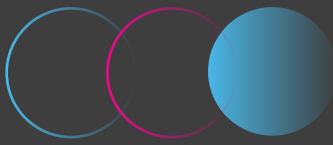


# How to Meet DHS and CISA Guidelines Supporting White House Executive Order 14028 on Improving the Nation's Cybersecurity

BY CHUCK BROOKS, PRESIDENT  
BROOKS CONSULTING INTERNATIONAL

A Call for an Inventory of All  
Data Assets as Foundational to  
Implementing a **Zero Trust Architecture**



## ABOUT THE AUTHOR

### Chuck Brooks, President, Brooks Consulting International

Chuck is a globally recognized cybersecurity and emerging technology thought leader. Chuck's extensive expertise includes serving as a two-time presidential appointee, leadership at the Department of Homeland Security, teaching cybersecurity and risk management at Georgetown University, and authoring dozens of articles on cyber tech and policy for publications such as Forbes, Huffington Post, The Hill, and many others. Chuck was named the top person to follow on Tech by LinkedIn and is the President of Brooks Consulting International. He currently serves on Anacomp's Advisory Board providing strategic guidance focusing on cybersecurity, Zero Trust, and data protection for the D3 Data Discovery solution.



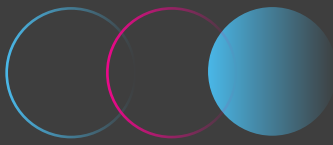
80% of critical infrastructure experienced a ransomware attack in the last year<sup>2</sup>

## ZERO TRUST: A GOVERNMENT MANDATE

Recent high-profile hacks such as SolarWinds and Colonial Pipeline (and a spate of other) have called attention to the vulnerability of critical infrastructure. The number of data breaches through September 30, 2021 exceeded the total number of events in 2020 by 17% (1,291 breaches up to Sept. 30, 2021 compared to 1,108 breaches in 2020).<sup>1</sup> Trends in sophisticated data breaches will likely continue to rise in 2022, and are often coordinated by state actors.

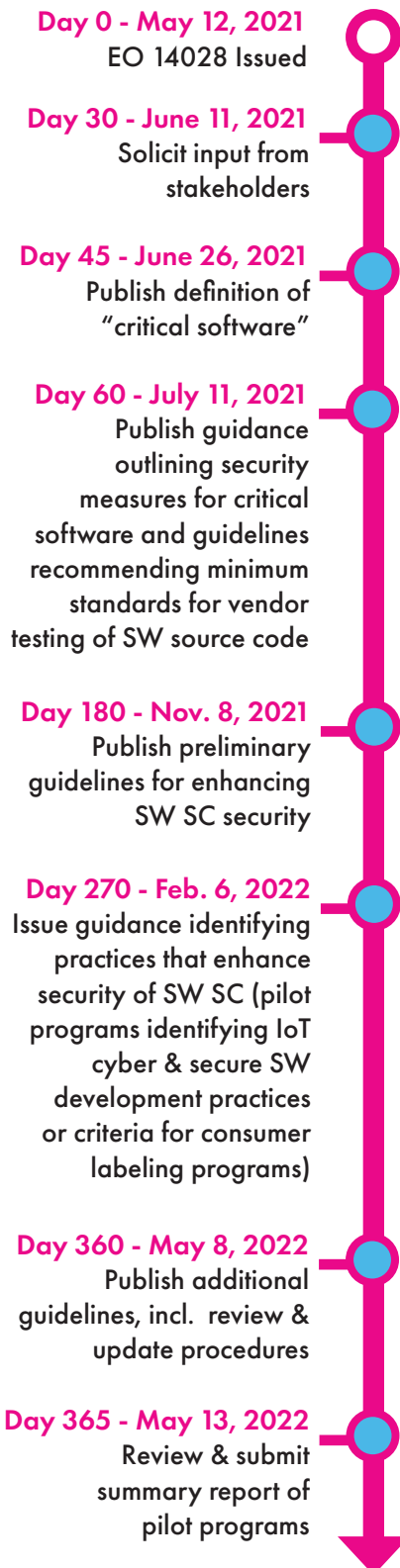
As a result of too much sensitive data at risk in government agencies and in the private sector, the **White House issued Executive Order (EO) 14028, "Improving the Nation's Cybersecurity" on May 12, 2021.**<sup>3</sup> The EO was essentially a call to action to devise a strategy and modernize to meet the new threats impacted by greater connectivity in the digital ecosystem that fuels the engine of national security and our economy. This strategy has centered around the concept of Zero Trust Architecture.

- 1 Dan Lohrman, "Data Breach Numbers, Costs and Impacts All Rise in 2020," Government Technology, Oct. 10, 2021, [www.govtech.com/blogs/lohmann-on-cybersecurity/data-breach-numbers-costs-and-impacts-all-rise-in-2021](http://www.govtech.com/blogs/lohmann-on-cybersecurity/data-breach-numbers-costs-and-impacts-all-rise-in-2021)
- 2 Claroty, "The Global State of Industrial Cybersecurity 2021," 2021, [security.claroty.com/report/global-state-industrial-cybersecurity-survey-2021](http://security.claroty.com/report/global-state-industrial-cybersecurity-survey-2021)
- 3 Executive Order on Improving the Nation's Cybersecurity, The White House, May 12, 2021, [www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/](http://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/)



# EXECUTIVE ORDER 14028

## NIST Guidance Ordered by EO 14028



## WHAT IS EXECUTIVE ORDER 14028?

White House executive orders are usually issued with a sense of urgency. This is the case for EO 14028. In essence, it is a new and evolving road map for cybersecurity that will hold government agencies accountable to fortify their defenses and capabilities to address cyberthreats. The concept of meet existing and future cyber challenges is being formulated in a "Zero Trust Architecture."

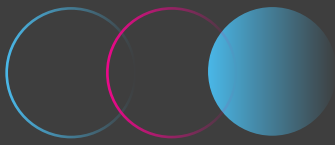
According to **Cybersecurity and Infrastructure Security Agency (CISA)**, EO 14028 pushes agencies to adopt Zero Trust cybersecurity principles and adjust their network architectures accordingly. To help this effort, CISA developed a **Zero Trust Maturity Model** to assist agencies as they implement zero trust architectures.

The maturity model complements the **Office of Management and Budget's (OMB) Zero Trust Strategy**, designed to provide agencies with a roadmap and resources to achieve an optimal Zero-Trust environment.

According to the **National Institute of Standards and Technology (NIST)**, Section four of EO 14028 directs NIST to solicit input from the private sector, academia, government agencies, and others and to identify existing or develop new standards, tools, best practices, and other guidelines to enhance software supply chain security. Those guidelines are to include:

- criteria to evaluate software security
- criteria to evaluate the security practices of the developers and suppliers themselves
- innovative tools or methods to demonstrate conformance with secure practices

**Zero Trust is a paradigm shift in cybersecurity posture that breaks implicit trust in tools and redefines how data must be identified and protected**



## HUMANS TRUMP NETWORK SECURITY

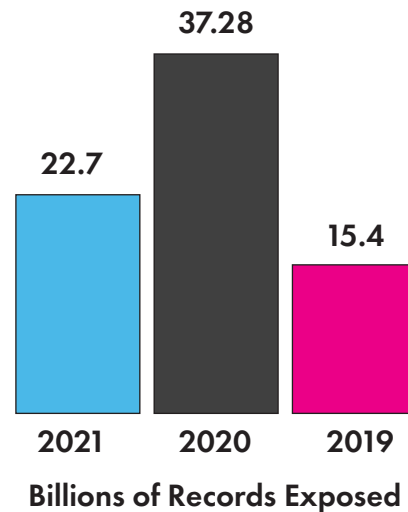
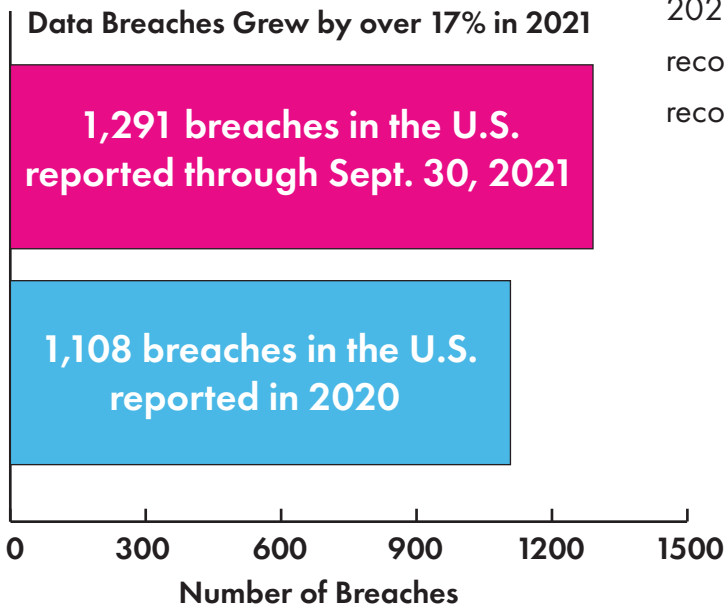
Zero Trust is a paradigm shift in cyber defense strategy away from trust in perimeter-based network security, to a new “Zero-Trust” approach that is data-centric, with the assumption that breaches will occur and devices and users should have least-privilege access.

Humans are often the weak link. The human element, such as social engineering, and phishing in particular, is the leading cause of breach, per the [Verizon 2021 Data Breach Investigations Report](#).<sup>4</sup>

## INCIDENTS RISE & BILLIONS STOLEN

Cybercriminals and state actors are increasingly using sophisticated methods to target employees and vulnerable systems in all sectors including critical infrastructure. As mentioned earlier, there were 1,291 data breaches through September 30, 2021, which was 17% higher than the 1,108 events in the full-year 2020.<sup>1</sup>

Although the number of records exposed decreased from 2020 to 2021, 2021 was the second highest year of records breached since 2005 with 22 billion confidential records compromised.<sup>5</sup>



<sup>4</sup> Verizon, “Verizon 2021 Data Breach Investigations Report,” [www.verizon.com/dbir/](http://www.verizon.com/dbir/)

<sup>5</sup> Risk Based Security and Flashpoint 2021 Year End Report, Data Breach QuickView, [www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/](http://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/)

Problems cybersecurity professionals said could have been prevented if their organization hadn't been short staffed<sup>6</sup>

Misconfigured systems	32%
Not enough time for risk assessment & mgmt	30%
Slow to patch critical systems	29%
Oversights in process & procedure	28%
Rushed deployments	27%
Being aware of all threats active against our network	27%

CISA's Known Exploited Vulnerabilities Catalog contains over 647 items with patch due dates

[www.cisa.gov/known-exploited-vulnerabilities-catalog](https://www.cisa.gov/known-exploited-vulnerabilities-catalog)

## STAFFING SHORTAGE CRISIS

In a perfect world, software vulnerabilities are identified quickly and get patched immediately and organizations have ample cybersecurity experts on hand to do the job. Unfortunately, this is not the reality.

With “**The Great Resignation**” of 2021 leading to record employee turnover and demand for cybersecurity professionals outpacing supply, proactively managing risk is a huge challenge. According to the [\(ISC\)<sup>2</sup> 2021 Cybersecurity Workforce Study](#), 67% of cybersecurity professionals reported a cybersecurity workforce shortage at their organization.<sup>6</sup> The same study found that 60% of these professionals believe their organization is at extreme or moderate risk of a cyberattack due to staffing issues.

## SUPPLY CHAIN VULNERABILITIES

Software supply chain risk has become a focal point of weakness within cybersecurity after multiple high-profile attacks. The **SolarWinds** malware-poisoned software update in spring 2020 led to the compromise of federal agencies and many well-known enterprises.

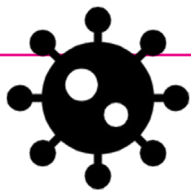
Then, cybersecurity staff received the most unwanted gift of 2021 when the high-risk **Log4j** vulnerability was identified in late November 2021 and federal agency cyber staff were ordered to patch by Christmas. Log4j may continue to be with us for some time, [per the testimony](#) of Apache Software Foundation President David Nalley to the Senate Homeland Security & Government Affairs Committee in February, 2022.<sup>7</sup>

According to an [Anchore survey](#), nearly a third of respondents (30%) were either significantly or moderately impacted by a software supply chain attacks in 2021. Log4j was a factor in increasing attacks, with 65% of respondents saying they had suffered a software supply chain attack after December 9 versus 55% before that date.<sup>8</sup>

6 (ISC)<sup>2</sup> 2021 Cybersecurity Workforce Study, [www.isc2.org/Research/Workforce-Study#](https://www.isc2.org/Research/Workforce-Study#)

7 David Jones, “Apache tells US Senate committee the Log4j vulnerability could take years to resolve,” *Cybersecurity Dive*, Feb 9, 2022, [www.cybersecuritydive.com/news/apache-senate-log4j-years/618567](https://www.cybersecuritydive.com/news/apache-senate-log4j-years/618567)

8 John P. Mello Jr., “Software supply chain attacks hit three out of five companies in 2021,” *CSO from IDG*, Feb 14, 2022, [www.csoonline.com/article/3650034/software-supply-chain-attacks-hit-three-out-of-five-companies-in-2021.html](https://www.csoonline.com/article/3650034/software-supply-chain-attacks-hit-three-out-of-five-companies-in-2021.html)



In February 2022, the FBI and U.S. Secret Service issued a [joint advisory](#) regarding BlackByte ransomware. As of November 2021, BlackByte ransomware had compromised multiple U.S. and foreign businesses, including entities in at least three U.S. critical infrastructure sectors.<sup>9</sup>

## MAL-BEARS ON THE MOVE



CrowdStrike's 2022 Global Threat Report highlighted two Russian malware adversaries known as Fancy Bear and Cozy Bear. Fancy Bear has shifted tactics to focus less on malware and more on credential-harvesting tactics. Cozy Bear is highly proficient in post-exploitation tactics for lateral movements within cloud environments, and has been identified using authentication cookie theft to bypass multifactor authentication (MFA).<sup>10</sup>

## A NATIONAL SECURITY RISK

Ransomware and sophisticated cyberattacks are an increasing threat to both public and private sectors, with state-sponsored actors and cybercriminals targeting critical infrastructure. OT and IT systems are increasingly linked and connected to cloud or internet to facilitate remote operations, creating new risks to processes at facilities. A breach at an Oldsmar, Florida water treatment facility in February 2021, whereby the hacker changed lye levels using the plant's software, highlights the risks involved. Espionage and financial motives are at play in many attacks.

With the Russian-Ukrainian tensions mounting in January 2022, a [joint advisory](#) was issued by CISA, NSA, the FBI and international authorities on February 9, 2022 stating that in 2021, an increase in sophisticated, high-impact ransomware incidents had been observed against critical infrastructure organizations globally.<sup>10</sup> The alert stated **14 of the 16 U.S. critical infrastructure sectors were targeted** and that cybercriminals are gaining access to networks via phishing, stolen Remote Desktop Protocols (RDP) credentials or brute force, and exploiting vulnerabilities. Phishing emails, RDP exploitation, and exploitation of software vulnerabilities remained the top three initial infection vectors for ransomware incidents in 2021.

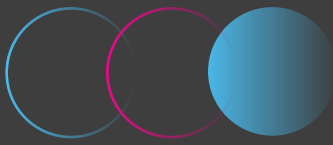
A 2022 [report by CrowdStrike](#) noted an **82% increase in ransomware-related data leaks in 2021** and ransomware-related demands averaged \$6.1M per ransom, up 36% from 2020.<sup>10</sup> The same report also found an increase in living-of-the-land attacks (LOTL), whereby cybercriminals don't write malware to the endpoint but use legitimate credentials and built-in tools to evade detection by antivirus products. Sophistication in phishing, smishing (impersonating organizations with tainted links in mobile messaging), and Man-in-the-Middle malware designed to bypass multi-factor authentication, means that the real threat of data leaks has to be assumed at all times.

9 CISA, "FBI and USSS Release Advisory on BlackByte Ransomware," Feb. 15, 2022, [www.cisa.gov/uscert/ncas/current-activity/2022/02/15/fbi-and-uss-s-release-advisory-blackbyte-ransomware](http://www.cisa.gov/uscert/ncas/current-activity/2022/02/15/fbi-and-uss-s-release-advisory-blackbyte-ransomware)

10 CISA, "Alert (AA22-040A): 2021 Trends Show Increased Globalized Threat of Ransomware," Feb. 9, 2022, [www.cisa.gov/uscert/ncas/alerts/aa22-040a](http://www.cisa.gov/uscert/ncas/alerts/aa22-040a)

11 CrowdStrike, "2022 Global Threat Report," [www.crowdstrike.com/resources/reports/global-threat-report/](http://www.crowdstrike.com/resources/reports/global-threat-report/)





**Zero Trust eliminates implicit trust in any one element and depends on real-time information from multiple sources**

## THE ZERO TRUST REQUIREMENT

With the growing sophistication of cyberattacks and ransomware, the prevalence of human errors, and a shortage of cybersecurity staff to keep pace with the rapidly changing threat landscape, White House EO 14028 states:

**“Section 3. Modernizing Federal Government Cybersecurity.** (a) To keep pace with today’s dynamic and increasingly sophisticated cyberthreat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity, including by increasing the Federal Government’s visibility into threats, while protecting privacy and civil liberties. The Federal Government must adopt security best practices; advance **toward Zero Trust Architecture**; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals.

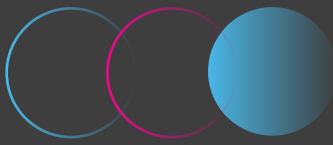
**Section 10. Definitions. For purposes of this order.** (k) the term “Zero Trust Architecture” means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The **Zero Trust security model eliminates implicit trust in any one element, node, or service** and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses.”<sup>12</sup>

## THE CISA ZERO TRUST ROADMAP

CISA’s role is to coordinate Zero Trust strategy and standards with other agencies. The **CISA Zero Trust Maturity Model** is “one of many roadmaps for agencies to reference as they transition towards a Zero Trust architecture. The maturity model, which includes **five pillars** and three cross-cutting capabilities, is based on the foundations of Zero Trust. The maturity model assists agencies in the development of their Zero Trust strategies and implementation plans and presents ways in which various CISA services can support Zero Trust solutions across agencies.”<sup>13</sup>

12 The White House, “Executive Order 14028: Improving the Nation’s Cybersecurity,” May 12, 2021, [www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/](https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/)

13 CISA, “Executive Order on Improving the Nation’s Cybersecurity,” [www.cisa.gov/executive-order-improving-nations-cybersecurity](https://www.cisa.gov/executive-order-improving-nations-cybersecurity)



## CISA'S ROLE IN EO 14028<sup>14</sup>

- 1 Remove Barriers to Threat Information Sharing Between Government and the Private Sector
- 2 Modernizing and Implementing Stronger Cybersecurity Standards across the Federal Government
- 3 Improve Software Supply Chain Security
- 4 Establish a Cyber Safety Review Board
- 5 Create Standardized Playbook for Responding to Cybersecurity Vulnerabilities and Incidents
- 6 Improve Detection of Cybersecurity Incidents on Federal Government Networks
- 7 Improve Investigative and Remediation Capabilities

## A DATA-CENTRIC APPROACH

According to the [CISA Zero Trust Maturity Model](#), "Zero Trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. The goal is to prevent unauthorized access to data and services and make access control enforcement as granular as possible.

**Zero Trust presents a shift from a location-centric model to a more data-centric approach** for fine-grained security controls between users, systems, data and assets that change over time; for these reasons. This provides the **visibility** needed to support the development, implementation, enforcement, and evolution of security policies. More fundamentally, Zero Trust may require a change in an organization's philosophy and culture around cybersecurity."<sup>14</sup>

The Zero Trust Maturity Model focuses on an evolution of implementation across five pillars, heading towards continuous monitoring and optimization over time.

**The pillars include Identity, Device, Network, Application Workload, and Data.**

## THE DATA PILLAR FOUNDATION

A foundational pillar of the new EO and the CISA Zero Trust Model is data trust. The White House stresses the need for maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components in its order.

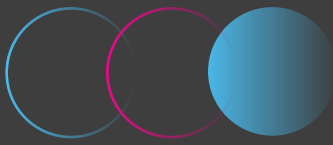
Similarly, the Data Pillar of CISA's Zero Trust Model states that "Agency data should be protected on devices, in applications, and networks. **Agencies should inventory, categorize, and label data, protect data at rest and in transit, and deploy mechanisms for detection data exfiltration.**"<sup>14</sup>

**A foundational first step in Zero Trust is an accurate inventory of all critical assets including data.**

**You can't protect what you don't know you have.**

14 CISA, Zero Trust Maturity Model, [www.cisa.gov/zero-trust-maturity-model](http://www.cisa.gov/zero-trust-maturity-model)

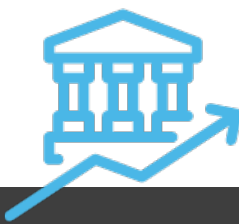




# ZERO TRUST: A DATA-CENTRIC APPROACH

## OMB Ordered Data Actions<sup>15</sup>

- 1 OMB will work with Federal chief data officers and chief information security officers to develop a Zero Trust data security strategy and associated community of practice.
- 2 Agencies must perform some initial **automation of data categorization and security responses, focusing on tagging and managing access to sensitive documents.**
- 3 Agencies must audit access to any data encrypted at rest in commercial cloud infrastructure.
- 4 Agencies must work with CISA to implement comprehensive logging and information sharing capabilities, as described in [OMB Memorandum M-21-31](#).



## THE OMB ON DATA VISION

The OMB, the agency responsible for executing (EO) 14028 elaborates on the importance of data trust and the CISA mission in the **January 26, 2022 OMB Memorandum titled, “[Moving the U.S. Government Toward Zero Trust Cybersecurity Principles](#).”**<sup>15</sup> The memo “sets forth a Federal Zero Trust Architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year 2024 in order to reinforce the government’s defenses against increasingly sophisticated and persistent threat campaigns.”

Specifically, OMB deadlines state that, “**Agencies will have 30 days from the publication of this memorandum to designate and identify a Zero Trust strategy implementation lead for their organization.** OMB and CISA will work with agencies throughout Zero Trust implementations to capture best practices, lessons learned, and additional agency guidance on a jointly maintained website at [zerotrust.cyber.gov](http://zerotrust.cyber.gov).”

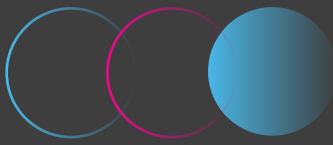
This strategy also calls on federal data and cybersecurity teams within and across agencies to jointly develop pilot initiatives and government-wide guidance on **categorizing data based on protection needs, ultimately building a foundation to automate security access rules.** This collaborative effort will better allow agencies to regulate access based not only on who or what is accessing data, but also on the sensitivity of the data being requested.

“**Agencies are on a clear, shared path to deploy protections that make use of thorough data categorization.** Agencies take advantage of cloud security services and tools to discover, classify, and protect their sensitive data, and have implemented enterprise-wide logging and information sharing.”

## THE CHALLENGES OF TACKLING ZERO TRUST DATA INVENTORY & CATEGORIZATION

The OMB memo acknowledges that “Developing a comprehensive, accurate approach to categorizing and tagging data will be challenging for many agencies. While agencies have been required to inventory their datasets for some time, a comprehensive Zero Trust approach to data management requires going beyond what agencies may be accustomed to thinking of as ‘datasets.’ Agencies must not only develop protections for the packaged datasets they store in databases or publish online, but must also grapple with more loosely structured and dispersed data systems (such as email and document collaboration) and intermediate datasets which exist principally to support the maintenance of other primary datasets.”<sup>16</sup>

15 The White House OMB M-22-09, “Moving the U.S. Government Towards Zero Trust Cybersecurity Principles,” Jan. 26, 2022, [www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf](http://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf)



## COLLABORATION & AUTOMATION

Several themes have emerged in managing cybersecurity risk in light of the rapidly evolving technology landscape, particularly in terms of the huge increase in remote and hybrid work and sophistication of cyber adversaries. Trends include **public-private collaboration** between government agencies like CISA and the developer community. Investing in **artificial intelligence and automation** technologies to improve monitoring in the face of cybersecurity staffing shortages is also a focal point.

The OMB acknowledged the challenges of identifying and managing data, and stated, “To ensure engagement and progress on tackling this challenge, the Federal Chief Data Officer (CDO) Council and the Federal Chief Information Security Officer (CISO) Council will create a **joint committee on Zero Trust data security** for federal agencies, chaired by the OMB. This committee will develop a data categorization and protection guide for federal agencies, and oversee a community of practice that can assist agencies in tackling specific areas of focus.”<sup>16</sup> Agency Chief Data Officers will be relied on to develop a system of **automating categorizations for sensitive documents to monitor and restrict how they are shared.**

Additionally, the OMB stated, “[A]utomation of security monitoring and enforcement will be a practical necessity. This capability is often referred to as **Security Orchestration, Automation, and Response (SOAR)**. . . . [T]o successfully automate security events surrounding data, systems for orchestration and permission management **will need rich information on the types of data being protected.** Agencies should strive to employ heuristics rooted in machine learning to detect anomalous behavior or categorize the data they use throughout their enterprise.”

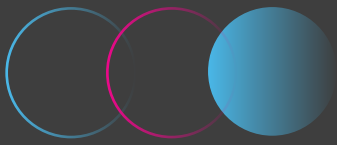
**While all pillars of the Executive Order are very important in the Zero Trust approach, it is critically important to have the capabilities of data visibility that includes an inventory of data assets (both structured and unstructured).**

Data inventory requires an optimized approach to identify, organize, and manage data assets. Simply put, it will be critical for agencies to identify what data needs to be protected, and that originates with **data discovery.**

“It’s important to have the tools, artificial intelligence or machine learning, to help you sift through this massive amount of data.”<sup>16</sup>

Kenneth Clark, Assistant Director, U.S. Immigration and Customs Enforcement

<sup>16</sup> Patience Wait, “Data is the Fuel of Digital Transformation, Officials Say,” Nextgov, Jan. 20, 2022, [www.nextgov.com/emerging-tech/2022/01/data-fuel-digital-transformation-officials-say/360957/](https://www.nextgov.com/emerging-tech/2022/01/data-fuel-digital-transformation-officials-say/360957/)

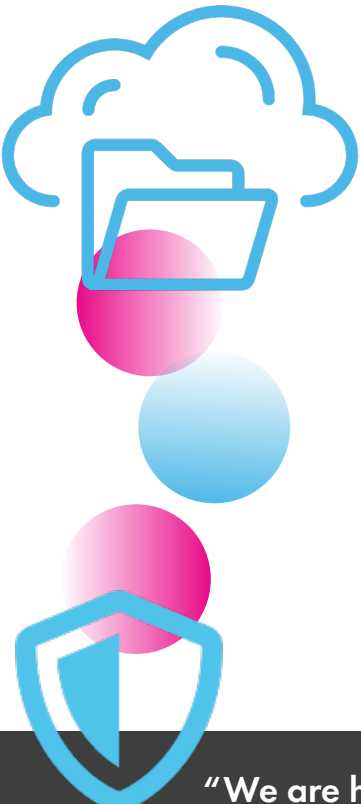


## DATA VISIBILITY IS CRITICAL TO PROTECTION

With unstructured data growing exponentially to over 80% of all data, agencies will not only have to determine what data may lie on premises or in cloud in their data centers, but also identify what is on desktops and mobile devices. Data will first have to be located during the data discovery process, and then be indexed and categorized by importance of what needs to be first protected.

In a Zero Trust model, this consists of data flows from every individual user as no one can be trusted. This component of the EO will be challenging, particularly with processing **huge volumes of unstructured data** that may be found on devices, including separate files and emails. Unstructured data may include video, audio, web server logs, and social media.

The need for identifying and protecting data has been echoed across federal agencies. Leaders need to be able to quickly be able to analyze sensitive relevant data while it is being protected through intelligent data management.



**“We are holistically, across the enterprise, in our infancy of knowing what’s in the enterprise. [If] you look over time, the sensitivity, the classification, changes . . . We have to look at a use case and see how we’re using the data, make sure we have intelligent data management in place [so] that it might not be tagged or classified at that level over time.”<sup>16</sup>**

Ron Thompson, Agency Chief Data Officer and Deputy Digital Transformation Officer at NASA

With the volume of data existing, a comprehensive process of classification would certainly need to be automated via machine learning for visibility, context, and to be granularly managed throughout the data life cycle. Also, once you know what data has been identified and needs to be protected, elements of encryption and masking can be implemented to secure it from adversaries.

According to a [Meritalk report](#), **more than 70% of federal agencies are aggressively adopting Zero-Trust principles.**<sup>17</sup> The Executive Order has made it an imperative for all agencies to begin this critical transition.

<sup>17</sup> Help Net Security, “How ready are federal agencies for zero trust implementation?,” Feb. 1, 2022, [www.helpnetsecurity.com/2022/02/01/federal-agencies-zero-trust/](http://www.helpnetsecurity.com/2022/02/01/federal-agencies-zero-trust/)



# D3 DATA DISCOVERY AUTOMATED INVENTORY



## D3 SUPPORTS EXECUTIVE ORDER 14028

Anacomp's D3 Data Discovery solution is uniquely positioned to help identify, manage, and protect data in accordance with CISA Guidelines supporting EO 14028 on Cybersecurity. Specifically, NIST and CISA guidelines call for an inventory of all data assets as foundational to implementing a Zero Trust Architecture.

**Anacomp's D3 Data Discovery & Distillation (D3) Solution** is a fast, automated, highly accurate data discovery and indexing solution that reduces data cybersecurity risks and costs for storage and compliance. D3's AI/ML discovery engine will crawl, identify, and index all data assets within all data stores.

D3 Data Discovery ingests every structured and unstructured file type and creates an "index of everything" using **AI/ML technology for unsupervised metadata tagging**. All file properties are analyzed (author, file type, creation date, etc.), encryption status identified, and lineage mapped. Risk filters enable monitoring of high, medium, and low risk data to aid in prioritizing data protection actions.

Typically within days an entire data estate will be inventoried with low burden of resources. This actionable inventory enables data tagging and segmentation for ongoing, real-time, workflow protection of at-risk data and reduction of Redundant, Obsolete, and Trivial (ROT) storage costs. Data remains in place and alerts can be set up to automatically monitor for changes to data.

**D3 identifies and inventories both privacy data and business intelligence to manage and protect the entire data estate**

**Get started on Zero-Trust data protection with D3 Data Discovery & Inventory**

**Contact Anacomp for a free consultation**

**(703) 234-3910**

**sales@anacomp.com**

**Anacomp has helped over 100 Federal agencies and dozens of Fortune 500 companies gain data visibility and insight for over 50 years**

