COMMVAULT

WHITE PAPER

Ensuring Operational Readiness with a Data-Led Approach to Zero Trust

Leveraging FedRAMP High solutions to accelerate the path to ZTA

Overview

Government agencies, like any other modern organization, run on data. To accomplish their mission, employees need easy access to the right data at the right time, and many government services must ensure citizens have access to services virtually. Rising cyberthreats and growing concerns about privacy amplify the data readiness challenge for agencies needing to find ways to keep data secure without impeding operational readiness. Balancing access against data protection can be an extremely difficult balance to strike. This challenge is at the heart of the emerging zero trust architecture (ZTA) as the definitive security model for the digital age.

One of the core tenets of ZTA is providing the right level of access to the right people in the right context while rooting out excess or outdated access rights – the concept of least privilege. But what happens in practice can be a different story. While government agencies focus on implementing ZTA as a key cybersecurity objective, actual operational readiness is much greater than compliance checklists. What really matters is the practical, real-world implementation of ZTA, protecting critical data and ensuring necessary data access to support the mission.

To date, many white papers addressing ZTA have focused on credentialling: identifying users and their privileges using technologies such as identity and access management (IAM), customer identity and access management (CIAM), identity governance and administration (IGA), privileged access management (PAM), and so on. But users are only part of the people, process, and technology enterprise picture. To protect and manage data effectively, agency leaders first must be able to understand their data in context – what it is, how it's used, why it is collected, and who should be allowed to access it and under what circumstances, from what locations, and at what times. Moreover, the dynamic nature of modern data, constantly created, changed, and moved, makes contextualizing data an even more significant challenge than managing user identities and privileges.

> **To protect and manage data effectively, agency leaders first must be able to understand their data in context – what it is, how it's used, why it is collected, and who should be allowed to access it and under what circumstances, from what locations, and at what times.**

This complex real-time data environment is driving intelligent data management to become a vital component of the strategy to operationalize ZTA. In fact, the U.S. Department of Defense Zero Trust Strategy released in November 2022 recognizes efficient data management, including visibility, global access, robust end-to-end encryption, data tagging, and ease of use, as fundamental to technology acceleration and identified it as one of the key ZTA pillars.

This white paper will address the role of intelligent data management and data protection in ZTA and how it drives operational readiness.

Ensuring data security while driving digital transformation

Government agencies face relentless, often conflicting pressures to advance digital transformation without increasing risk. Citizens and organizations expect near real-time virtual access to a wide range of government services with perfect data. Congress demands that government agencies leverage emerging technology, automation, and cloud technologies to improve operational efficiency. Meanwhile, government security experts convey that cyberattacks continue exploiting existing technical and procedural gaps and vulnerabilities. Attempts at rapid innovation all too often end up exacerbating the risk agencies face.

Security technologies and solutions play a large part in managing risk and reducing vulnerability. Data encryption can safeguard data at rest and in transit – augmented with key management tools to ensure that data can be decrypted only by the right people and systems in the right circumstances. Authentication, authorization, and accounting (AAA) controls help agencies manage and track how user privileges to data access are granted. The National Institute of Standards and Technology (NIST) Privacy Framework offers guidance to identify and manage privacy risks while building innovative products and services. When all else fails, recovery point objectives (RPOs) and recovery time objectives (RTOs) set targets for restoring user access to data following a breach or system failure. Again, great guidance that needs context within an agency.

As agencies focus on realizing the benefits of cloud and digital transformation, they must recognize how fundamental human behavior often poses the most significant risk factor. The rise of remote work and ongoing cloud migration further amplify new dimensions of vulnerability to existing gaps, such as long-standing imperfect security practices by individuals. Within this complex, fast-paced, ever-changing environment, ZTA aims to provide that data framework for agencies to secure high-value data and mission-critical applications while still allowing people the needed privileges to get their work done.

Enabling secure productivity with zero trust architecture

ZTA offers protection without hindering productivity. In a recent GovLoop government industry webinar, Dr. Amy Hamilton, Senior Cybersecurity Advisor of Policy and Programs at the U.S. Department of Energy (DoE), explained the advantages of this model over a traditional hardened security perimeter using the analogy of defending a castle with a moat and drawbridge. While barring access can succeed in preventing attacks on critical resources, it fails to improve operational security. A castle sealed off from its village can no longer perform its essential governing services for those who depend on it. Operational readiness in this context means agencies must be able to continue delivering services, interacting with constituents, and working with data even while under threat of attack: a threat that, in today's world, means ransomware, insider threat, malware, and data exfiltration if security fails.

In the same session, Dovarius Peoples, CIO, U.S. Army Corps of Engineers (USACoE), highlighted ongoing work by the USACoE Advanced Operational Engineering Research Center, which evaluates and validates emerging capabilities from industry in the context of ZTA. Both speakers observed that, as the federal government continues its journey to the cloud, understanding the fundamentals of data management and ZTA is critical. Access management, the immutability of critical data and applications, data management both on-premises and in the cloud, and ease of use will be critical success factors for the next generation of data protection modernization.

If ZTA offers a path to data protection in a virtual world, the question becomes how to achieve it. As originally defined by thought leader and former Forrester Research analyst John Kindervag, zero trust incorporates measures such as building continuous authentication and authorization into the fabric of the organization, adhering to the principle of least privilege, limiting movement through micro-perimeters and micro-segments, and deploying multilayered, integrated security technologies such as antivirus, next-generation web firewall (AGWAF), data loss prevention (DLP), SSL/TLS encryption, and others. However, approaching zero trust as a compliance checklist can fail to ensure true operational readiness – achieving real-world data protection within the operational context of delivering government services to citizens.

> **"Zero Trust is a cybersecurity strategy designed to resonate to the highest levels of any organization yet be tactically implantable using commercially available technology."**
> John Kindervag Creator of Zero Trust, SVP, Cybersecurity Strategy | ON2IT

Building intelligent data management as part of zero trust

Issued in May 2021, Executive Order 14028, Improving the Nation's Cybersecurity, spurred a heightened focus on cybersecurity, including a discussion of the necessity and design of zero trust architecture (ZTA) for government agencies. The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security followed up with additional guidance, noting that the path to zero trust is an incremental process that will take years to fully implement.

Simply put, data security has to be an integral component from the outset as part of real-time service delivery. Rapidly establishing trust in a virtual environment, in a dynamic manner, for each new session is a fundamental zero trust mechanism. To function effectively in real-time operations, ZTA depends on user credentialing and synchronization with comprehensive data management.

User credentialing

Secure data access begins with determining who should have the rights to access specific data and how to manage that access in each instance, as responsibilities can be both role-based and situation-based. ZTA manages these instances through the presentation of user credentials that validate the individual's identity and role, as well as the circumstances in which access is requested, AND includes some protection measures to prevent these credentials from being spoofed or corrupted.

While a robust identity and access management ecosystem drives compliance on a theoretical level, operational readiness depends on a more nuanced and dynamic real-time understanding of the data and applications being used. Agencies must first get a handle on specific data sets and how they drive operations – and then use this knowledge to architect the network to support the scale, speed, and global reach needed to deliver secure access at today's unprecedented operational tempo.

Data context

Not all data is created equal. Highly sensitive data calls for a higher level of protection and more tightly restricted access, while less critical information can be shared more widely without introducing excessive risk. While a very common-sense observation, this determination helps drive the definition of least privilege in a ZTA context. Do people in a given role truly require access to a given data set, or is it merely a nice-to-have? How strictly should necessity be defined? ZTA can outline the premise of these questions, but agency operational leaders teamed with data experts are the key to answering them.

ZTA security parameters and operational priorities drive the answers. As mentioned previously, both factors depend on a solid understanding of the data and applications in question. Who is creating the data, and what business process does it enable? Where and how is the data stored and indexed? Is the exchange of data bi-directional, as new information is created? Intelligent data management provides this context for data, including characteristics such as:

- Access control policies (both location and individual)
- Time of data creation
- Keyword elements
- Compliance assessment (e.g., does the data include a social security number)
- Encryption status in flight and at rest

When these data characteristics complement mission priorities from agency leaders, operational readiness and resilience can be realized and achieve ZTA goals. For example, while timecard data, supply chain data, and data on the location of repair parts all support agency operations, they differ significantly in their direct impact on operational readiness: The inability to access timecard data – an inconvenience; finding a certified replacement part for a critical equipment failure – operational failure.

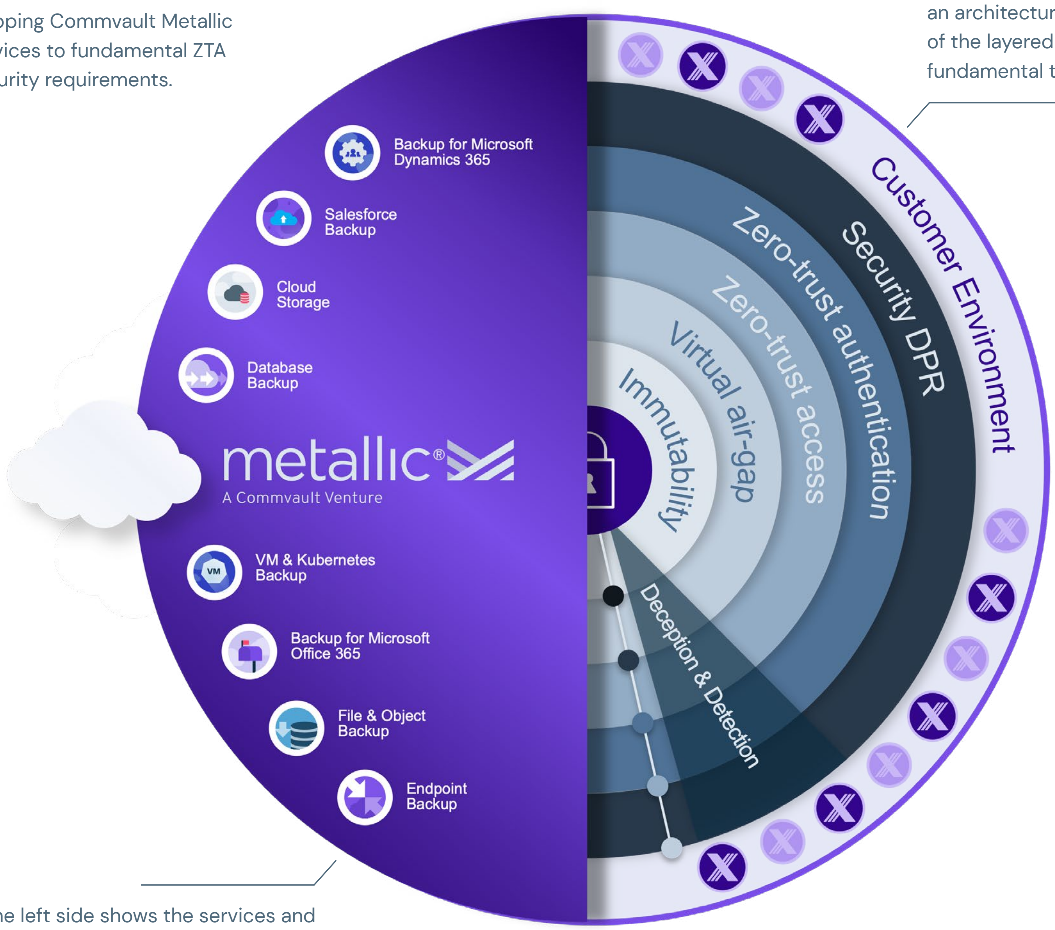
Implementing ZTA in the Government

The successful and smooth evolution to ZTA in government will depend on collaboration between agencies and industry partners. Agencies can learn from industry best business practices developed for ZTA, and in turn, industry vendors can understand an agency's digital criteria for operational readiness. Integrating both allows an agency to create a roadmap to implement critical zero trust architectural requirements.

As a real-world example, the diagram below provides a holistic view of many of the concepts outlined in this paper, supporting the data pillar of ZTA.

FIGURE 1

Mapping Commvault Metallic services to fundamental ZTA security requirements.



The right side of the diagram presents an architectural view of key components of the layered security requirements fundamental to the ZTA data pillar.

The left side shows the services and capabilities agency teams need to have available – the operational drivers of their organization's operational ecosystem.

Existing industry solutions, such as those from Commvault, provide a practical model for government agencies with comprehensive data management and protection. For example, Metallic Government Cloud – built by Commvault – was specifically developed to meet FedRAMP High standards – capable of meeting the most stringent confidentiality, integrity, and availability standards recognized by the U.S. government, allowing government agencies and federal contractors to protect data at every stage of digital transformation and cloud adoption journey.

Supporting better data protection and, more importantly, rapid recovery of mission-critical data begins with broad visibility using an intuitive enterprise data dashboard to ensure that important data is actively managed and protected. Monitoring within this context enables the identification of any abnormal activity, potentially identifying a ransomware event or even an insider threat. By using a single comprehensive dashboard for protecting data and workloads that may be running on a wide variety of different infrastructure instances – IT/SecOps teams need only one data management tool across the enterprise. Comprehensive visibility is fundamental to identifying the time of an anomalous event, impacted files, impacted devices, and individual accounts and provides a simple, effective means to rapidly restore clean data. The methodology allows for a highly automated recovery process to reduce the time needed to get up and running. The automated tools also allow for the granular deletion of any compromised files, attachments, or emails when properly validated by government IT/SecOps teams.

> **By using a single comprehensive dashboard for protecting data and workloads that may be running on a wide variety of different infrastructure instances – IT/SecOps teams need only one data management tool across the enterprise.**

With the comprehensive, automated approach leveraging integrated AI, agencies can rapidly reach ZTA objectives for the Data Pillar, providing outstanding operational readiness throughout their modernization. There is an immediate positive action that agencies can put in place now to advance the ZTA to protect their data while becoming much more operationally resilient.

Metallic® Government Cloud solutions from Commvault meet FedRAMP High standards and are already operational in many Federal agencies. They are hosted on Azure Government Cloud (GCC High) and meet the most stringent confidentiality, integrity, and availability standards set forth by the U.S. government.

Agency benefits include:

- **Rapidly recover from deletion, corruption, or malicious attack**
- **Optimize operations with automated data backups and low-touch management**
- **Maintain compliance and meet regulatory SLAs**
- **Meet federally mandated data security standards and requirements**
- **No hardware, maintenance, or upfront capital investments required**

To learn more about Commvault strategies and solutions to support zero trust architecture in government agencies, request a **complementary assessment >**

COMMVAULT® Be ready™