Clearedin

CASE STUDY

Case Study: Lee Company

Top 3 Case Study Highlights:

- Strengthens existing Secure Email Gateway (SEG) IT foundation as critical element to protect diverse construction and service business profiles; Clearedin automates a multi-threaded anti-phishing security layer to block third- party email impersonation
- Prevents Business Email Compromise (BEC) targeted social engineering threats including executive impersonation across any O365 collaboration (Email, Teams, OneDrive, SharePoint Online) for gift cards, credit payments or bank transfers; negates phishing's financial consequences
- Provides real-time staff training and assistance to prevent phishing without demoralizing staff or disrupting Work from Home users; layered phishing protection for business operations across increasing numbers of email and collaboration platforms

Who is the Lee Company?

Leon Lee founded Lee Company in 1944 as a community-minded construction and building services firm. 76 years later, operations for this family-owned $300 million company have grown to nearly 1,500 staff dedicated to handling all facets of home, facilities, and construction projects. Covering Tennessee, Alabama and Kentucky, Lee Company services include HVAC, plumbing, electrical, and appliance repair, as well as huge construction projects. The firm works with homeowners and clients in government, institutional, commercial, healthcare, and industrial organizations.

What is the current email, cloud, and collaboration security architecture at Lee Company?

Email is critical at Lee Company—everyone uses it. Email defined the initial conscious investment in secure email gateway (SEG) functionality. With more than 100,000 emails weekly between staff, suppliers, and customers, the SEG rejects nearly 25 percent of that correspondence. Phishing threats, especially third-party email impersonation, are prevalent as vendor supplier communications are corrupted leading to

LEE COMPANY

Headquarters:
Franklin, TN

Founded:
1944

Industry:
Manufacturing

www.leecompany.com

"We live and die by email. That requirement has evolved to require additional protection like Clearedin's Trust Graph to help us manage compliance risks across 0365, Teams, SharePoint Online and OneDrive."

– Chris Reaves, Director of IT Lee Company

malicious attempts inside Lee Company. Clearedin's additional four connected security cross beams of chat (Teams), email (O365), collaboration (SharePoint Online), and file sharing (One Drive) adds important compliance and phishing protection to the existing SEG.

"Our SEG is rejecting nearly 25 percent of inbound email traffic, phishing is clearly a growing multi-vector concern and we need to build additional layers of protection into our security stack using Clearedin," said Chris Reaves, Lee Company Director of IT.

How is Lee Company handling advanced persistent threats?

Protecting against social engineering and emails coming from newly registered domains is driving an uptick in BEC and spear phishing attempts. Lee Company found it urgent and necessary to address new gaps identified in SEG filters. Look-a-like domains or emails coming from newly registered domains go undetected for weeks or months as they gain access to high value employee targets and remain undetected for an extended period. Solving more advanced threats is critical since a single successful phishing attempt rapidly spreads laterally inside the company. Data Loss Protection (DLP) capabilities are critical for Work From Home file sharing and messaging into and out of OneDrive and SharePoint.

What were Lee Company's unique needs and requirements? Why select Clearedin over other solution providers?

Clearedin protects Lee Company against BEC (especially emails from newly registered domains), targeted third-party email impersonation & social engineering phishing attacks that continue to evade the email gateway. Combining Trust Graph with in-app user training, dynamic dashboards and reminders helps make phishing a top-of-mind concern for all employees. Moving beyond the manual intervention requirements of other phishing solutions, Lee Company depends on Clearedin to automatically consolidate previously disparate compliance enforcement across 0365 email, Teams collaboration, OneDrive file or link sharing and SharePoint collaboration links. Machine Learning (ML) powers Trust Graph visibility and manages risks. Clearedin automates the removal of inappropriately shared links that deliver many DLP holes.

"The Lee Company operates more than 2,500 individual Microsoft Teams instances mapped to specific projects. All projects have sensitive business and client data that needs Clearedin phishing protection to keep vendors, employees and customers secure," said Chris Reaves, Lee Company Director of IT.

Clearedin

"Clearedin is excited to partner with Lee Company to help stop the uptick in targeted socially engineering attacks over email and ensure compliance for their WFH digital collab channels like Teams, OneDrive and Sharepoint Online."

– Ajay Mishra
CEO , Clearedin

What are Lee Company's primary goals to deploying a phishing prevention platform?

Lee Company's primary purpose for deploying Clearedin is to build a best practice, defense in depth email, cloud-collaboration security, and compliance approach to reverse the uptick in phishing as they pursue growth in construction services and the energy market. Lee Company needs a scalable solution with strong foundation functions including:

- Dynamic security dashboard with automated remediation
- Proactive threat hunting and active defense against emails coming from look-a-like or newly registered domains
- 3rd party email impersonation prevention
- Blocking ATO (outsider) attacks on 0365
- Unified phishing prevention across 4 channels: 0365 Email, Teams Collab, DLP for both OneDrive and Sharepoint Online file sharing

Did Lee Company have specific anti-phishing use case requirements?

More than 2,500 Team instances are live at Lee Company as every project operates a unique Microsoft Teams environment. Correspondingly, large quantities of email, collaboration messages and alerts originate from Teams, requiring an immediate 24-hour domain block SLA for suspected phishing incidents. Clearedin's powerful ML via Trust Graph and corresponding Trust Score raise the roof on automating a best-in-class phishing prevention backbone to manage compliance risks over 0365, Teams, SharePoint Online and OneDrive. Clearedin partner Dominion Security is helping Lee Company provision and scale the deployment.

Clearedin

Clearedin is an innovative cybersecurity platform that uses AI-driven Trust Graph technology to help IT teams eliminate phishing. Clearedin's Cloud Security platform delivers 4 channels of phishing protection for all popular B2B software platforms: chat, email, collaboration, and file sharing. Clearedin protects against dangerous social engineering and malicious exploits across all of your communication and collaboration channels.

LET'S GET STARTED

Request a demo today!
info@clearedin.com
www.clearedin.com