maintaining an easy to manage messaging architecture

Other attacks asked for specific information like personnel data or if it was the CFO or CPO, Merger & Acquisition information," recalls the Senior Director of Information Security. "Display Name impostor-based attacks that would use previously employed identities was also a big issue for us. Attackers would conduct research on our company to identify a previously employed executive. They would impersonate this identity and reach out to current executives attempting to retrieve sensitive data."

The organization had recently migrated to native Microsoft 365 and therefore was leveraging Exchange Online Protection (EOP) as their Secure Email Gateway. In addition, they also purchased the M365 Advanced Threat Protection (ATP) add-on to combat these threats. And yet they continued to face challenges. EOP with ATP was effective in stopping spam, known viruses, and other content-based attacks but were ineffective at safeguarding against highly targeted, impostor-driven attacks. Their initial solution forced them to manually generate content filtering rules for every missed spear phishing attempt and Business Email Compromise (BEC) attack. Unfortunately, the process consumed too many resources from both the Messaging Operations and InfoSec teams. What's more, EOP was too limited in the type of filters it could create, and introduced too many delays to be effective. "Aligning the teams was very challenging. Message operations did not know enough about the threat landscape and feared an interruption in legitimate mail flow while the InfoSec team did not have the M365 configuration skills to optimize protection," mentions the Senior Director. "It would take several hours to days to implement rules and by that time, new attacks would surface."

The situation finally hit a breaking point when several key individuals' credentials were nearly compromised as a result of an undetected partner-spoofing phishing attack. Fortunately, the potential loss of sensitive data was averted, but it was a clear sign that a solution needed to be found—fast. The InfoSec team risked the complete loss of executive trust and future program investments if they could not deploy an effective solution.

Agari Stops Executive Impersonation

The team established that solving the problem meant the solution would require:

1. Out-of-box policies with minimal-to-no configuration needed
2. 'Out-of-band' and high-availability, cloud-based deployment
3. Immediate and on-demand email policy enforcement via M365 mailbox API
4. Reporting that provides visibility into the volume of email analyzed, the number of malicious email detected, types of threats detected, and more

The InfoSec team evaluated multiple solutions and ultimately chose Cloud Email Protection. "EOP with M365 ATP was our primary solution but cybercriminals had gotten very good at avoiding these controls. We needed a solution that understood the relationships with ATP in our mail flow to pick out the mail that didn't belong. We evaluated Proofpoint's Protection Server with Targeted Attack Protection (TAP) but ultimately selected Cloud Email Protection because of its superior effectiveness and data-driven approach," mentions the Senior Director. "In addition, our mail configuration had been simplified with M365 Native so we needed a product that didn't need to be 'in-line' but could still provide protection via mailbox API integration. Agari also offered this capability by default."

Since the deployment of Cloud Email Protection, the team hasn't seen anywhere near the high number of executive escalations that strained their resources. Nor have their executives had to change their user behavior when communicating via email.

"Our executives work in a fast-paced capacity and have done so successfully for the past 20+ years of their careers. When it comes to email, they don't want to stop and wonder if an email is malicious. They want to read and respond quickly because any delay could mean a missed opportunity for the business. We wanted our executives to continue being successful and did not want to change their user behavior that made them so. Ultimately, our goal was to find a solution that removed the threat completely out of the inbox," says the Senior Director.

"EOP with M365 ATP was our primary solution but cybercriminals had gotten very good at avoiding these controls. We needed a solution that understood the relationships within our mail flow to pick out the mail that didn't belong. We evaluated Proofpoint's Protection Server but ultimately selected Cloud Email Protection because of its superior effectiveness and data-driven approach."

"Today, Cloud Email Protection stops an average of 18,000 unwanted messages per month from reaching our employees' inboxes. That's 18,000 messages our team does not have to worry about analyzing or archiving and 18,000 messages our employees don't have to waste time manually filtering or deleting every month."

– Senior Director of Information Security

Agari Fortifies O365 by Stopping Over 18,000 Unwated Messages/Month

By deploying Cloud Email Protection, the security leaders have regained the trust from their executive team and subsequently reduced the operational load for both Messaging Operations and InfoSec, while also improving internal collaboration. Messaging Ops in particular, no longer has to spend cycles manually creating EOP content-filtering rules and risk interruption to legitimate mail flow. Both teams have been able to work collaboratively within Cloud Email Protection to validate policies prior to rolling them out into production. Finally, Cloud Email Protection has been performing better than expected, as it is also eliminating a significant amount of non-targeted, "scattershot" phishing and spam attacks. This has been a huge plus for both teams as it helps maximize the organization's investment in Exchange Online.

For the InfoSec team, eliminating high-profile attacks has also removed the need for an analyst to spend several hours determining if a true compromise occurred. For compromised executives, this processes was highly disruptive and extremely cumbersome due to the fact that the analyst had to piece together unauthorized sessions, the timing of the attacks, and what data may have been impacted, in order to make a final determination. The team simply did not have the resources or the expertise to consistently come to the right conclusions. Today, most incidents are trivial annoyances that can be remediated in as little as 15 minutes.

Secure Email For Today and Beyond

In the near future, the InfoSec team plans to extend the use of expert-generated and verified intelligence by integrating the data into their SIEM and Security Automation and Orchestration solutions. The Senior Director believes this data could be valuable in helping investigate non-email related incidents. Additionally, with Agari's newest Account Takeover (ATO)-based attack prevention and reporting capabilities, the organization can now stop targeted attacks launched from a compromised email account. The visibility provided will help the organization and its partners regain control of these rogue accounts and ensure that the entire email ecosystem is safe.

SUMMING THINGS UP: This leading cloud data management organization chose Cloud Email Protection over other options because it's the most effective solution available for stopping executive impersonation and other advanced spear-phishing attacks. Its flexible architecture design enabled quick onboarding and a seamless integration into the organization's architecture. Automated and on-demand policy enforcement saves users' time and reduces exposure, even as zero-day risks have arisen. Finally, its reporting capabilities gives the organization full visibility into the total number and types of threats that are actively bypassing their existing secure email gateway, easily justifying continued investment. What's more, the organization demanded a security partner that would align with its focused priorities—and Agari delivered. As the Senior Director puts it: "As a cloud service provider, protecting the platform, our customer's data, and maintaining trust in our security capabilities is crucial. With email as our primary mechanism for engaging with current and future customers, securing this channel was a top priority. By partnering with Agari to stop customer phishing and targeted email attacks, we have enabled our customers, partners, and employees to communicate freely—without fear of being compromised."

Learn more at: www.agari.com/products/cloud-email-protection

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.