SYMMETRY

WHITE PAPER

Federal Government

With the largest, most complex, and decentralized networks comprising over 100 agencies, the US Federal government has more data systems than any organization in the world. It accounts for a larger percentage of domestic data breaches each year, in part due to a shortage of skilled cybersecurity professionals and manual efforts prone to delay and errors. In 2021, Thales reported that 47% of federal government respondents experienced a breach in the prior 12 months. Major data breaches, such as the Solarwinds Breach in 2020, surfaced the urgent need for better cyber threat visibility.

Breaches are increasing in number, strength of impact, and attack effectiveness against federal, state and local governments, military organizations, and educational institutions. Traditional network defenses have focused on preventing intrusions, but attackers continue to evade them. Federal government cybersecurity teams need to establish data security practices to protect their data, their most critical asset.

Federal Government Data Security Challenge: Protecting Classified Data

TRANSITION TOTHE CLOUD

The move to the cloud continues to compound this challenge. Federal agencies must satisfy the requirement of moving data from unclassified, sensitive, and classified enclaves while ensuring that secure access to sensitive data can be maintained. The Data Center and Cloud Optimization Initiative (DCCOI) sets aggressive targets for IT transformation projects, which also apply to 300,000 Defense Industrial Base organizations assisting the modernization of cybersecurity.

ATTACK VOLUME AND VELOCITY

Ransomware attacks have been growing in volume and in effectiveness over the past few years. In 2020, 44% of global ransomware attacks targeted municipalities alone. Over the past 3 years 246 ransomware attacks have been on the U.S. government, costing taxpayers around $51 billion. Ransomware by nature seeks to take control of data and a lot of times organizations aren't able to evaluate if the data is sensitive, protected, or mission critical. In order to properly evaluate the risk or or impact of ransomware attacks, federal government organizations need to classify their data. They also need to have data security measures in place to make sure that ransomware actors cannot move laterally across cloud data stores, picking and choosing the data they consider worth holding for ransom.

Data Security Best Practices with Cloud Adoption

Execute the Cloud First directive per Federal and DoD Data Strategy while satisfying the regulatory requirements by DCCOI, Cybersecurity Maturity Model Certification (CMMC), FedRAMP, FISMA, CSA STAR, CIS Standards, NIST 800-53, NIST 800-171, etc.

Fill the growing cybersecurity skill gap with automation and enable security teams to effectively identify and respond to data anomalies.

Gain better visibility into the security posture of government data spanning across data stores, databases, and data lakes in hybrid cloud environments.

Symmetry Systems DataGuard

Symmetry's platform is engineered specifically to address modern data security and privacy challenges at scale from the data out, providing organizations the ability to innovate with confidence. With total visibility into what data you have, where it lives, who can access it, and how it's being used, Symmetry safeguards your organization's data from misuse, insider threats, and cybercriminals, as well as unintended exposure of sensitive IP and personal information through use of generative AI technologies.

WHAT WE DO

Symmetry offers comprehensive visibility and control over your data, addressing all aspects of your data security requirements, including the full spectrum of functions outlined in the NIST Cybersecurity Framework.

Identify

Discovers, classifies, maps, and monitors sensitive data across cloud, on-prem, and hybrid environments.

Detect

Identifies and creates alerts for abnormal data behaviors and data policy violations in real-time.

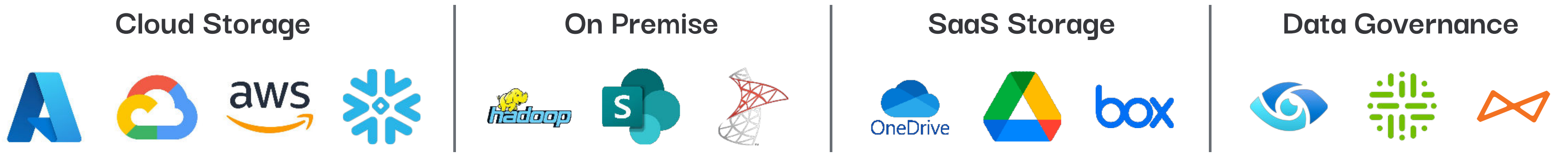
Protect

Discovers, classifies, maps, and monitors sensitive data across cloud, on-prem, and hybrid environments.

Respond & Recover

Contain the security and business impact of compromised identities and impacted data with speed and precision.

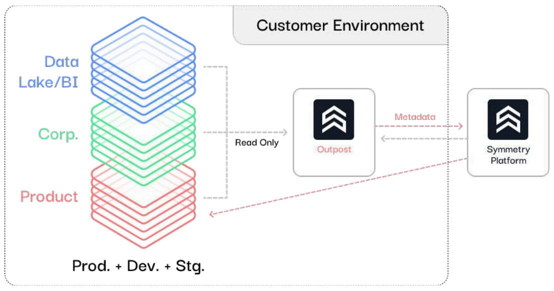
INTEGRATION INTO YOUR MODERN DATA+AI SECURITY STACK



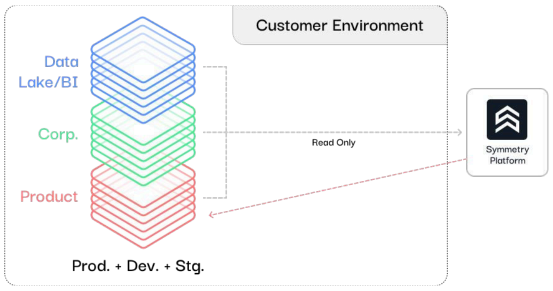
FLEXIBLE DEPLOYMENT MODEL FOR YOUR ENVIRONMENT

Our deployment model is tailored to your operational needs and risk appetite. Whether it's air-gapped, fully in your cloud, traditional SaaS, or hybrid-cloud – we have done it.

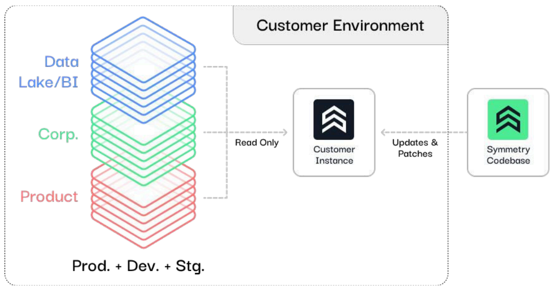
SaaS Model



Outpost Model



Air-Gapped/In-Your-Cloud Model*


Customer Environment
Data Lake/BI
Corp.
Product
Read Only
Customer Instance
Updates & Patches
Symmetry Codebase
Prod. + Dev. + Stg.