IDC PERSPECTIVE

Cybersecurity, Cloud Smart, and AI: Government's Toolkit for Thwarting Cybercriminals

Adelaide O'Brien

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: Cybersecurity, Cloud Smart, and AI — Government's Toolkit for Thwarting Cybercriminals

This IDC Perspective highlights three important tools in agency arsenals to thwart cybercriminals: zero trust required by an executive order, Cloud Smart to reduce the barrier of entry for cloud migrations while maintaining cybersecurity, and AI to connect diverse data sources and be able to better scope out threats.

Key Takeaways

- The shift to zero trust is driven by recent executive orders to protect agencies from ransomware, phishing, email compromise, and nation-state attacks.
- In a zero trust design, every device, user, network connection, and data exchange is authenticated and authorized.
- Cloud Smart reduces the barrier of entry for cloud migrations and plays a pivotal role in modernizing IT to improve services and accessibility and maintain cybersecurity.
- Agencies are adopting AI to connect diverse data sources and be able to better scope out threats.

Recommended Actions

- Work to gain visibility into all devices, including trusted user connectivity, device usage, and ongoing activity. Establish trust criteria and inspect devices for integrity and trust inference.
- Work with vendors that are capable of helping your agency advance in the CISA zero trust maturity model.
- To expand cybersecurity staff skills and capability, consider managed security services with various levels of support for deeper investigation analysis along with enhanced guidance on containment, remediation, and future mitigation.
- Leverage authorized and vetted contractors to minimize third- and fourth-party supply chain vulnerability.

Source: IDC, 2021

November 2021, IDC #US48346721

SITUATION OVERVIEW

The COVID-19 pandemic exacerbated the need to secure government data. Before the pandemic, agencies typically relied on firewalls and similar border protections to secure government information within agency offices. When the pandemic forced the closure of agency offices, in addition to scrambling to providing softphones and PCs to employees who had never worked at home, agencies became vulnerable as virtual interactions exposed new attack surfaces that can be exploited by cybercriminals. This heightens the potential risk to agency information as well as personal information.

We are seeing the shift from relying on perimeter security to more adaptive approaches like zero trust that offers more multifaceted and pervasive defenses. This shift is driven by the need to protect a hybrid workforce and increasingly distributed and virtual cloud-based environments from more numerous and cunning cyberattacks. The shift is also driven by recent executive orders to protect agencies from ransomware, phishing, email compromise, and nation-state attacks, primarily the Executive Order (EO) 14028 on Improving the Nation's Cybersecurity, issued on May 12, 2021. This EO makes prevention, detection, assessment, and remediation of cyberincidents a top priority for agencies and essential to national security. As a result, there is increasing recognition that detection and response speed is the new battlefield, as this can dramatically reduce the potential damage and impact of cybercriminals. This EO focuses on modernizing cybersecurity defenses by protecting federal networks and digital supply chains, holding contractors and service providers to higher security standards, improving information sharing between the U.S. government and the private sector on cyber issues, and strengthening the ability to respond to incidents when they occur. Agencies are required to:

- Improve the federal government's visibility into threats.
- Adopt widely accepted security best practices that align with established security standards (i.e., NIST 800-53).
- Deploy a zero trust architecture, with better access controls, encryption, and token-based authentication.
- Deploy multifactor authentication, encryption, and endpoint detection and response (automated when possible).
- Work to increase the skills of security teams.

Zero Trust: An Adaptable Approach

Continued reliance on firewalls and similar border protections alone leaves organizations vulnerable and unprotected. The federal government spends more than $100 billion on IT and cyber-related investments annually. However, when it comes to cybersecurity, many federal agencies have failed or performed poorly, have been inadequately managed, and have security weaknesses, according to a March 2021 report by the U.S. Government Accountability Office (GAO). GAO indicates that over 28,000 security incidents were reported by federal executive branch civilian agencies to the U.S. Department of Homeland Security (DHS) in fiscal year 2019. And the most recent FITARA scorecard indicates that agencies are struggling with cybersecurity compliance. As of July 2021, only two agencies scored an "A," five agencies scored a "B," eight agencies scored a "C," seven agencies scored a "D," and one agency scored an "F" on the cybersecurity scorecard.

Zero trust provides data, network, identity, and access management solutions at scale. In a zero trust design, every device, user, network connection, and data exchange is authenticated and authorized. Zero trust enables agencies to implement a layered, risk-based approach using integrated threat

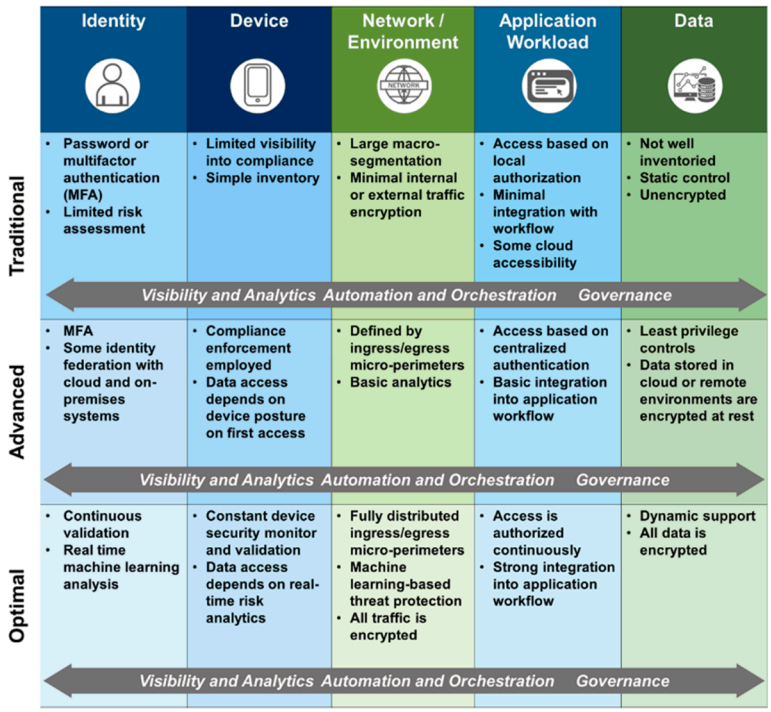
intelligence, automation, and analytics to detect and more quickly eradicate threats anywhere in the environment.

To assist agencies, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has published the zero trust maturity model (see Figure 2). CISA defines the stages as follows:

- **Traditional** – Manual configurations and assignment of attributes, static security policies, pillar-level solutions with coarse dependencies on external systems, least function established at provisioning, proprietary and inflexible pillars of policy enforcement, and manual incident response and mitigation deployment
- **Advanced** – Some cross-pillar coordination, centralized visibility, centralized identity control, policy enforcement based on cross-pillar inputs and outputs, some incident response to predefined mitigations, increased detail in dependencies with external systems, and some least privilege changes based on posture assessments
- **Optimal** – Fully automated assigning of attributes to assets and resources, dynamic policies based on automated/observed triggers, assets that have self-enumerating dependencies for dynamic least privilege access (within thresholds), alignment with open standards for cross-pillar interoperability, and centralized visibility with historian functionality for point-in-time recollection of state

FIGURE 2

CISA's Zero Trust Maturity Model



Source: U.S. Cybersecurity and Infrastructure Security Agency, 2021

The Impact of Cloud on Cybersecurity

Although IDC's *Industry CloudPath Survey* of 100 federal government decision makers indicates that improved IT security is the greatest benefit agencies have seen from cloud (selected by 41% of federal survey respondents), agencies need to do more. Agencies are confronted by an evolving cyber-risk environment as they increasingly use hybrid cloud and multicloud and deploy a growing number of applications in their cloud environments. Many agency applications rely on highly sensitive data that freely flows between on-premises and multicloud locations. This flow of information is attractive to hackers, who are continually seeking ways to exploit potential weaknesses in this environment. Data must be protected at all costs. Early priorities around information security and data protection were mainly focused on compliance, but the threat landscape has proven to be dynamic and increasingly sophisticated.

Cloud services should be designed as highly secure services (including SaaS, PaaS, and IaaS). The Cloud Smart Strategy, released by the U.S. Office of Management and Budget (OMB) in October 2018, reduces the barrier of entry for cloud migrations and plays a pivotal role in modernizing IT to improve citizen-facing services and accessibility and maintain cybersecurity. Cloud Smart emphasizes the need for Trusted Internet Connections (TICs) that are more compatible with agencies' requirements for solutions that are agile and flexible enough to securely manage the flow of internet traffic.

TIC 3.0 gives agencies a framework to adopt stronger security postures in their increasingly complex environments with a zero trust approach that grants access on a strict verification basis instead of a perimeter basis. Users must now be cleared for access at each level or entry point before they are able to enter an application. TIC 3.0 offers four use cases that provide agencies — including their remote users — with alternative approaches to traditional network security, allowing them to adopt public cloud in a secure way that minimizes exposure to risks, data breaches, and data leakage. To help secure data and information during the unprecedented surge of federal workers teleworking, the U.S. Cybersecurity and Infrastructure Security Agency released the *TIC 3.0 Interim Telework Guidance* document in support of OMB Memorandum 20-19 that provides security capabilities for remote federal employees securely connecting to private agency networks and cloud environments.

Cloud Smart calls for organizations to do a full inventory of the applications in their environments. They are asked to assess the need for those applications, where those applications live, and what services those applications require to function properly and securely, such as load balancing and web application firewalls (WAFs).

Cloud Smart advocates for continuous data protection and awareness as agencies take a risk-based approach to securing cloud environments. This requires that agencies transition to a multilayer defense strategy and also provide data-level protection, otherwise known as defense in depth. Specifically, the guidance suggests that agencies should place "protections at the data layer in addition to the network and physical infrastructure layers."

The EO on cybersecurity complements Cloud Smart by instructing agencies to continue to use cloud technology in a "coordinated, deliberate way that allows the federal government to prevent, detect, assess, and remediate cyberincidents." And agencies are to adopt zero trust as practicable to facilitate the migration to cloud. NIST, CISA, and others are working to improve cloud service governance frameworks that will include an expanded cloud security strategy. Cloud service providers will see a growing demand for solutions that support zero trust connections and supporting systems.

Cloud Smart also recommends implementing the Federal Risk and Authorization Management Program (FedRAMP), which provides a standardized way of assessing security and continuously monitoring for threats. IDC expects more agencies to select FedRAMP-authorized cloud providers and hold them to higher standards with more rigorous cybersecurity requirements including a zero trust architecture. The EO on cybersecurity advises updates to FedRAMP driven by CISA's *Cloud Security Technical Reference Architecture.* According to CISA's current draft, major changes to FedRAMP will include:

- Scoping and defining the authorization boundary in the cloud
- Defining data types, including federal data and federal metadata in the cloud
- Leveraging interconnections, external and corporate services

Cloud platforms and modern architectures are driving adoption of application services. As cloud and container-native application architectures mature and scale, more organizations are deploying related application services, such as ingress control and service discovery, both on premises and in the public cloud. Modern applications require modern application services to support scale, security, and availability requirements. How well agencies protect web applications and APIs can determine whether their online presence is reliable and trusted. Application security is the result of using technologies and processes to protect applications from dynamic threats, including application exploits, malicious traffic, and bots. This approach may include securing applications with a web application firewall that's powered by behavioral analytics and identifies and responds to new threats in real time. It may also include privileged user access to consistently protect access to sensitive assets such as unique military deployment guides.

Advanced analytics and AI need the massive compute and storage capabilities of cloud. IDC's *Industry CloudPath Survey* indicates that 64% of agencies surveyed report that cloud-based predictive analytics to identify, contain, measure, and address security risk is critical — business would stop without it. Advanced/predictive analytics are important/very important in choosing a cloud service provider for 63% of agencies surveyed. And 38% of agencies surveyed currently use cloud-based predictive analytics to identify, contain, measure, and address security risk, while 20% expect to move to the cloud for this app within 24 months.

Leveraging AI for Cybersecurity

Agencies realize they need much faster and more scalable analytics for cybersecurity. In addition to cybertelemetry, agents will need to analyze all the data that the EO requires them to collect. Agencies are required to share data, information, and reporting, as they relate to cyberincidents or potential incidents relevant to any agency with which they have contracted. Further, agencies are to collaborate with federal cybersecurity or investigative agencies in their investigations of and responses to incidents or potential incidents on the federal information system.

Since the issuing of EO 14028, the release of Memorandum M-21-31 on August 27, 2021, addresses the detailed logging, log retention, and log management requirements of Section 8 of EO 14028 — breaking down what fields are most important to be captured for visibility before, during, and after a cybersecurity incident. This collection of data logs may generate petabytes of data that needs to be analyzed in a timely fashion. Speed is critical so that agencies can operate on the same scale and on the same timeline as cybercriminals — basically minutes to hours versus the typical weeks if not months it takes to detect a cyberincident. Agencies are adopting AI to be able to better scope out threats. For example, GSA received funding from the Technology Modernization Fund (TMF) to deploy zero trust and adopt increased machine learning- and AI-driven algorithms. This use of AI will help connect diverse data sources and highlight threats while providing security oversight for cyber supply

chain risk management as well as enhancing core security operations centers to include governmentwide public-facing digital services. The proliferation of cybergangs and adversarial nation-states necessitates that agencies use AI to expedite the analysis and adaption of defenses when context is added to full packet collection or metadata collection.

ADVICE FOR THE TECHNOLOGY BUYER

As agencies identify gaps in their organization's cybersecurity practices and undertake a systematic approach for identifying, assessing, and managing cybersecurity risks, they have many choices. With the ongoing changes occurring in today's security landscape, along with the rapidly evolving pace of technology, organizations must evaluate offerings for today and for the future. In addition to zero trust, EO 14028 may spur deployment of continuous testing/monitoring, iterative testing, and managed security services including managed detection and response, XDR, and monitoring and addressing volatilities within agencies' environments. IDC recommends agencies:

- Work to gain visibility into all devices, including trusted user connectivity, device usage, and ongoing activity. Establish trust criteria and inspect devices for integrity and trust inference.
- Work toward software-defined access and access controls that can provide attribute-based network micro-segmentation. This can start with software-defined perimeter access and then extend into mobile device connectivity and applications management, with device trust inference.
- With access control and network visibility in place, move to a multiyear strategy to expand zero trust deployment. Develop a project portfolio that meets both the business needs of your agency and the needs of citizens.
- Define adaptive rules and policies for future installations and enhance endpoint configuration management and device trust inference capabilities. Ultimately, a zero trust model decrees that all hosts be treated as if they are internet facing. The locations where they reside, including internal networks, should be considered potentially hostile.
- Work with vendors capable of helping your agency advance in the CISA zero trust maturity model. Zero trust is about measuring and establishing trust in both people and devices.
- Strive to provide high-performing incident response, which is time-consuming and needs skilled personnel — that most of the agencies lack. To expand cybersecurity staff skills and capability, consider managed security services with various levels of support for deeper investigation analysis along with enhanced guidance on containment, remediation, and future mitigation.
- Leverage authorized and vetted contractors to minimize third- and fourth-party supply chain vulnerability. Large SIs, and other vendors, have been known to dedicate resources to open source efforts in order to maintain involvement and some level of quality and control.

LEARN MORE

Related Research

- *IDC FutureScape: Worldwide National Government 2022 Predictions* (IDC #US47241921, October 2021)
- *Operationalizing and Scaling AI in Federal Government* (IDC #US48236521, September 2021)

- *The New Normal: How AI Is Enabling Resiliency in Federal Agencies* (IDC #US48145721, September 2021)
- *IDC's Worldwide Digital Transformation Use Case Taxonomy, 2021: National Civilian Government* (IDC #US46548221, August 2021)
- *IDC PlanScape: Cybersecurity for Government's Multicloud Environment* (IDC #US47663121, May 2021)

Synopsis

This IDC Perspective highlights three important tools in agency arsenals to thwart cybercriminals: zero trust required by an executive order, Cloud Smart to reduce the barrier of entry for cloud migrations while maintaining cybersecurity, and AI to connect diverse data sources and be able to better scope out threats.

"With the ongoing changes occurring in today's security landscape, along with the rapidly evolving pace of technology, organizations must evaluate offerings for today and for the future," says Adelaide O'Brien, research director, IDC Government Insights. "Transitioning to a zero trust architecture will not be a quick or easy task but requires bold changes and significant investments to defend national vital institutions," she adds.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights.

Copyright 2021 IDC. Reproduction is forbidden unless authorized. All rights reserved.