Achieve Zero Trust With TIC 3.0

INDUSTRY PERSPECTIVE

govloop

MICRO FOCUS Government Solutions

MFGS INC Micro Focus Government Solutions Master Supplier

Moving Beyond Perimeter Security

The recent and rapid adoption of cloud, mobility and related technologies has dramatically altered the federal IT environment. While these technologies have facilitated the development of a whole new range of IT services, they have also created new cybersecurity concerns.

Traditionally, agencies have relied on perimeter-based security solutions. These methods worked (to some extent) when most employees were working within the perimeter and accessing applications and data through the data center. But more and more frequently, that's not the case.

Branch offices or employees working remotely often are accessing applications and data through the cloud. Under the Trusted Internet Connections (TIC) policy, network traffic was required to be routed through the security controls in the data center, which led to numerous problems with performance and security.

Hence the genesis of TIC 3.0, which enables agencies to create a more distributed network architecture, in which the security controls can be moved to the cloud in closer proximity to users. Expectations are high that TIC 3.0 will significantly improve security in today's cloud-based IT environment. But in order to achieve the full benefits, agencies are recognizing they must also adopt a Zero Trust security model.

Zero Trust, like TIC 3.0, recognizes perimeter-based security is no longer sufficient. This is due in part to so many users or systems working outside the perimeter; further, malicious actors have become far 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.

To move forward, successful agencies will leverage TIC 3.0 and Zero Trust in tandem.

To learn more about how agencies can successfully deploy Zero Trust as part of TIC 3.0, GovLoop interviewed John Fanguy, Chief Technology Officer at Micro Focus, which provides enterprise-grade software solutions to support digital transformation. This resource outlines how Zero Trust can help agencies achieve the security objectives of TIC 3.0.

The Playbook: Zero Trust and TIC 3.0

Despite the considerable interest within federal government IT circles, implementation of the Zero Trust model won't be a slam dunk. TIC 3.0 can illuminate the way, providing clarity in the form of five security objectives that align with the conceptual framework of Zero Trust.

Pursuing these security objectives will move agencies toward their Zero Trust destinations. In this section, we will examine those objectives, the ways in which they promote Zero Trust and how agencies might think about their adoption.

Managing Traffic

Observe, validate and filter data connections to align with authorized activities, least privilege and default deny.

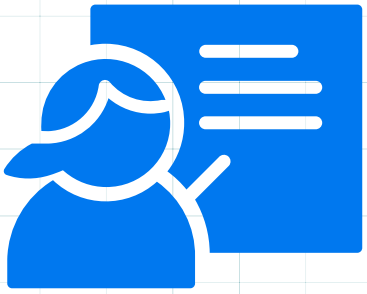
The challenge of effectively managing traffic is knowing where data is and who or what should have access to it at all times – at rest and in transit. In order to gain that knowledge, agencies need tools that develop a consistent, overarching view of identities inside and outside organizations. An effective tool collects and curates identity governance data, providing insight into who has access, why access was granted and whether that access is still needed. Continuous monitoring and updates provide a single source of truth for identity and access.

Managing traffic entails "observing, validating and filtering data connections to align authorized activities, and in that comes least privilege," Fanguy said.

To discern the way toward Zero Trust, agencies can begin by assessing where they are in the security matrix relative to identity and access management (IAM). IAM is a multi-tiered model in which each level of security provides a foundation for successive levels.

- Level one security has four components. First is single sign-on and perhaps some level of federation at the department level.
- Level two is the capability to do user provisioning in an automated, auditable fashion – as opposed to a would-be user receiving a piece of paper or an email to create a user form.
- Level three is user self-service to ensure users are authenticated for access, recent permissions, past use, etc., in an auditable fashion.
- Level four is delegated administration.

"Those are the four core capabilities that we've seen agencies get the most value from in the fastest time and for the least cost," Fanguy said. "That creates the foundation for level two."



Protecting Traffic Confidentiality

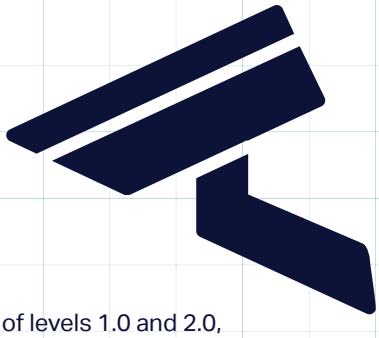
Ensure only authorized parties can discern the contents of data in transit, sender and receiver identification, and enforcement.

The challenge of protecting traffic confidentiality centers on encrypting data in transit, including unstructured data, and confirming the identities of senders and receivers.

One solution is technology that embeds kernel drivers into the file system stack of Windows and non-Microsoft systems, operating transparently to the end user. A driver intercepts files, encrypting and decrypting data on the fly, and works with all applications and file types. Organizations can use policy rules to ensure the automatic encryption of data in real time, without slowing workflow. These solutions also enable monitoring of data at runtime, including the capture and analysis of such information as when and where a file was opened and how it was used.

Protecting traffic confidentiality involves format-preserving encryption, and level two of identity access management spans a half-dozen or so capabilities. First is multifactor authentication, including a spate of new login capabilities introduced during the pandemic, in response to the increase in remote work. Second is increased visibility around governance, with regard to who has access to various assets. Third is privileged access management, an area dealing with different levels of security that system administrators can access and guard.

Fourth is a virtual directory of users and capabilities that is regularly updated and never static. Fifth are service security and change monitoring, and next are data security and encryption. Taken together, all of these capabilities constitute level two. "If you don't have 1.0, it's really hard to do 2.0," Fanguy said.



Protecting Traffic Integrity

Prevent alteration of data in transit and detect altered data in transit.

Protecting alteration of data in transit is critical, because organizations' stewardship of information is often substandard under the best of circumstances. A survey of 300 federal agencies found that 99% of them were unable to determine what data various groups of users have access to, or how many copies of that data exist.

"If you don't know where the data is and how many copies there are and who has access, it's really hard to design a security system to prevent the most obvious breaches," Fanguy said.

Adoption of level 3.0 is in its infancy. Other than issuance of requests for information and "maybe a procurement or two, it's still a ways off," Fanguy said. "But increasingly, both industry and the government are coalescing around this. Ultimately it's where you want to get to."

Building on the foundation of levels 1.0 and 2.0, agencies seeking to attain level 3.0 security will have to acquire four major security capabilities: policy management, active threat detection, behavioral analytics and data analytics.

"In the context of attaining those tools, it can be helpful to think in terms of variable trust security, in which trust varies by device, person or activity," Fanguy said.

Behavioral analytics, which looks at who's doing what and when, for example, ties in well with the idea of variable trust, such as when an employee who always works from 8 a.m. to 5 p.m. attempts to log in at 1 a.m. "Sometimes it's just a time of day question," Fanguy said.

Ensuring Service Resiliency

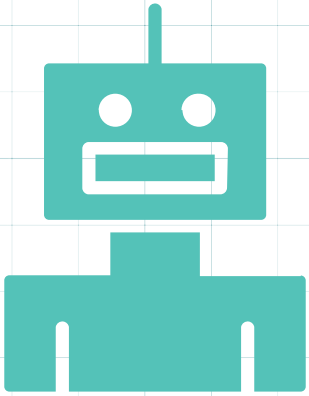
Promote resilient application and security services for continuous operations as the technology and threat landscape evolve.

Mission effectiveness requires system continuity and reliability. Guaranteeing uptime can be a challenge when demands on a system spike or a network is under attack, especially if the IT team is stretched thin. Automating mundane and repetitive tasks, and adding in workflow processes can lighten the load on human workers and keep operations running.

Specialized software has the capacity to handle half or more of incident response tasks. Workflow automation and AI can interrogate endpoints, configure firewalls, isolate computers in a network and lock user accounts. These technologies also assist human analysts by gathering data to speed analysis and undertake remediation. In use case studies, integrated AI and machine learning can speed investigation of and response to incidents by a factor of 10.

When it comes to threat detection and response, every second counts. A powerful security information and event management (SIEM) platform will detect, analyze and prioritize those threats in real time. Effective platforms also support security operation centers (SOCs) with workflow, response and compliance management. An industry-leading threat correlation engine will promote effective security analytics in an SOC.

"Basically, you're trying to ensure that applications are resilient and that there are failover capabilities in place," Fanguy said.



Ensuring Effective Response

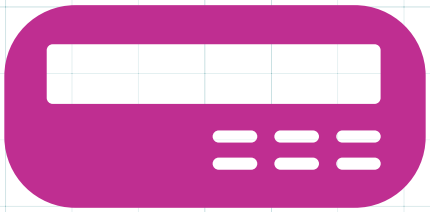
Promote timely reaction and adapt future responses to discover threats; define and implement policies; simplify adoption of new countermeasures.

An unfortunate legacy of perimeter security is a pervasive false sense of security. By hyper-focusing on keeping intruders outside the wall of protection, enterprises were vulnerable to inside threats. Breaches of security often went undetected for many months.

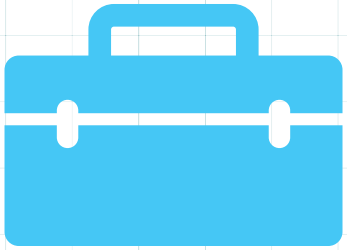
The inside threat today exists largely in the form of application code. On average, applications used by government agencies are 80% custom code or open source code. They're not from a vendor that has enterprise-grade software testing capabilities. "That's a weakness," Fanguy said. "Cyber incidents and breaches are, 85% of the time, the result of custom or open source code. That code is the real opportunity for security problems."

At present, organizations routinely respond to large volumes of alerts and threat data requiring immediate attention. To manage the unrelenting flow of critical data, agencies in the future will leverage more machine-driven automated activities. Agencies moving toward TIC 3.0 and Zero Trust will benefit from technologies that help organizations to have a central place for collecting alerts and threat feeds – and to respond and remediate incidents at machine speed.

For agencies pursuing this security objective, "the bullseye is automated security incident response," said Fanguy.



The Toolbox



Advanced authentication framework will make it possible to centralize authentication and authorization management. Streamlined management from a single solution cuts costs and bolsters security. Solutions that can leverage open standards allow for quick integration and protect against security breaches and the risk of vendor lock-in. The built-in flexibility of an advanced authentication framework allows for customizing security protocols and methods, plus improvement of the overall user experience.

Cloud data security tools protect sensitive data across multi-cloud, hybrid and on-premises environments. The best of these tools embed data-centric security across hybrid IT and accelerate safe migration to cloud environments.

Enterprise-grade backup and disaster recovery solutions built on scalable architecture combine security and analytics, thus enabling agencies to maintain continuity in a reliable and cost-effective way. Data-centric backup and disaster recovery solutions meet the challenges of complexity, scalability and data security found in dynamic and diverse IT environments, while enabling centralized data protection across diverse cloud environments.

Real-time threat detection and response, powered by an open, intelligent SIEM platform, detects, analyzes and prioritizes threats as they occur, while supporting SOCs with workflow, response and compliance management.

How Micro Focus Helps

Micro Focus delivers trusted and proven mission-critical software that keeps the digital world running, from private companies to federal agencies. Using a pragmatic, disciplined, customer-centric approach, Micro Focus helps customers succeed in today's rapidly evolving marketplace.

Micro Focus offers an array of security solutions that benefits agencies moving toward Zero Trust.

- AI and machine learning capabilities that monitor user behavior and potential insider threats
- Centralized identity and access management to ensure least privileged access to all managed systems, which help agencies digitally transform their environment and build a solid security foundation for the Zero Trust methodology
- This platform unifies credentialing, access and change synchronization so it's done once, rather than for every instance of the identity in the ecosystem.

Helping agencies move toward Zero Trust is a process that begins with careful, long-range planning. "We sit down with an agency to try to help them understand where they are and what they should invest in now, versus five years from now," Fanguy said.

Learn more at www.mfgsinc.com and www.microfocusgov.com

Conclusion

For years, the federal IT community had unwavering faith in the ability of strong perimeter security to protect enterprise assets. It wasn't just the best way. It was the only way.

In just a decade, a new security model has emerged. Zero Trust turns perimeter security inside out. Trust no one. Authenticate everything. Scan the environment for anomalies. The idea of a perimeter that constitutes a bright line between safe and unsafe suddenly seems quaint.

Zero Trust makes sense, but the path for getting to that enviable state from the starting point of legacy security is, for most agencies, not immediately apparent. There is no map, no case study to use as a guide. It's all too new.

There is, however, a way forward.

"There will never be one tool that you can purchase that will give you Zero Trust," Fanguy said. "The best approach is to sit down with someone who's been doing [security] for years and understand where you are on the maturity model … identify the most critical capabilities for your agency and create a multiyear program to move up the capability maturity model in an organized fashion."

MICRO FOCUS Government Solutions

Micro Focus Government Solutions is a US based, purpose-built, independent, government compliant company that serves US public sector clients. Micro Focus Government Solutions is backed by one of the largest pure-play software companies in the world, Micro Focus. This independent US company is committed to helping your organization's mission-critical IT challenges with their agile and modern software solutions.

Learn more at www.microfocusgov.com.

MFGS INC Micro Focus Government Solutions Master Supplier

MFGS, Inc. is a Master Supplier of Micro Focus' best-in-class portfolio of enterprise-grade scalable software solutions to the U.S. Government, its partners, and system integrators. We are an independent, 100% U.S.-based, employed and owned company. MFGS, Inc. is customer-centric, government compliant and purpose built to fulfill, support and deliver Micro Focus government solutions to the U.S. Federal Government.

Learn more at www.mfgsinc.com.

govloop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

www.govloop.com | @GovLoop

1152 15th St. NW Suite 800
Washington, DC 20005

P (202) 407-7421
F (202) 407-7501
www.govloop.com
@GovLoop