

September 2025

Persistent Data-Centric Security for DISA's Classified and Unclassified Workloads

DISA Emerging Technology Directorate(EM)
Technical Exchange Meeting (TEMS)

Seclore: Leading Data-Centric Security Platform

SECLORE™

Our platform enables **security and compliance of data** as it flows within and across **enterprises, the cloud and third parties**

What We Do:



Prevent Data Theft

- Insider Threat Protection / IP Protection
- 3rd Party Risk Management / Secure Collaboration
- Application Data Security / Cloud Data Security



Achieve Data Compliance

- Data Privacy
- Industry-specific Compliance
- Cybersecurity Frameworks

Global Presence



~400 employees globally



HQ: Santa Clara, CA

Operations in India, the Middle East & Europe

Enterprise Customers



Financial Services



Manufacturing



Government

Key Metrics

Situation

Tasked with an incredibly difficult objective: Ensuring the right people get the right information at the right time ... securely...anywhere... to defend the nation.

This responsibility to safeguard the Department of Defense's most sensitive information extends across both classified and unclassified workloads, each with its own operational realities.

- Unclassified data is increasingly moving to cloud environments.
- Classified mission data remains anchored to on-premises infrastructure.

These realities create two different worlds, one benefiting from modern innovation, the other locked down *for security*.

Problem Landscape

1. Petabyte-Scale Classified Repositories: SIPRNet and higher-classified environments store vast volumes.
 - **Result:** enormous operational complexity in applying consistent security controls at this scale.
2. Strict Data Handling Requirements: Protection required throughout the lifecycle with zero tolerance for disclosure.
 - **Result:** traditional perimeter - or system-based controls break down when files move between systems or users. (example: DLP)
3. Hybrid Security Gap: Risk of isolation or inconsistent protection across environments.
 - **Result:** a fragmented security posture that creates both operational inefficiencies and risk exposure.

Why does this matter?

Mission Integrity:

When protection isn't consistent, classified data can fall through the cracks. A single mishandled file, shared outside the right enclave or left unsecured on the wrong system, can expose operational plans, troop movements, or intelligence sources.

Operational Agility:

Today's mission tempo depends on speed and coordination. Yet when classified workloads are locked in environments with inconsistent or outdated protections, users can't leverage the same tools, automation, or collaboration their unclassified counterparts enjoy.

Adversary Advantage:

Near-peer adversaries are probing relentlessly for weak points in the U.S. cyber and information security posture.

Persistent Data-Centric Security

Perimeter defenses and **system-centric** controls are not enough. The only way to close the seams is to carry security with the data itself—making the file the fortress.

- **Persistent Security:** Protection is bound to the file, not the storage system. It stays encrypted, access-controlled, and governed even if copied, shared, or moved between classified and unclassified domains.
- **Consistency Across Domains:** Whether on SIPRNet, NIPRNet, or in the cloud, the same policies and controls apply—no more inconsistent experiences or gaps.
- **Mission-Ready Access:** Permissions follow mission roles, ensuring only those who need the data can view, edit, or share it, down to the individual file.

How It Works (Practical Walkthrough)

Seclore makes this possible for DISA by embedding policy and protection directly into the data, creating a uniform layer of security across every environment.

1. **Location-Independent Security:** A file is always encrypted, always policy-bound—whether stored on a SIPRNet enclave, a NIPRNet SharePoint drive, or a forward-deployed laptop.
2. **Cross-Domain Enforcement:** Automated classification and policy rules prevent unauthorized downgrades, accidental disclosures, or risky transfers across classification tiers.
3. **Granular Access Control:** Access decisions are tied to mission roles and attributes, not static networks. Viewing, editing, printing, and sharing can be limited or revoked instantly, even after distribution.
4. **Audit & Visibility:** Every access attempt is logged, giving DISA full visibility into how data moves, who uses it, and where controls need to adapt. (*making DLP far more efficient btw*)

“

Hey Marine, can you give me some real-world examples already?

Generic Use Cases

Accidental Data Spillage

(Common in Cross-Domain Environments)

- ❑ **Impact:** Accidental spillage requires costly remediation, system wipes, and risks exposure if not caught quickly. (e.g., copy/paste from SIPRNet to NIPRNet, attaching a classified doc to an unclassified email).
- ❑ **Persistent Data-Centric Security:** File-level encryption and access policies remain intact in any cloud, ensuring **consistent protection across hybrid architectures**.

Cloud Migration of SBU Data

(Sensitive but Unclassified)

- ❑ **Impact:** Sensitive data could be overshared, improperly retained, or accessed outside mission scope.
- ❑ **Persistent Data-Centric Security:** File-level encryption and access policies remain intact in any cloud, ensuring **consistent protection across hybrid architectures**.

Pentagon Email Breach (2016)

What happened (publicly available)

- Attackers (suspected Russian state actors) compromised **20,000 DoD employees' email accounts**.
- The breach exposed not just the emails themselves but also **attachments containing unstructured mission data**: memos, meeting notes, planning documents, and personnel information.
- Because emails and attachments weren't encrypted at the file level, once the inbox was compromised, all content was accessible in clear text.

Impact:

- Sensitive communications about operations, logistics, and personnel were exposed.
- Adversaries gained insight into U.S. defense activities through unstructured text and document analysis.
- The breach damaged trust and forced DoD to shut down parts of its unclassified email system temporarily.

Pentagon Email Breach (2016)



Persistent Data-Centric Security

- ❑ **File-Level Encryption:** Attachments (Word, PowerPoint, PDF, Excel, etc.) would have remained encrypted even if the inbox was compromised. Stolen files would be useless, regardless of environment/personnel.
- ❑ **Policy-Bound Documents:** Persistent controls would restrict actions such as forwarding or saving, printing, copying, etc. beyond approved personnel.
- ❑ **Granular Access & Revocation:** If an account was compromised, access to sensitive attachments could be instantly revoked—cutting off adversaries even after breach.
- ❑ **Audit Trail:** Every attempt to open a file could have been logged, offering forensic visibility to identify which data was actually at risk.

Typo sends millions of US military emails to Russian ally Mali

17 July 2023

Bernd Debusmann Jr BBC News, Washington

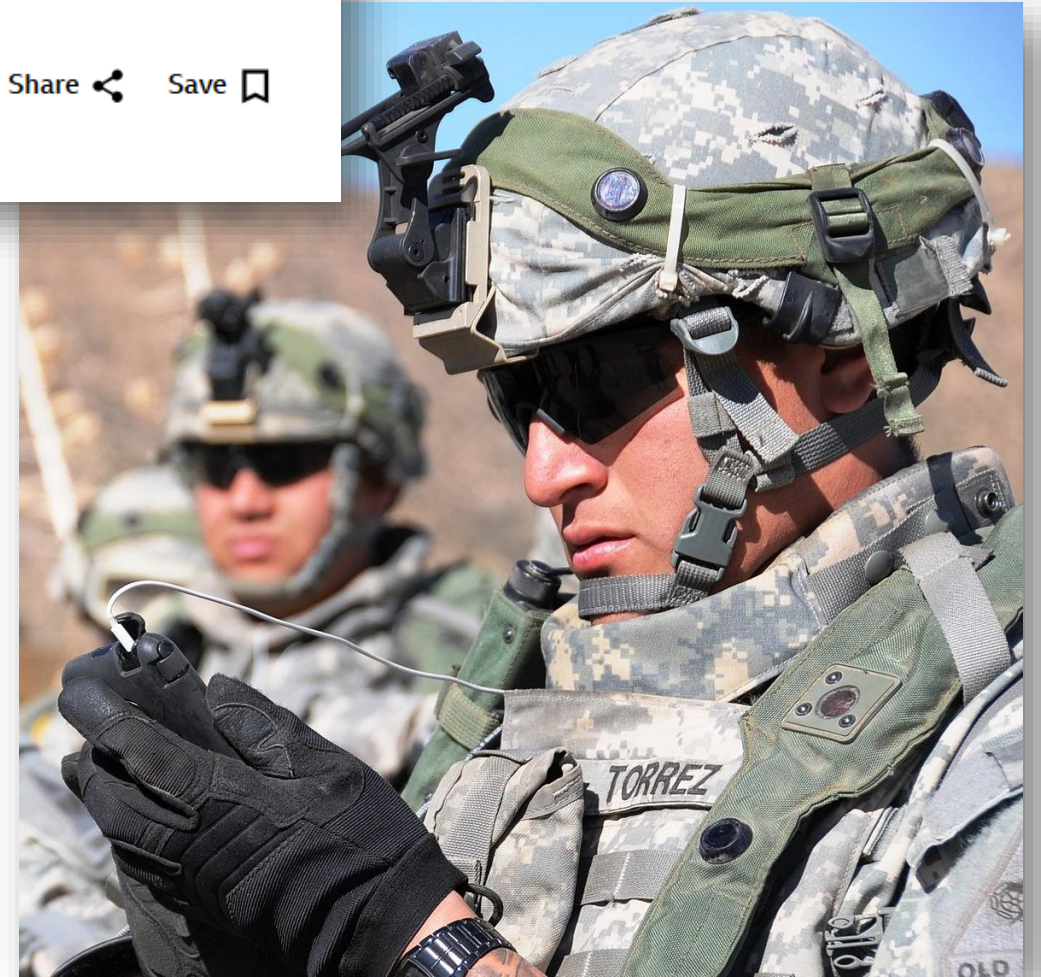
Share  Save 

A simple typo directed millions of emails with sensitive information to the African country Mali rather than their intended U.S. military recipients.

For years, a misspelling of .MIL in the suffix of military email addresses as .ML unintentionally led to a “typo leak”.

As a result, everything from diplomatic documents, tax returns, passwords, and travel details of top officers has been exposed.

SECLORE™



“

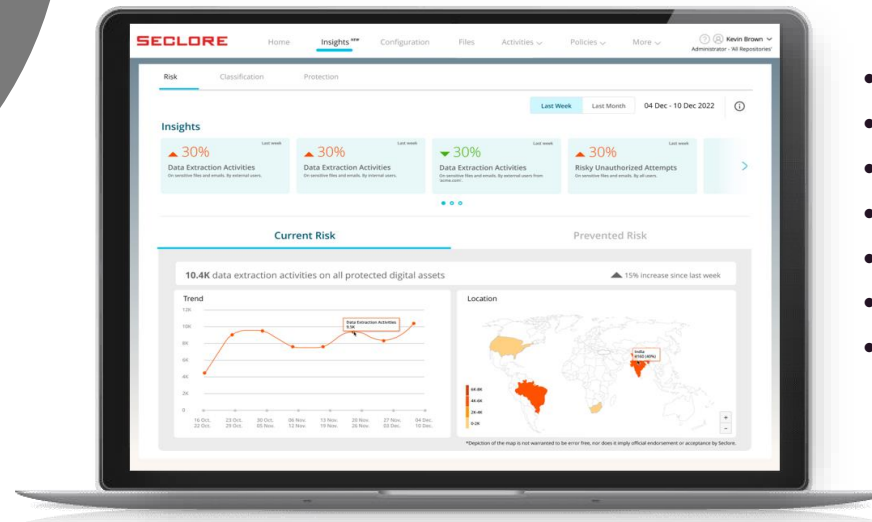
“How can we protect our data persistently? How does it work?”

Possession is no longer Access

SECLORE™



- AES256 Encryption
- Dynamic/Granular Access Control
- Active File Security (Geofence, Print, Edit, Screen Capture, Decrypt)
- Dynamic Watermarking



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

“

“Any other examples you can provide?”

High Profile Use Cases

Edward Snowden

NSA Data Exfiltration (2013)

- ❑ **Impact:** Insider threats remain one of the most complex problems to solve, especially in classified environments where contractors and partners often have elevated access.
- ❑ **Persistent Data-Centric Security:** Even if an insider obtains files, persistent file-level controls can prevent opening them outside the right mission enclave, block copying/printing, or revoke access after suspicious behavior is detected, or make them time-bound.

Manning / WikiLeaks

DoD Cable Leaks (2010)

- ❑ **Impact:** Sensitive battlefield reports and diplomatic cables were exposed, damaging U.S. credibility and potentially endangering sources.
- ❑ **Persistent Data-Centric Security:** Granular, role-based access would have limited downloads to mission-relevant content. Persistent controls could have flagged or blocked mass extraction, and usage logs would have offered early detection.

These incidents show that breaches rarely happen because firewalls or networks fail; they happen because once **data leaves the system, it loses protection**. Persistent data-centric security closes that gap by making the file itself the control point, ensuring security **travels with the data**.

Questions?
Demo?

Book time with Seclore

Thank You!

