Clearedin

Case Study: Ledn

Top 3 Case Study Highlights:

- Enforce Canadian, multi-national PCI/PII compliance regulations over email (G Suite), collaboration (Slack), file share (G Drive) and conferencing like Google Meet

- Deliver better phishing protection and manage external file sharing data leak prevention (DLP) risks caused by links shared inappropriately over G-Drive

- Protect employees against Business Email Compromise (BEC) and targeted social engineering threats on Gmail, and set the highest standard for cloud email, collaboration security and compliance within the digital asset industry

Who is Ledn?

Ledn is Canada's largest digital asset lender, building financial products that help people save in bitcoin and other digital assets like stablecoins. Ledn has four live products including a savings account that pays up to 11.7% APY and is proud to serve clients across 100 countries. Ledn is focused on building technology that makes financial products accessible, simple, and secure to use. The cryptocurrency industry currently has a market cap of over $330 billion and experts estimate the cryptocurrency trading volume in 2019 was $227 billion with a CAGR of 15.7 percent. The ability to lend digital assets is one of the fastest growing segments of this industry with an estimated $6 billion of digital asset loans outstanding as of June 2020.[1]

What problems is Ledn solving in their email and cloud collaboration compliance security through Clearedin?

Ledn reviewed a wide range of secure email gateway and anti-phishing solutions but needed a consolidated level of customer account credential and BEC protection and a multi-channel security layer across email, chat,

Ledn

Headquarters:
Toronto, Ontario

Founded:
2018

Industry:
FinTech

www.ledn.io

[1] reports.credmark.com/TheCryptoCreditReport-q2-2020.pdf

Ledn

web, and file share platforms. The company asked Clearedin to solve this complex problem and add powerful visual cues for phishing protection using G Suite including email. Specifically, Ledn requires security to prevent spear phishing, business email compromise (BEC) and account take over (ATO) attacks.

"Our most important job is protecting client assets - both financial assets like bitcoin as well as client data. Given this, we are always looking for the best tools to protect against any security threats. Clearedin adds a layer of anti-phishing to protect our team and global clients from non-static attacks and unintentional human error," said Ledn CEO Adam Reeds.

Ledn Sr. Software Engineer & Security Lead Anton Livaja added, "Cryptocurrency is a highly-targeted industry for digital theft and cyber-attacks. Clearedin is an important tool in our security toolbox providing an additional safeguard and competitive advantage."

Phishing protection drives compliance globally and Ledn needed an approach with sufficient analytics and protection to satisfy our high standard for client asset and data protection. The regulations require Ledn to address customer cross-channel visibility and security coverage for tools like Slack. Clearedin delivers these as part of its real-time threat-hunting and incident response using a rich, intuitive, and user-friendly patented Trust Graph platform.

Ledn follows local regulations and compliance requirements including FINTRAC and GDPR. Use of Clearedin's Identity Trust Graph will help Ledn align its business with Know Your Customer (KYC) rules for monitoring customer transactions and filing suspicious activity reports.

How will Ledn leverage Clearedin to block prominent security attack vectors over email and chat/collab tools?
Ledn is banking on Clearedin's Identity Trust Graph, Trust Scores, and dynamic dashboard to rapidly identify known versus unknown and untrusted external users. For unknown users, Ledn relies upon Identity Trust Graph to pinpoint attack vectors attempting to impersonate external people and domains Ledn already trusts. With phishing on the rise, this compounds the risks of dangerous BEC and Spear-Phishing attempts that inevitably leak through both Microsoft 365 and G Suite's security filters.

Data Leakage Protection (DLP) boosts valuable attack targets for Google Drive, OneDrive and Microsoft 365 SharePoint. The Ledn team will use Clearedin to continuously monitor file sharing from G Drive. Leveraging the

Clearedin

power of Identity Trust Graph, Ledn's security and compliance teams gain rapid visual insight into file sharing with inappropriate known and unknown recipients, including sensitive files shared with anonymous links. Clearedin's powerful Machine Learning (ML) engine accelerates Identity Trust Graph to rapidly control compliance risks from G Suite email, Slack, and Google Drive.

To combat multiple, socially engineered threat vectors, Clearedin allows clients to proactively address:

- 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 Microsoft 365
- Unified phishing prevention across 4 channels: Teams Collab, DLP for both OneDrive and Sharepoint Online file sharing

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