EDM Webinar

Securing Data in the Era of Third-Party Revolution:

Redefining Data Security with Copilot and GenAI

A conversation with

Mark Sutera
VP, Enterprise Sales
Seclore

Jim Halcomb
Global Head of Research & Development
EDM Council

SECLORE™

EDM Council

Today's panel

Moderator

Jim Halcomb
Global Head of Research & Development
EDM Council

Mark Sutera
VP, Enterprise Sales
Seclore

© 2022 EDM Council Inc.

Agenda

- The Evolution of Third-Party Collaboration
- Understanding Copilot and GenAI
- Data Security Challenges
- Flipping the Economic Incentive on Adversaries
- Best Practices for Mitigation
- Q&A

©2024 Seclore. Proprietary and Confidential.

Poll Question

How does the security and data interact in your organizations?

- Governance
- Adhoc
- Combined teams
- SDLC
- Not at all

©2024 Seclore. Proprietary and Confidential.

Data Breaches Are Becoming Endemic

Notable data breaches in the Banking Sector involving 3rd party vendors

Global US Bank:

PII and PCI like names, SSNs, Acct numbers, and balances for more than **11,000** customers was shared after a 3rd party collections recovery group gained access to information they shouldn't have.

IT consulting Giant Infosys:

U.S. based subsidiary, McCamish Systems, had an enormous data breach of **6+ million** records. First thought to be just 57,000 individual's PII (SSN, DOB, medical details, Biometric data, emails, passport #s, address, driver license numbers, and financial account information.

Third Party Data Breach: Large Global Investment Bank

Data security incident revealing personal and financial information of 450,000+ individuals

What happened?

Retirement plan account information for more than 451,000 users released:

- Names
- Addresses
- Social Security Numbers (SSNs)
- Payment and deduction amounts
- Bank routing & account numbers
- Credit/Debit card numbers
- Codes, passwords, and PIN #'s

How did it happen?

Vendor-provided software exploit issue led to unauthorized access

- 3rd party Software exploit (introduced 8/26/21, patched 8/23/24)
- Three (3) unauthorized users accessed sensitive plan information in this timeframe.

How can Seclore help?

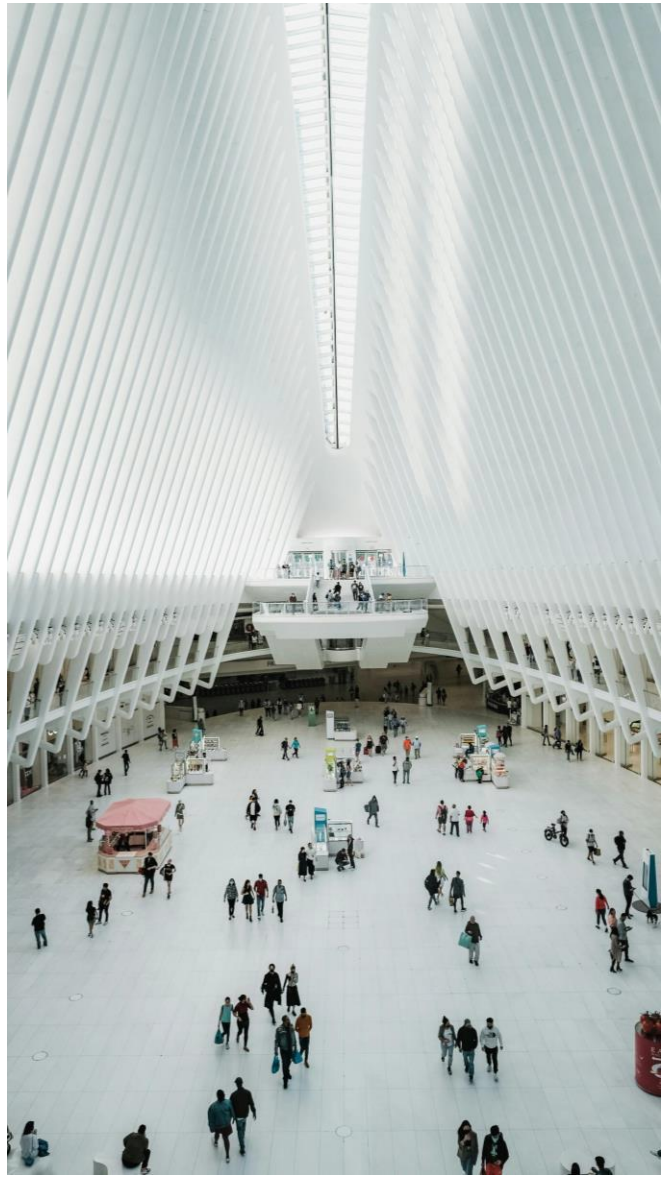
By protecting digital assets beyond the perimeter

- Encrypt sensitive data
- Authenticate users before they access files
- Track activity
- Revoke access any time

Avoiding Third-Party Data Breaches

Persistently protect sensitive data shared with third-parties

- ✓ Attractive targets for cyber criminals
- ✓ Popular target industry for cyber criminals
- ✓ Data breaches cost more every year
- ✓ Vendor management is time-consuming
- ✓ Access to non-public personal information (NPI)
- ✓ Third-party data security practices



Redefining Data Security with Copilot and GenAI

The Impact of GenAI on Third-Party Collaboration

Manual processes and paper-based agreements

- Limited to specific functions such as supply chain and vendor management.
  Our biggest problem was inefficiencies and data silos

Digital Transformation: Shifting Towards AI-Driven Collaborations

- Introduction of cloud-based platforms
- Transition from manual to digital collaboration tools; **eg.** Box, SharePoint, etc.
- Use of basic AI for data analytics and process automation
- Enhanced communication through real-time messaging and video conferencing

GenAI: A Game-Changer for Third-Party Collaboration

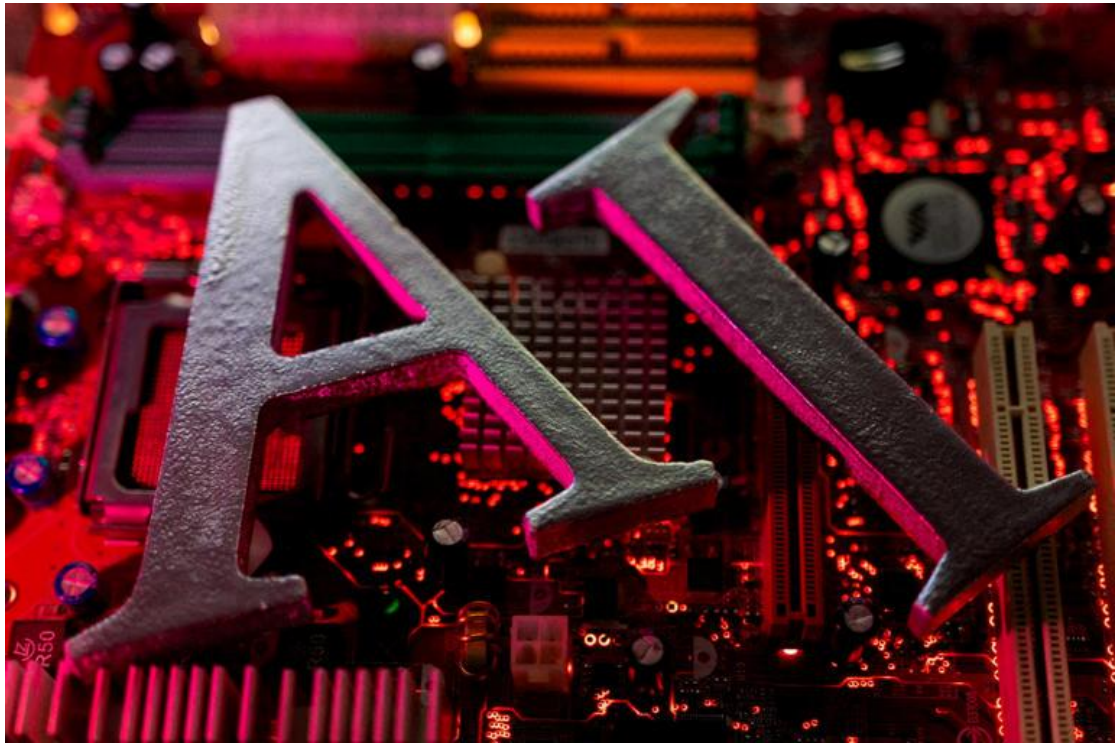
- Enhanced communication through real-time messaging, document collaboration, video conferencing, text/voice translation (real-time), etc. **LIMITLESS POSSIBILITIES**

©2024 Seclore. Proprietary and Confidential.

What our LOBs are thinking

The Promise And Possibility Of Generative AI

- ❑ Enhanced decision-making
- ❑ Optimized operations and efficiency
- ❑ Personalized customer experiences
- ❑ Efficient Software and product development
- ❑ New business models
- ❑ Accelerated Content Creation
- ❑ Greater Valuation



Just two years ago, it would've been almost preposterous to ask organizations how many end users are using public GenAI tools – but today, GenAI in the business is table stakes.

©2024 Seclore. Proprietary and Confidential.

The Evolution of GenAI, LLM & CopilotTechnologies

Relevant business drivers and considerations for protecting sensitive data, when applying GenAI and LLM Technologies.

Interpretations of Data Use Cases: the marketplace wants to know about data changes real-time; doing so is not necessarily a binary or linear process. Often interpretations are subjective or discretionary across data use cases, for example, with principle-based policies or regulatory rules. These involve applying GenAI and LLM technologies to perform such interpretations correctly, checking for the relevant and right data types and their content, conducting language translations, and stitching the data together sensibly and accurately.

Change Management: Being able to reconcile data types and content across the use cases must be done efficiently and effectively, while protecting the data, e.g., access rights and visibility. AI technologies help master these activities via comparative analyses while recording decisions for future reference on use cases.

Workflow automation: the resulting outcomes of GenAI and LLM enabled and tracked data changes are expected to lead to more automation in data workflows while knowing, controlling, and protecting the data, e.g., eliminating previously manual tasks while being conformant to data privacy rules.

Strong data lineage: having good traceability and data lineage is key for understanding changes made systemically using AI based technologies on a historical basis in the event that there are data, rule, change management, or other types of discrepancies.

©2024 Seclore. Proprietary and Confidential.

The Evolution of GenAI, LLM & Copilot Technologies

With the proliferation of AI technologies applied in data intelligence, there are important safeguards to consider for mitigating risks that are high on the radars of regulators and marketplace participants alike.

Being in violation of a regulation:

- Ensure strong set of repeatable checks and balances on data interpretations and protections.
- Run changes in a prod parallel environment with UAT.
- Perform regression testing in prod post code deployment.

Lack of staff awareness and training:

- Ensure staff are trained on the data types and use cases.
- Have a capable Business Analysis function for data applications, interpretations, and protections.

Poor perception with using GenAI and LLM technologies to manage data activities across mandated functions, e.g., regulatory reporting:

- Proactive marketplace awareness of the benefits for using the technologies.
- Promoting the best practices and controls of a data-centric security solutions suite linked to the GenAI and LLM technologies and their related data use cases.

©2024 Seclore. Proprietary and Confidential.

Shadow AI: Learning from the Past

The unintended consequences of querying AI engines reared its ugly head, as evidenced by the early 2023 incident at Samsung, who found trade secrets had been blithely uploaded into ChatGPT.

©2023 Seclore. Proprietary and Confidential.

New Learnings: Copilot Chaos

A Deeper Dive Into Copilot

> **"It's important that you're using the permission models available in Microsoft 365 services, such as SharePoint, to help ensure the right users or groups have the right access to the right content within your organization."**
>
> Source: Data, Privacy, and Security for Microsoft 365 Copilot

However, we all know empirically, that most organizations are about as far from least privileged as they can be. The average organization listening to this today has an M365 tenant with:

- **40+ million** unique permissions (Direct, SharePoint, Guest/External/Public/Link access, M365, etc.)
- **113K+** sensitive records shared publicly **(>3%** shared externally with **ZERO** controls)
- **27K+** sharing links

To make matters worse, permissions are mostly in the hands of end users, not IT or security teams.

©2024 Seclore. Proprietary and Confidential.

The Path Forward

The Promise And Possibility Of Generative AI

- Starts with having a strong data governance program
- identify, classify and PROTECT your data
- Communication, Education and Cooperation

70%

of CISOs believe that generative AI will create an asymmetrical battlefield that will inevitably be tipped in favor of cyber adversaries.

©2024 Seclore. Proprietary and Confidential.

Flipping the Financial Incentives

A Call to Action: Vigilance is Proactive, Not Reactive

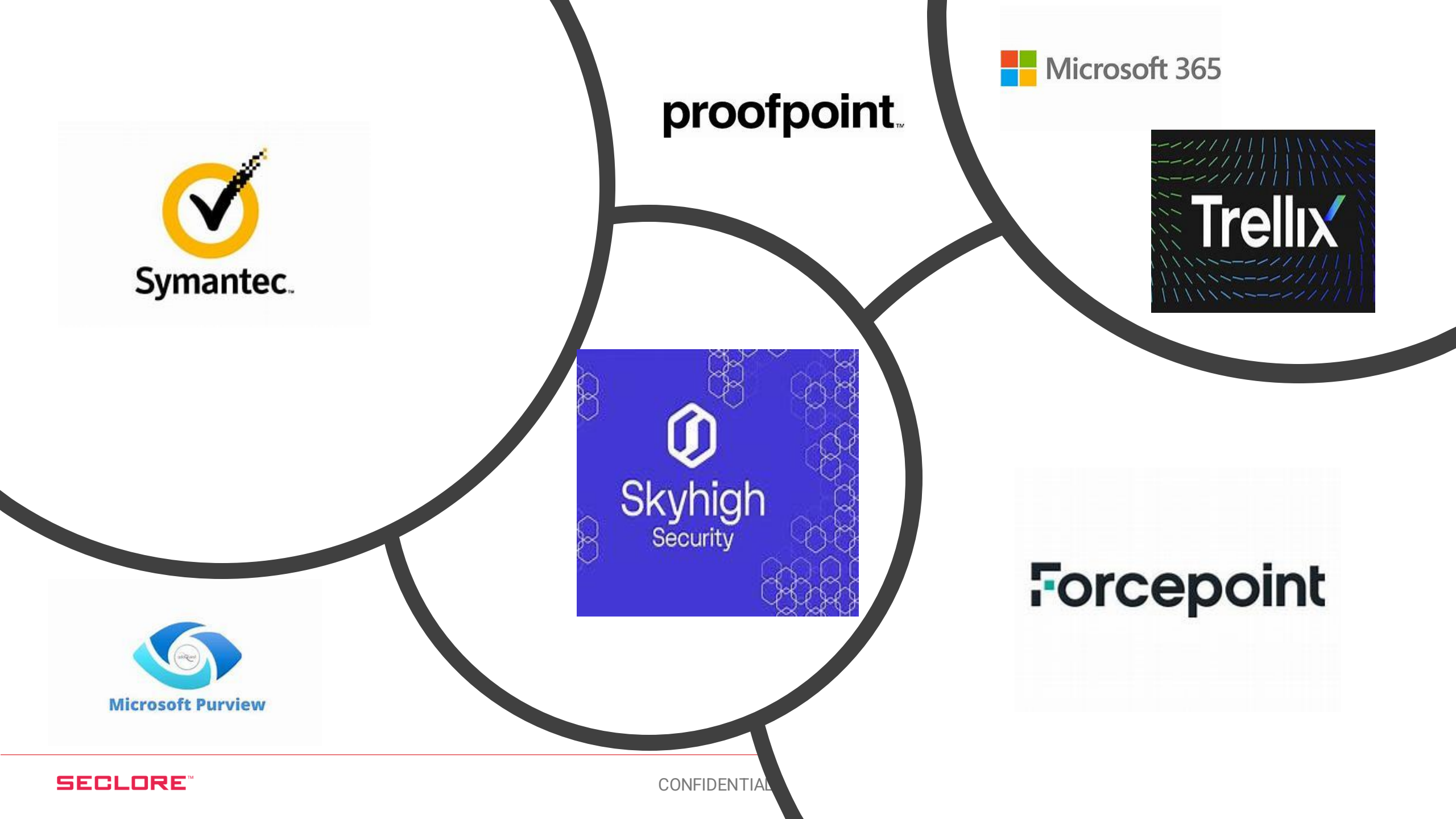
Scenario 1

Imagine your legal team is working on a confidential contract, feeling uncertain about the foreign language and writing. They find a powerful AI tool that can improve their writing to perfection. They eagerly send their contract to the AI, and it delivers as promised. However, they later realized that their confidential document was fed into the AI model and could potentially be reviewed by AI trainers. Even worse, their contract might be used to train the model and appear in other users' outputs.

Now imagine it’s not your team, but your business partner’s legal team does the same.

- How does your exposure change?
- What recourse do you have?

©2024 Seclore. Proprietary and Confidential.


proofpoint
Microsoft 365
Symantec
Trellix
Skyhigh
Security
Microsoft Purview
Forcepoint

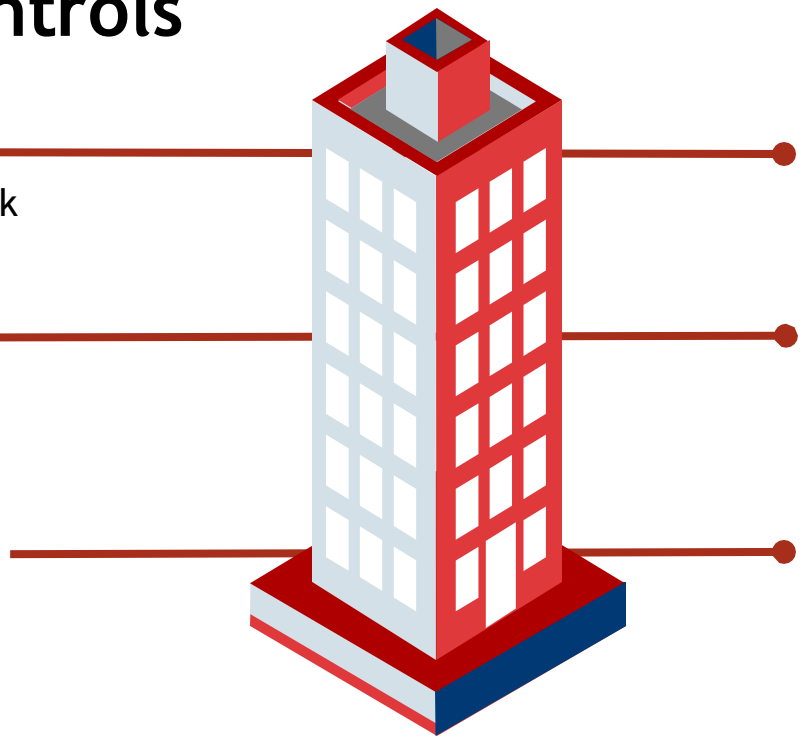
Extending your Security Investments

Common Security Controls

CASB:
Security check point between cloud network users and cloud-based applications.

DLP
Detects and quarantines sensitive data egress at endpoints and perimeter

CLASSIFICATION
Helps to sort and identify information but doesn't enforce usage rights or access controls



SECLORE™

Protects data before, during, and after it leaves the customer's environment.

Secures sensitive data and allows legitimate business flow to continue.

Allows policy-based, automated encryption and security based on Classification wherever the data travels.

Common Use Cases

The Seclore Zero Trust Data-Centric Security Platform is purpose-built for lifecycle control of enterprise-sensitive digital assets (including email). Sensitive data is comprehensively protected and managed in accordance with corporate governance and regulatory requirements. The platform combines the most advanced data security and management technologies to safeguard sensitive data throughout its lifecycle, regardless of location. Critical sensitive data security and privacy functions are consolidated into a single highly automated sequence of processes.

- IP Protection
- Endpoint Security
- Cloud Security
- Compliance
- Remote Worker
- Secure Collaboration
- Email Protection
- AI Content Mgmt.

Questions?

SECLORE™

EDM Webinar

“Seclore-It” - Securing Sensitive Data Persistently

256 Encryption

The first layer of protection is encryption. Each file is encrypted with a unique encryption key. Data itself is protected and travels with the file

Dynamic/Granular Access Control

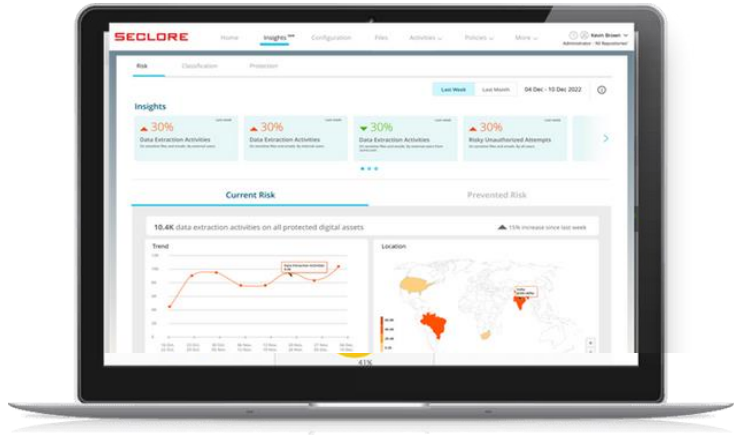
Identity-aware access control by users, roles, and groups Permissions can be set and modified (add/remove/revoke). Whether it’s a group/user/etc.

Active File Security

Explicit control on what can be done with the file/email. Share, edit, print, or even the time that they’re allowed to have access. Trace files anywhere know access usage, remote delete

Dynamic Watermarking

Dynamically indicate the sensitivity of a document, with terms like “CONFIDENTIAL” to ensure that important documents are never mishandled.



- Real-time Access Revocation
- Dynamic Policy Federation
- Risk Insights & Trends
- Access Patterns & Usage Analytics
- Location Awareness
- Compliance Reporting
- “Chain of Custody” Reporting

SECLORE™

Protecting the world's sensitive data wherever it goes. Seclore protects and controls digital assets to help enterprises close their data security gap to prevent data theft and achieve compliance.

TRUSTED & PROVEN

> 60 Million documents and emails protected each month across 2,000+ global customers.

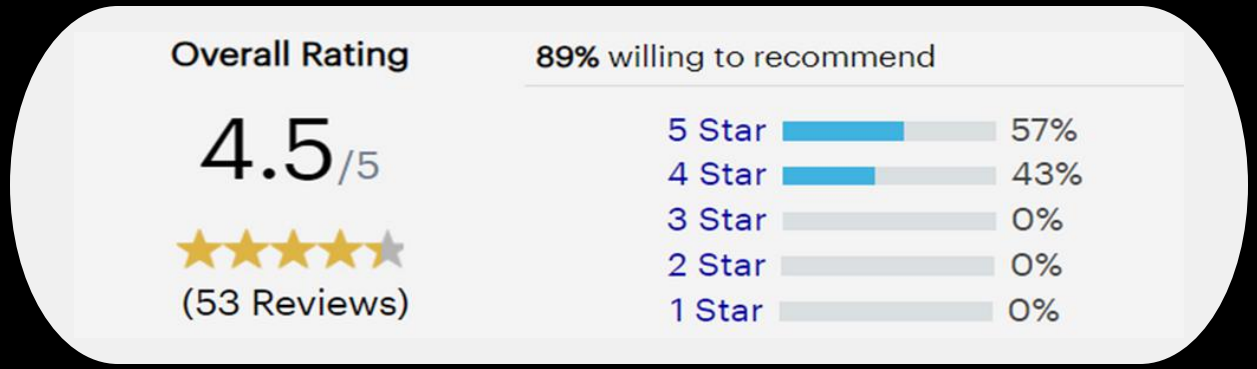
GLOBAL REACH

Deployed in 60+ countries with offices in six countries.

PERVASIVE

Relied on by organizations in every vertical:Financial Services, Manufacturing, & Gov't.

Gartner peerinsights™



WHY SECLORE?

- PROTECTION (AES 256)
- ACCESS CONTROL
- DYNAMIC WATERMARKING
- GRANULAR USAGE CONTROLS
- CLASSIFICATION VISUAL LABELING
- TIME BASED CONTROLS
- LOCATION BASED CONTROLS
- DYNAMIC POLICY FEDERATION
- REAL TIME ACCESS REVOCATION
- ACCESS PATTERNS & ANALYTICS
- RISK INSIGHTS & TRENDS
- GEO LOCATION AWARENESS

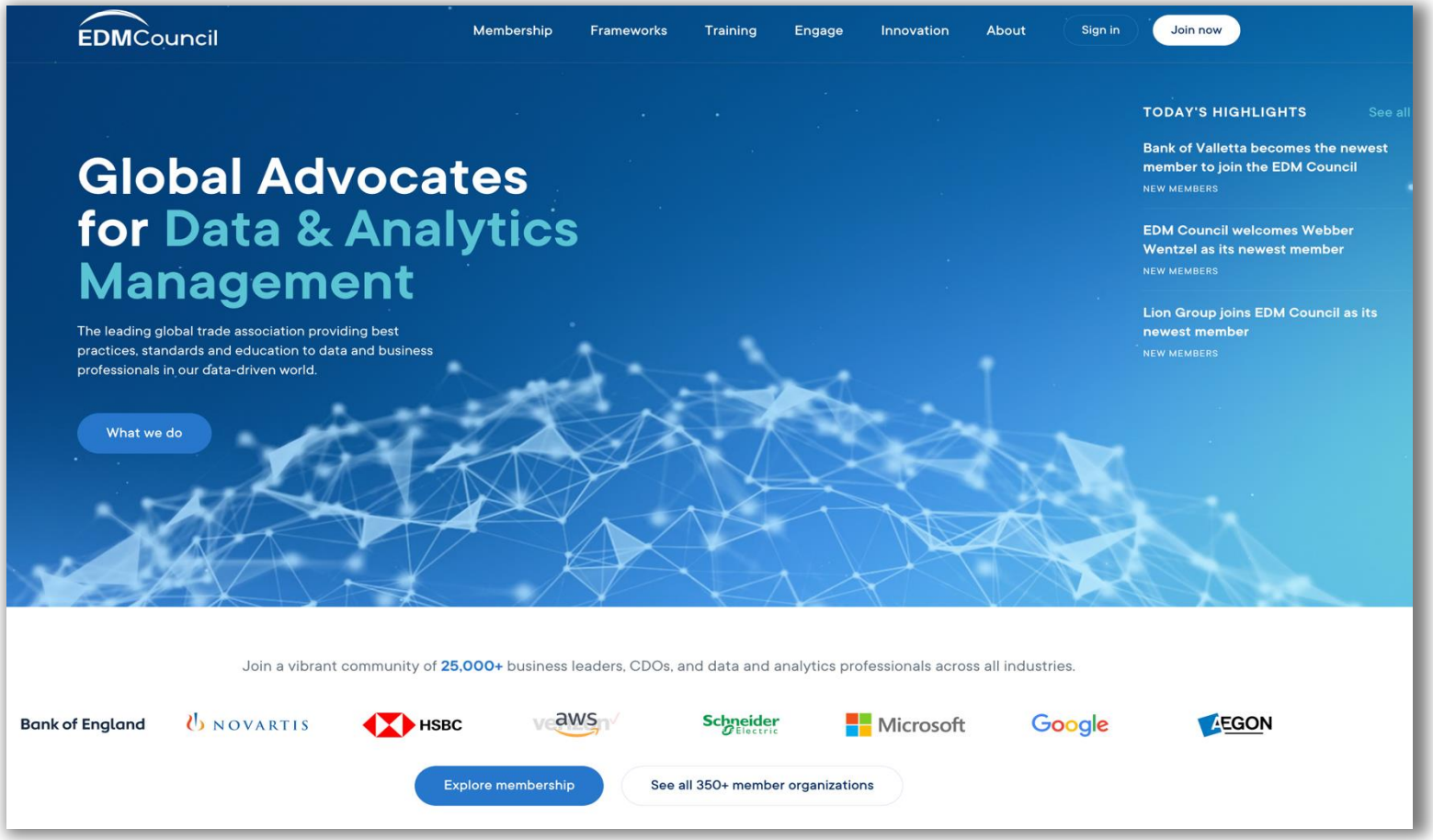
©2024 Seclore. Proprietary and Confidential.

SECLORE™

Schedule a Discussion with Me Here

EDM Webinar

Join EDM Council and our membership community of companies…



EDMCouncil

350+ Member Firms
Cross-industry,
including Regulators

25,000+
Professionals

Worldwide
Americas, Europe,
Africa, Asia, Australia

edmcouncil.org

DCAM

CDMC EDMCouncil

Data ROI EDMCouncil

ESG EDMCouncil

Open Knowledge Graph INNOVATION LAB

elc eLearningCurve










EDM Webinar

Thank you!

FOR MORE INFORMATION:

Mark Sutera
VP, Enterprise Sales
mark.sutera@seclore.com
Call 617-872-1305

SECLORE™

EDM Council