

USAF Enterprise Data Loss Prevention Pilot

USAF-688 CW-C-InT E-DLP Pilot | October 1, 2021

TABLE OF CONTENTS

[Introduction](#)

[USAF E-DLP Pilot](#)

[Selected Candidate for Pilot was Symantec® Data Loss Prevention Suite](#)

[E-DLP Pilot Success Story](#)

[How E-DLP Fits into the USAF's Zero Trust Strategy](#)

[Conclusion](#)

Introduction

On May 5, 2021, the United States Deputy Secretary of Defense, Kathleen Hicks, stated the following in a memorandum for all Senior Pentagon Leadership, Combatant Commanders, Defense Agency, and DoD Field Activity Directors,

“Data is a strategic asset. Transforming the Department of Defense (DoD) to a datacentric organization is critical to improving performance and creating decision advantage at all echelons from the battlespace to the board room, ensuring U.S. competitive advantage. To accelerate the Department’s efforts, leaders must ensure all DoD data is visible, accessible, understandable, linked, trustworthy, interoperable, and secure...

Maximize data sharing and rights for data use: all DoD data is an enterprise resource...

Implement industry best practices for secure authentication, access management, encryption, monitoring, and protection of data at rest, in transit, and in use...

Data is essential to preserving military advantage, supporting our people, and serving the public. **Leaders at all levels have a responsibility to manage**, understand, and responsibly share and protect data in support of our shared mission.”

**SYMANTEC DATA
LOSS PREVENT SUITE
DELIVERS A SINGLE
CONSOLE FOR POLICY
MANAGEMENT AND
ADMINISTRATION ACROSS
ALL COMMUNICATION
CHANNELS TO ALLOW
OPERATORS TO WRITE
ONCE AND PUBLISH
EVERYWHERE.**

*“Data is a strategic asset. Transforming the Department of Defense (DoD) to a datacentric organization is critical to improving performance creating decision advantage at all echelons from the battlespace to the board room. **Leaders at all levels have a responsibility to manage, understand, and responsibly share and protect data in support of our shared mission.”***

Kathleen Hicks,
United States Deputy Secretary of Defense

From the highest echelons of government, organizations are being directed through documents such as the President’s National Cyber Strategy and DoD Cyber Strategy, to protect the U.S. competitive advantage through fiercely protecting data. Meeting these directives head-on, the USAF has been approaching the problem set of *protecting USAF data* several ways—one of which being the contract award of an Enterprise Data Loss Prevention (E-DLP) Pilot.

USAF E-DLP Pilot

Beginning on September 28, 2020, and running through May 31, 2021, the vendor team (Iron Bow, Broadcom, and Infolock) worked in conjunction with the USAF’s Air Combat Command to conduct a Pilot of an E-DLP system at JBSA-Lackland. The primary purposes of the E-DLP Pilot were to deploy and integrate a candidate E-DLP capability for evaluation by the USAF, specifically the 68th Network Warfare Squadron (68 NWS), to identify and protect USAF sensitive information, build a framework for a DLP Program, and functionally validate that the capability meets the technical requirements. The E-DLP capability provides central security policy management and orchestration from JBSA-Lackland, while ensuring data monitoring and protection for data-at-rest, data-in-motion, and data-in-use. Insider Threat (InT) was an additional stakeholder of the pilot as information about data loss and risky user behavior is essential to their mission.

Selected Candidate for Pilot was Symantec® Data Loss Prevention Suite

The selected candidate for the E-DLP Pilot contract award was Symantec® Data Loss Prevention (DLP) suite, which provides a comprehensive, widely adopted, and trusted solution for data monitoring and protection. It delivers a single console for policy management and administration across all communication channels (web, email, endpoints, storage, and cloud) to allow operators to write once and publish everywhere. Symantec DLP integrates with a wide range of other solutions, adapts to evolving architectures, and is capable of scaling to the USAF size and complexity of a full enterprise deployment.

NEAR THE CLOSE OF THE PILOT, MEMBERS OF THE GOVERNMENT ASSESSMENT TEAM STATED THAT THE CANDIDATE SYMANTEC CAPABILITY DEMONSTRATED ADVANCED DETECTION CAPABILITIES AND WAS POSTURED TO SIGNIFICANTLY ENHANCE THE CURRENT SUITE OF CAPABILITIES COMPROMISING THE WEAPON SYSTEM.

The E-DLP system that was deployed at JBASA-Lackland consisted of contractor-owned, government operated (COGO) physical hardware equipment and licensing, Symantec-specific DLP training, and cyber security services. During the Pilot, the vendor team assisted the USAF with building a notional organizational E-DLP Program and obtaining an Interim Authority to Test (IATT) to evaluate the efficacy of the Symantec DLP platform over the Pilot period.

Understanding that the USAF desires to shift toward a Zero Trust architecture, every capability needs to demonstrate how it aligns with that strategy. The following brief details the E-DLP pilot's accomplishments and how E-DLP will fit into the USAF's Zero Trust architecture moving forward.

E-DLP Pilot Success Story

The USAF's E-DLP Pilot, sponsored by the 688 CW, was a resounding success. Working in concert with the 68 NWS, the vendor team was able to demonstrate that the capability can be deployed on the AFNET, and not only meet, but exceed the technical requirements. Beginning the pilot with project kickoff and stakeholder interviews, post IATT, the vendor team was able to quickly deploy, configure, and integrate the Symantec DLP capability into the AFNET. The project and vendor team successfully deployed endpoint agents, network sensors, as well as Symantec Insider Threat/User and Entity Behavior Analytics (UEBA) capability (Information Centric Analytics) to provide USAF Cyber Operators with a proactive view of risk analyzed through user actions considered outside the realm of normal, daily activity.

Once the capability was successfully installed into the AFNET, the 68 NWS and vendor team executed rigorous functional testing to validate each of the DLP capability components. After completion of the functional validation testing, the vendor team was able to successfully communicate to the USAF that each capability component was functioning as expected within the AFNET, and properly integrated into the USAF's environment. Near the close of the pilot, members of the government assessment team stated that the candidate Symantec capability demonstrated advanced detection capabilities and was postured to significantly enhance the current suite of capabilities compromising the weapon system.

Over the course of the eight-month pilot, the combined vendor and USAF Team successfully met all communicated requirements. Particularly, the E-DLP Pilot achieved the following goals:



Validation:

- Validated E-DLP capability functionality with the USAF Statement of Objectives.
- Reviewed USAF governance documentation.
- Architected capability to work within USAF.
- Obtained IATO for the E-DLP Pilot.



Program development:

- Interviewed key USAF stakeholders.
- Prepared the E-DLP Program Report and delivered recommendations.
- Created E-DLP policies and conducted use case testing within the Pilot environment.
- At the end of the E-DLP Pilot, the vendor team provided inputs to the USAF for the USAF's Pilot's After-Action Report (AAR).



Implementation:

- Core E-DLP capability components Symantec DLP, ICA, ICDx, and SSLV.
- Deployed E-DLP Endpoint agents to 100 user systems.
- Integrated networks with Symantec Security Analytics (Solera) and endpoint with HBSS.



Configuration:

- Network traffic monitoring for the transmission of sensitive data.
- Scanning file shares for sensitive data at rest.
- Agent-based monitoring for sensitive data on user systems.
- Events feeding into ICA for insider threat.



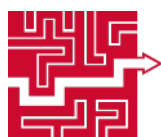
Asset development:

- Provided documentation to guide ongoing development.
- Created a recommended incident response workflow for managing and remediating E-DLP incidents.



Training:

- Provided customized training to administrators, policy authors, incident responders, and insider threat teams.
- Conducted show and tell sessions with demos and Q&A.
- Completed knowledge transfer during work sessions.



Backout plan:

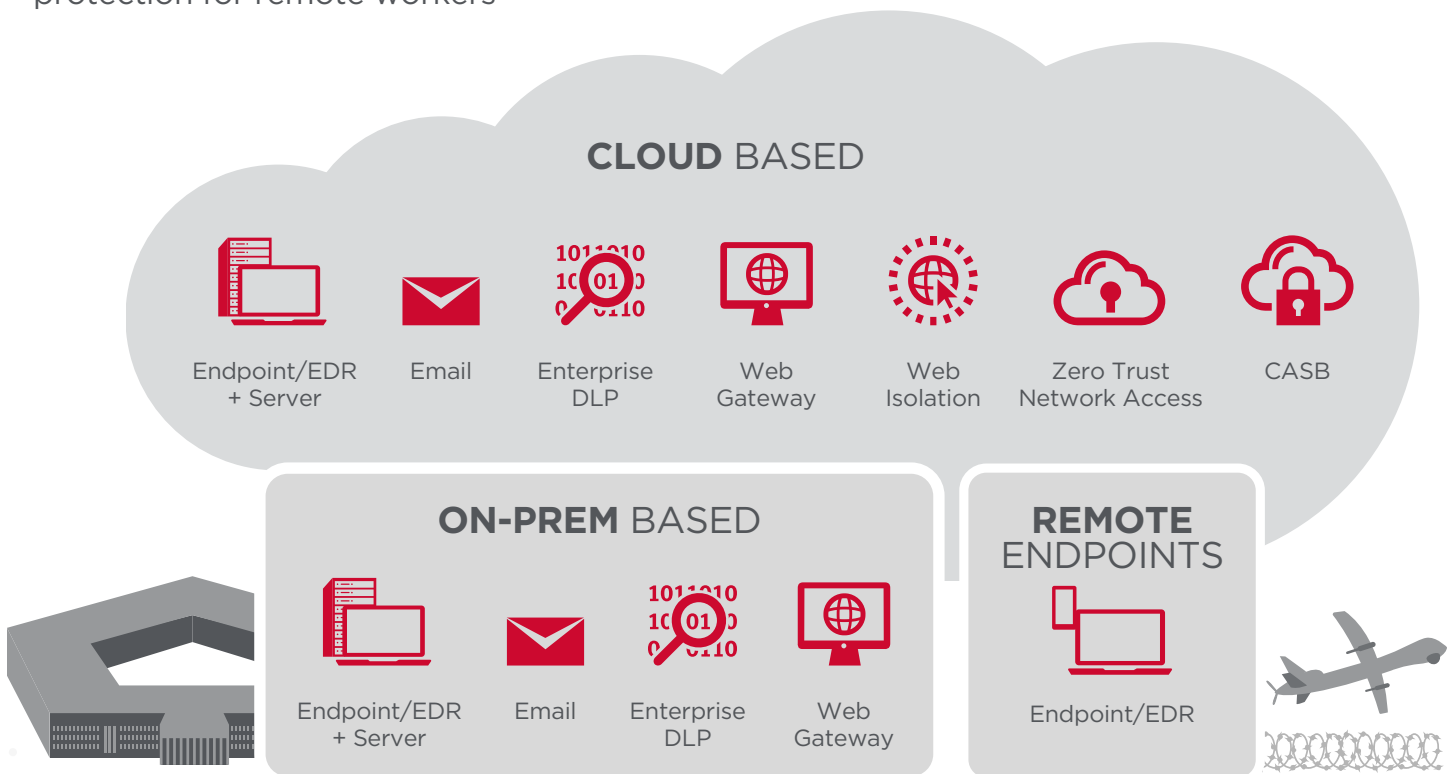
- Proving the capability can be provided to the USAF truly *as a platform*. The vendor team was able to successfully remove the capability from the USAF environment at the conclusion of the Pilot with zero impact to the AFNET.

How E-DLP Fits into the USAF's Zero Trust Strategy

Zero Trust architectures are based on the principle of *trust no one, verify everything*. It abolishes the idea of a trusted network within a security perimeter and requires companies to create centers of control around sensitive data. With this in mind, E-DLP not only fits within Zero Trust, it is an essential component of it because E-DLP discovers, monitors, and protects sensitive data on the endpoint, storage, network, email, and cloud. Zero Trust provides access to the data, DLP protects it.

Symantec Cyber Security Data-Centric, Hybrid-Enabled Platform

Industry-leading SASE solution with comprehensive endpoint protection for remote workers



**ZERO TRUST AND DLP
WILL HELP AIRMEN BUY
INTO THE FACT THAT
DATA PROTECTION IS
EVERY AIRMAN'S MISSION
AND PLAY AN ACTIVE
ROLE IN SUPPORTING
DATA RISK REDUCTION IN
THE USAF**

Airmen need to work with data, even sensitive data, and sometimes move it outside an organization. For example, an Airman might need to send PII data for personnel or other mission objectives. However, that Airman would not need to send that data to an unauthorized recipient or save it to unauthorized locations. Symantec DLP stands guard over sensitive data by monitoring, automatically discovering, and enforcing protective measures such as encryption, blocking, and preventing it from leaving the enterprise in unwanted or non-compliant ways

Symantec DLP does not stop there, it enables you to surveil behaviors relating to suspicious user behavior and prevent exfiltration of sensitive data. Symantec DLP can be configured to identify any type of sensitive information, enabling you to track its use and location, and regulate its flow. DLP integrates with the evolving USAF architecture and is scalable to meet the needs of an organization of its size and scope.

Working hand-in-hand with DLP, Symantec Information-Centric Analytics (ICA) implements UEBA, providing AI-and ML-enabled insight into user behavior. Every Airman has a normal working behavior pattern, which ICA observes, records, and compares to that of Airmen with similar responsibilities. When an Airman's behavior, or usage of a system, departs from the normal pattern, ICA takes note and assigns a risk score and reports to Insider Threat.

Zero Trust is not a silver bullet. It is a process that is best implemented with the goal of data protection at its core. Measures must be put in place and then enforced so they become part of a daily routine for all Airmen. When Airmen sense that complying with cumbersome security measures makes getting their jobs done more difficult, they are likely to work around those measures, using shadow IT applications and taking work to unsecured locations. Zero Trust and DLP will help Airmen buy into the fact that *data protection is every Airman's mission* and play an active role in supporting data risk reduction.





Data is a strategic asset and needs to be protected. As the USAF transforms to a data-centric organization and moves toward a Zero Trust architecture, make sure that Symantec DLP and ICA are part of the solution.

Conclusion

As required by the DoD, the USAF must implement information security controls vital to safeguarding sensitive, protected, and classified data from falling into the wrong hands. Like other national security interests, the USAF must protect its data by utilizing a purpose built, proven solution. Mitigating the risk of data breaches, account takeover fraud, lateral movement attacks, and shadow IT, Symantec DLP delivers the highest level of protection to mitigate data breach and compliance risks. Symantec DLP, providing enterprise-wide and fully integrated data loss prevention will ensure that the USAF’s data is protected from the moment it is created and throughout the entirety of its lifecycle. Symantec DLP delivers a world-class data access and protection platform, providing visibility and control of information everywhere it goes.

As described throughout this document, the Symantec division of Broadcom has a DLP technology that meets all of the USAF’s E-DLP requirements. Providing exactly the versatility needed for the USAF’s ever evolving networks, Symantec DLP discovers, monitors, and protects sensitive data across all endpoints, networks, data centers, and cloud applications. Integrating data monitoring, protection, and access control policies, Symantec DLP ensures consistent and always-on protection that follows the data—wherever it goes, on whatever device.

In summary, DLP will provide the USAF with the following key benefits:

| | |
|---|--|
|  | Keeps confidential data safe from unauthorized exposure or exfiltration by insiders |
|  | Reduces risk of operational disruption, reputation damage, and financial loss arising from data breaches |
|  | Accelerates digital transformation initiatives by enabling enterprises to consume cloud services securely |
|  | Facilitates compliance with a multitude of data protection laws and regulatory requirements |

While delivering coverage for all communication channels (endpoints, web, email, storage, and cloud) the Symantec solution also simplifies management and reporting by streamlining workflow, processes, and procedures for USAF operators. Through an integrated management console (the Enforce platform), the Symantec solution allows for a single policy set to be deployed and enforced across all Symantec DLP sensors. With Symantec DLP, the USAF will undoubtedly be able to determine where its data resides and monitor its use, while also keeping it safe from accidental, negligent, or malicious data loss.



About Symantec

As part of Broadcom, Symantec helps organizations and governments secure against threats and compliance risks by protecting their users and data on any app, device, or network. The Symantec Integrated Cyber Defense approach simplifies cyber security with comprehensive solutions to secure critical business assets across on-premises and cloud infrastructures.



About InfoLock

Experts in data governance, InfoLock provides specialized consulting and advisory services that help organizations effectively discover, manage, and protect their data. Our deep understanding of risk management, combined with technical expertise with business acumen, makes us the ideal partner to help you regain control of your data.



About Iron Bow Technologies

Iron Bow Technologies has 35 years of exceptional technology implementation, customer experience, and full spectrum technology support across all USAF MAJCOMs worldwide. The Air Force Team has delivered USAF enterprise program capabilities for DCGS, RPA SOC, TDC, SCE, PKI Validation, Proxy system, WIN10, DRSN, and is proud to support the EDLP effort.