U.S. Government Body

About the customer.

This mid-sized U.S. government body handles large volumes of Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). As a federal contractor, it was required to meet the cybersecurity standards outlined in the Cybersecurity Maturity Model Certification (CMMC) framework to maintain eligibility for federal contracts.

The challenge.

To comply with CMMC, the organization needed to demonstrate maturity in areas such as access control, auditing, incident response, and risk management. But their existing infrastructure—based on Active Directory and on-premises File Servers—lacked the native tools necessary to meet these stringent requirements. Specifically, the organization struggled to:

- Define and enforce least privilege access to CUI and FCI.
- Generate auditable records of user behavior, permission changes, and system modifications.
- Detect and investigate anomalous activity across systems.
- Maintain a clear understanding of risk levels related to user access and data security.

Without a way to address these gaps, the customer faced the risk of non-compliance, disqualification from federal contracts, and increased exposure to insider threats and data leakage.

The solution.

The organization implemented the Lepide Data Security Platform to streamline CMMC compliance and improve their overall security posture. Lepide provided:

- **Detailed access control and permissions** reporting to support CMMC practices C001, C002, and C004—ensuring that only authorized users could access CUI and FCI.
- **Advanced auditing capabilities** for user behavior, permission changes, and system configurations (C007-C010), offering a complete trail of activity across the environment.
- **Real-time anomaly detection** and detailed logs to support incident response and post-incident analysis (C017).
- **A dedicated risk analysis dashboard** (C031) to identify high-risk users, events, and misconfigurations that could lead to compliance violations.

With Lepide in place, the customer successfully passed a CMMC audit conducted by an accredited Third Party Assessment Organization (C3PAO).

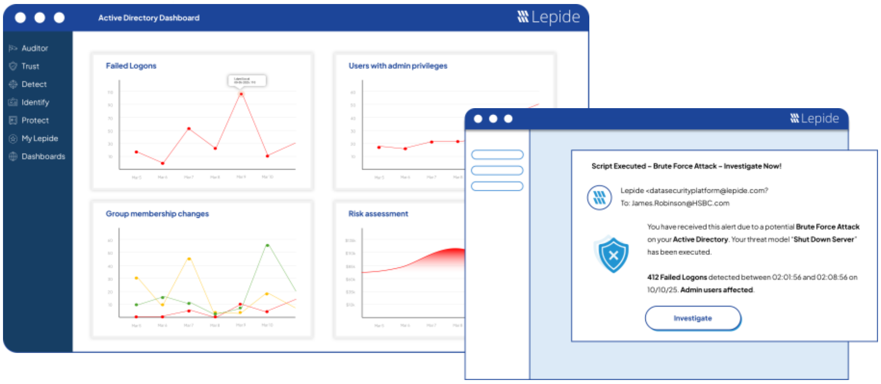
Key security outcomes.

Benefit	Impact
CMMC Certification Achieved	Enabled successful audit by a C3PAO with full alignment to access control and audit requirements.
Access Visibility and Control	Enforced least privilege and reduced risk of unauthorized access to sensitive government data.
Streamlined Audit Readiness	Delivered continuous monitoring and audit logging across AD and File Server environments.
Reduced Risk Exposure	Provided actionable insights through a centralized risk dashboard to help mitigate future threats.

What the customer said.

"In the end, Lepide was the most cost-effective way to ensure that we could implement the right access controls and processes for CMMC. We've got a better understanding of our CUI, FCI, and general unstructured data—and we feel confident that we've reduced our risk to data."

IT Director, U.S. Government Body



Script Executed – Brute Force Attack – Investigate Now!

Lepide <datasecurityplatform@lepide.com?
To: James.Robinson@HSBC.com

You have received this alert due to a potential **Brute Force Attack** on your **Active Directory**. Your threat model "**Shut Down Server**" has been executed.

412 Failed Logons detected between 02:01:56 and 02:08:56 on 10/10/25. **Admin users affected**.

Start your 20-day free trial today!