opentext™ | Cybersecurity

Position Paper

Zero Trust: Where CISOs and Mission Leaders Align

Introduction

The May 2021 Cybersecurity Executive Order has re-focused all Federal agencies on formalizing and accelerating many cybersecurity goals and mandates, including the new TIC 3.0 and various existing and pending legislation including the Information Transparency and Personal Data Control Act.

Studies have shown that over 45% of federal agencies' security breaches are now indirect, as threat actors target the weak links in their extended operation. This shift to indirect attacks blurs the true scale of cyberthreats. Organizations should look beyond their four walls in order to protect their operational ecosystems and supply chains. Fully 85% of federal respondents and 82% of organizations globally agreed that they need to think beyond securing their enterprise and take steps to secure their ecosystem in order to be effective.

Often, CIOs, CISOs, and Program Managers in agencies have diverging or different priorities, as you can see in their response to recent surveys below.

Rank	CISO Priorities Gartner Top Priorities IT Leadership	CIO Priorities IDG State of the CIO	Program Manager Priorities CIO.gov
1	Protecting Assets with Least Privilege	Security Management	Deliver smarter, better, faster service to citizens
2	Shifting Identity Management	Improving IT operations performance	Efficiency: Maximize value of Federal spending
3	Integrating DevSecOps	Aligning IT initiatives with organization goals	Deploy a world-class workforce and create a culture of excellence
4	Continuous Auditing and Reporting	Aligning IT initiatives with business goals	Support innovation, economic growth, and job creation
5	Moving to Proactive vs. Reactive	Driving Innovation	

The following sections present four actionable initiatives that are already mandated by legislation or executive orders, yet have not received enough priority within agencies to implement. Hence, the government remains unnecessarily exposed to threats, as evidenced by recent successful attacks. Additionally, these four initiatives address 6 of the top 14 priorities of key leaders within federal agencies, as shown in the shaded boxes above.

Limiting Access Greatly Limits Breach Impacts

"Trust, but verify," is an old Russian proverb made famous by President Ronald Reagan. With the growing number and increasing aggressiveness of nation-state actors, the federal government is dangerously relying only on verification for access to IT systems. Trust is the missing component.

In 2008, the US Department of Defense suffered a significant compromise of its classified military computer networks. It began when an infected flash drive was inserted into a US military laptop at a base in the Middle East. The flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the US Central Command. That code spread undetected on both classified and unclassified systems—establishing what amounted to a digital beachhead from which data could be transferred to servers under foreign control. Effectively, a rogue program was inside the wire, poised to deliver active military defensive plans to an unknown adversary.

Moreover, in 2020 and 2021, all five branches of the US Military, as well as the Pentagon, State Department, Department of Justice, NSA, NASA, and other federal agencies were compromised by the SolarWinds/Microsoft breach through a variety of sophisticated attack methods, including significantly exploited credentials of both administrators and system processes.

These are just two of many incidents that demonstrate that even though perimeter- and application-level security are the current standards in the federal government, lateral movement and privilege escalation allow virtually unlimited access to data through an application—regardless of the in-transit, application, and at-rest encryption methods and tools used.

The resulting zero trust architecture means exactly that: Nothing is trusted inside or outside the network. Entry requires strict access controls, user authentication, and continuous monitoring of networks and systems, among many other elements. Users and devices that request access to resources are continually authenticated.

Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.) rather than network elements because the data within the networked assets is at risk once the network perimeter has been breached. While it is a large effort in total, beginning to address zero trust with practical, tactical investments can yield significant reductions in both the frequency and impact of breaches.

Authentication and authorization (both subject and device) are discrete functions performed before a session with an enterprise resource is established. Zero trust is a response to enterprise network trends that includes remote users, bring your own device, and cloud-based assets that aren't located within an enterprise-owned network boundary.

The Executive Order emphasizes to agencies that perimeter-based security is no longer sufficient. This is due in part to an increased number of users or systems working outside the perimeter and malicious actors becoming much more proficient at stealing credentials and getting inside the perimeter.

Consequently, the best policy is to trust no one. The zero trust security model ensures security in an environment in which cloud, mobility, and related technologies have diminished the effectiveness of perimeter-based security. Zero trust also recognizes that in this era of phishing attacks and stolen credentials, there is no meaningful distinction between internal and external threats. Everyone on the network must be seen as a potential threat. Practically speaking, that means every time a user (or system) requests access to applications, data, or other network resources, the network should verify identity and privilege and whether the user or system should have access to that resource.

Automating to Improve Resiliency and Reduce the Exposure Window

A recent Accenture study entitled, "Achieving federal cyber resilience," helps explain how leading organizations within governments and commercial enterprises prioritize and spend to achieve cybersecurity excellence, including investing in automated detection and response.

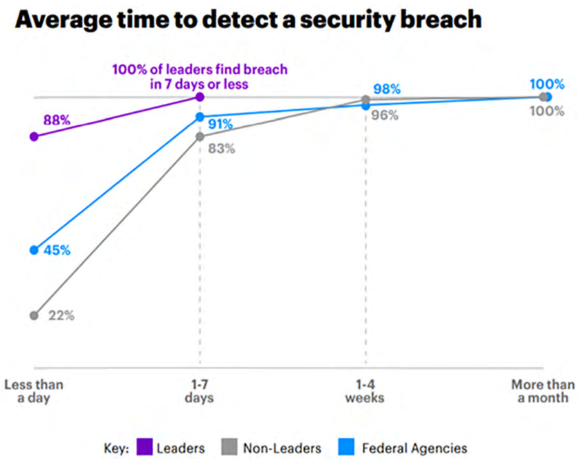


Figure 1. Source: Accenture

Mission effectiveness requires highly reliable and continuous availability. Guaranteeing uptime beyond 99.5% can be a challenge when a system is under attack or even during peak usage hours, as we have experienced in national emergencies. Automating mundane and repetitive tasks with workflow processes can be a significant force multiplier for human assets, which can drive much higher system availability. The last decade of rapidly evolving operations orchestration software (a.k.a., robotic process automation) has now begun to help SOC personnel with its ability to handle 50% or more of incident response tasks. Workflow automation and AI can interrogate endpoints, configure settings on network hardware, isolate devices, and lock out or modify permissions on user and system accounts. These technologies also assist human analysts by gathering data to speed analysis and undertake remediation. Use case studies have shown that integrated AI and machine learning can speed up investigation of and response to incidents by a factor of 10.

Organizations routinely respond to large volumes of alerts and threat data that require immediate attention. To manage the unrelenting flow of increasingly complex event information, agencies are now leveraging machine-driven automated activities. Agencies moving toward TIC 3.0 and zero trust will benefit from technologies that enable organizations to designate a central place for collecting alerts and threat feeds—and respond to and remediate incidents at machine speed.

A recent Forrester study concluded that by implementing an integrated enterprise SOAR platform, organizations would experience benefits such as:

- Saving an average of more than an hour of analyst time for each security incident.
- Reduced hardware and software tool maintenance costs by eliminating duplicate products.
- Increased end-user productivity due to a reduction in cyber incident-related remediation downtime.
- Improved audit efficiency.

Reducing the Value of Exfiltrated Data

The most recent breaches involving third-party software products (both commercial and open source) have proven that eventually data will be exfiltrated. Data exfiltration is the primary target for hackers—whether it be PII, credit card and social security information, health records, or (in the case of the OPM breach) foreign contacts of US citizens applying for a security clearance. The aggregate loss of Controlled Unclassified Information from commercial companies in the US increases the risk to national economic security. The Council of Economic Advisers, an agency within the Executive Office of the President, estimated that malicious cyber activity cost the US economy between $57 billion and $109 billion in 2016[1].

The US Department of Defense recently implemented CMMC (Cybersecurity Maturity Model Certification) as a step toward better protecting data that is ultimately used by companies doing business with the federal government. Further, suppliers to companies doing business with the federal government are required to “flow down” those protections to their operations. Practically speaking, in 2021 and into 2022, CMMC only requires a self-certification of process controls around data usage. And because the certifications are only periodic, any operational changes to processes or software obviate the audit. CMMC does nothing to actually improve how well the data is protected. This means the data remains an open and valuable target within applications, decrypted by system processes, and applications continuously.

Commercial companies in sensitive industries such as banking and healthcare use this technology pervasively, but federal agencies do not, as of yet. This technology eliminates the value of stolen data through partial field pseudonymization and tokenization based on the NIST Standard 800-53G, format-preserving encryption.

[1] The Cost of Malicious Cyber Activity to the U.S. Economy, CEA (February 2018)

These solutions encrypt partial fields of sensitive data such as social security numbers or medical information, but allow the data to be used by applications and data analytics.

Applications, users, malware, and bad actors all have access to the data, but only authorized users/apps can decrypt the de-identified fields on an exception basis. In many cases, data does not need to be de-identified: for example, the first five digits of a social security number when using the last four for user identification. And because the data maintains referential integrity, analytics can be run against even the encrypted data.

Managing the Inherent Risks in Open Source Components (Securing Your Software Supply Chain)

The inside threat today exists largely in the form of application code. Third-party components make up a significant portion of many applications' codebase, making software composition analysis a "must-have" AppSec capability. On average, applications used by government agencies are 80% custom code or open source code; and over 60% of cybersecurity data breaches can be traced to software defects. They aren't from a vendor that has enterprise-grade software testing capabilities. Rather, cyber incidents and breaches are largely due to applications that rely on third-party libraries.[2]

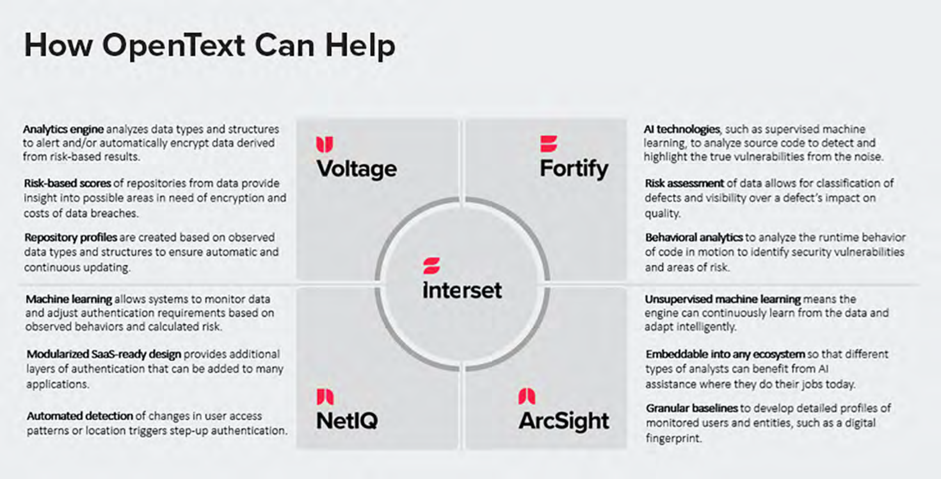
Conclusion

Historically, the federal IT community has focused heavily on strong perimeter security to protect enterprise assets, with some level of network login and application password security. But now—with the known realities of software supply chain risks, fractured identity management even within applications, and increasing data breach frequency in spite of greater spending—it's clear that network and device security isn't enough.

Zero trust means trust no one and nothing. Authenticate everything, continuously. Scan the environment for anomalies. The idea of a perimeter that constitutes a bright line between safe and unsafe suddenly seems quaint.

Learn more at
www.opentext.com

[2] 85% of the time, incidents are the 90% of applications that rely on third-party libraries that comprise up to 70% of code



How OpenText Can Help

Analytics engine analyzes data types and structures to alert and/or automatically encrypt data derived from risk-based results.

Risk-based scores of repositories from data provide insight into possible areas in need of encryption and costs of data breaches.

Repository profiles are created based on observed data types and structures to ensure automatic and continuous updating.

Machine learning allows systems to monitor data and adjust authentication requirements based on observed behaviors and calculated risk.

Modularized SaaS-ready design provides additional layers of authentication that can be added to many applications.

Automated detection of changes in user access patterns or location triggers step-up authentication.

AI technologies, such as supervised machine learning, to analyze source code to detect and highlight the true vulnerabilities from the noise.

Risk assessment of data allows for classification of defects and visibility over a defect's impact on quality.

Behavioral analytics to analyze the runtime behavior of code in motion to identify security vulnerabilities and areas of risk.

Unsupervised machine learning means the engine can continuously learn from the data and adapt intelligently.

Embeddable into any ecosystem so that different types of analysts can benefit from AI assistance where they do their jobs today.

Granular baselines to develop detailed profiles of monitored users and entities, such as a digital fingerprint.

Connect with Us
www.opentext.com

References

1. NIST 800-38G
2. Achieve Zero Trust with TIC 3.0
3. IT4IT
4. Resilient Digital Public Sector and Government Services Flyer (microfocus.com)
5. Gartner Reprint of CIO Priorities 2021
6. **IDG State of the CIO**
7. Achieving Federal Cyber Resilience
8. Defending a New Domain | Foreign Affairs
9. The CMMC—Myths and realities—Secure Cyber Defense
10. New NIST Security Standard Can Protect Credit Cards, Health Information | NIST

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

762-000054-003 | O | 01/24 | © 2024 Open Text