PUTTING ZERO TRUST INTO PRACTICE

Fitting the pieces together for advanced cyber defense

Federal agencies are racing to adopt a zero trust architecture to comply with urgent cybersecurity requirements. Some are further along than others in this journey, but all face the same questions: Where do we start? And how do we move our organization to the necessary architecture?

To answer these questions and pinpoint where improvements are needed, organizations must first step back and review their existing cybersecurity posture and technology roadmaps through a zero trust maturity assessment. This in-depth look at organizational and architectural issues—which provides deeper insights than typical cyber risk reviews—is designed to help organizations identify and address their zero trust gaps.

UNDERSTANDING THE PILLARS OF ZERO TRUST

Identifying zero trust gaps as early as possible will help organizations meet upcoming deadlines. Based on Executive Order 14028 and the federal zero trust strategy, agencies must achieve specific zero trust security objectives by the end of fiscal year 2024. To that end, they have been drafting implementation plans, which need to be refined and resourced to accomplish "ambitious, achievable goals," according to the White House's FY24 cybersecurity budget guidance.

Evaluating the current state of the enterprise's capabilities and gaps is the first step. This enables the security team to weigh priorities and craft tailored implementation guidance to achieve focused improvements over time.

This evaluation requires a framework—a basis for rating capabilities, setting targets for improvement, and achieving measurable progress. To that end, Booz Allen developed a maturity assessment model: It aligns to the Department of Defense (DOD) and Cybersecurity and Infrastructure Security Agency (CISA) maturity models, but provides a more granular look at an organization's capabilities across the seven pillars defined in the DOD reference architecture. For more detail on the pillars, see Figure 1 for a visual summary and examples of capabilities along the spectrum.

The model helps put the principles of zero trust—assume a breach; never trust, always verify; and allow only least-privileged access based on contextual factors—into action. It lets organizations rate their capabilities in all seven dimensions of zero trust using the five maturity levels: initial, minimal, basic, innovative, or leading. Insights from such an assessment can help an agency work toward deploying comprehensive security monitoring, granular dynamic and risk-based access controls, and system security automation in a coordinated way throughout infrastructure.

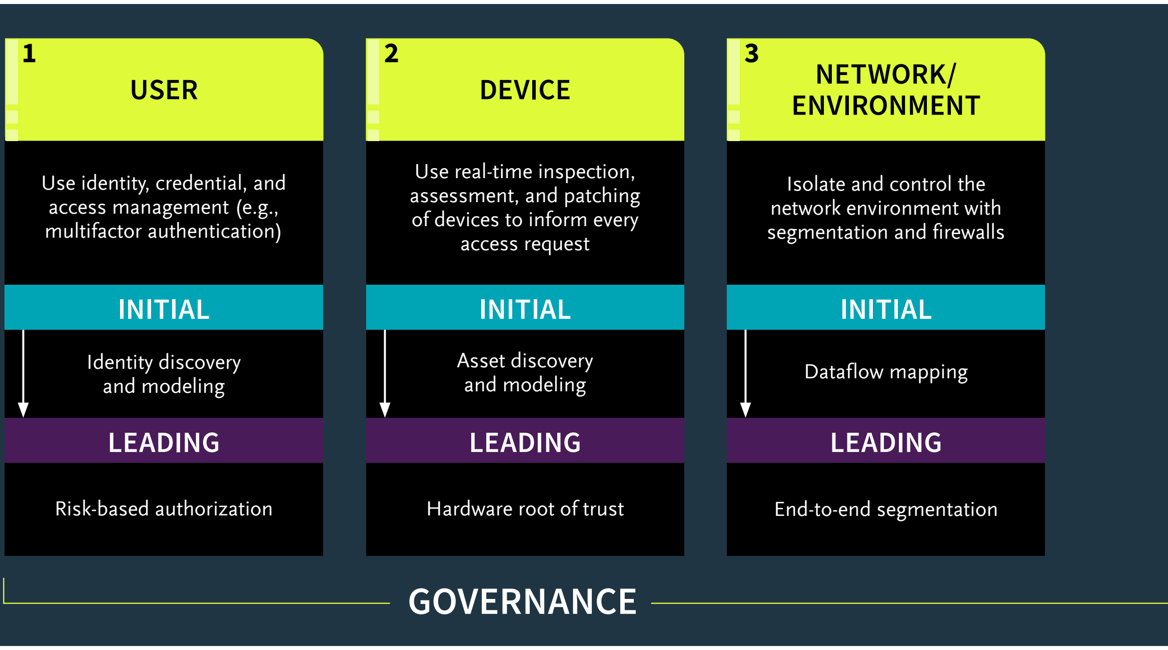
Armed with a threat-centric understanding of where an organization is along the spectrum, it's possible to set future targets that help drive down operational risk and give rise to new solutions for pressing needs.

Over time, organizations can continuously use the maturity assessment model to conduct follow-on assessments whenever they need to refresh their approach. The first step is always to diagnose challenges across the seven pillars by examining how people, process, and technologies form the organization's security solution. Next, organizations design a zero trust strategy, develop new fixes in the safety of a lab, and deploy new solutions.

The overarching strategy spans the zero trust pillars, provides a unified target state and a multiyear roadmap, and prioritizes the development of strong governance policies that drive enforcement of conditional access.

Elevate Security by Design with 7 Pillars of Zero Trust

Maturity model enables focused improvement, in several steps, from initial practices toward leading capabilities


1 USER

Use identity, credential, and access management (e.g., multifactor authentication)

INITIAL

Identity discovery and modeling

LEADING

Risk-based authorization

2 DEVICE

Use real-time inspection, assessment, and patching of devices to inform every access request

INITIAL

Asset discovery and modeling

LEADING

Hardware root of trust

3 NETWORK/ ENVIRONMENT

Isolate and control the network environment with segmentation and firewalls

INITIAL

Dataflow mapping

LEADING

End-to-end segmentation

GOVERNANCE

Figure 1

EVALUATING THE CURRENT STATE OF THE ENTERPRISE'S CAPABILITIES AND GAPS IS THE FIRST STEP. THIS ENABLES THE SECURITY TEAM TO WEIGH PRIORITIES AND CRAFT TAILORED IMPLEMENTATION GUIDANCE TO ACHIEVE FOCUSED IMPROVEMENTS OVER TIME.

Booz Allen uses this same approach internally to improve our own security posture. The firm is committed to making Booz Allen "client zero" for the development of all kinds of innovative new solutions as we operate and defend a global enterprise with more than 30,000 users supporting a wide range of critical missions.

TECHNICAL CHALLENGES TO FOCUS ON

Operationalizing a zero trust architecture along the path to maturity brings a host of technical decisions. Amid the multitude of potential priorities, here are three notable areas of focus for cyber and data practitioners.

DEALING WITH DATA

Every organization is unique. But the aspect of zero trust where most organizations tend to be the weakest is the data pillar. This area involves using end-to-end encryption, data rights management, and data tagging to protect data. Organizations should prioritize fixes in the area of data management to ensure the success of broader objectives.

For instance, as organizations try to conduct data discovery and classification, the first area they are looking to modernize is secure access to their networks (cloud and on-premises), otherwise known as zero trust network access (ZTN). To enable restricted access by default as desired, they first need to figure out how to classify and handle their data.

IMPLEMENTING IDENTITY

Another big hurdle for enterprise cybersecurity is implementing identity in an unfamiliar way. To achieve the federal vision for zero trust, agency staff need to use enterprise-managed identities to access the applications they use for work. However, employees change roles, routinely in some organizations. It is important, yet challenging, for security teams to maintain awareness of what these individuals should and should not be able to access based on their new position.

The identity management piece is a vital enabler for all zero trust principles. Strong authentication is also important to provide assurance around identities. Focusing on these areas from the start can set a strong foundation for further zero trust improvements. Also, organizations should establish a single source of truth for

4 APPLICATION AND WORKLOAD	5 DATA	6 VISIBILITY AND ANALYTICS	7 AUTOMATION AND ORCHESTRATION
Prevent the adversary from seeing, mapping, and traversing the network	Use end-to-end encryption, data rights management, and data tagging to protect data	Improve detection and reaction time, enabling real-time access decisions	Quarantine and/or terminate anomalous activity based on defined processes
INITIAL	INITIAL	INITIAL	INITIAL
Inventory workload configurations	Data discovery	Cyber analytics requirements and log identification	Defined security processes
LEADING	LEADING	LEADING	LEADING
Process policy enforcement	Data policy enforcement	Centralized visibility analytics	Analytics-driven command and control

identity credential and access management (ICAM)—one tool that systems can rely on to verify that particular people should have access to particular functions or features. In some cases, based on the size of the organization, federated ICAM solutions are needed.

MAKING THE MOST OF LOGS

Another major challenge is the proliferation of logs driven by zero trust's strong emphasis on continuous monitoring. Amassing countless new logs could overwhelm relatively small security teams. Organizations need to be smart and efficient in how they handle all that data.

Although the administration has introduced new advanced logging requirements, agencies aren't yet using all that data effectively within their security operations centers. On a continuous basis, it's important to evaluate what data is useful and what isn't—for instance, focusing on relevant data elements within broader data feeds.

What's more, organizations need to move away from retaining data in ways that are less cost effective for the long term. By adopting a data-driven cybersecurity approach, organizations can start using cloud-based solutions to store massive quantities of cybersecurity data for longer periods in a more cost-effective manner, which unlocks the benefits of security analytics at scale in real time. And this, in turn, can enable advanced cybersecurity that uses predictive analytics and turns threat intelligence into actionable insights.

Making investments in advanced technology like artificial intelligence (AI), machine learning (ML), and streaming analytics can help security teams make the most of their data, identify aberrant trends in network traffic, and get ahead of threats. For now, federal and defense agencies are just starting their efforts on this front, but increasingly they will be looking to the private sector to leverage such capabilities.

Over time, organizations can work toward implementing the architecture for a cloud-native, cyber-focused data pipeline for streaming analytics (threat hunt, detection, and compliance) and start to apply the principles of zero trust and data-driven cybersecurity to protect 5G and cloud-based networks.

ZERO TRUST IN 5G AND BEYOND

Imagine an adversary is out to steal and sabotage sensitive technology that underpins a major defense acquisition program designed to meet urgent military requirements. It could all start with a threat actor using 5G threat vectors to conduct espionage, compromise the supply chain, infiltrate a network, and move toward the target. Applying a zero trust mindset, however, could counter such threats with stringent authentication measures, network segmentation, and evolved threat hunting. This is one of two hypothetical scenarios our team developed using tactics and techniques from the MITRE ATT&CK® knowledge base to show the potential of **zero trust in 5G**.

Operators of 5G ecosystems need holistic security that includes zero trust architecture, 5G development, security and operations (DevSecOps), and a 5G workforce, as well as vulnerability research and embedded security. Zero trust principles can spread through the entire 5G architecture when analytics and automation are used to drive security improvements over time with policy updates aligned to the other pillars. The continuous development and deployment of new policies protects application authentication and access into the 5G network.

NEXT STEPS

EMBRACE ZERO TRUST WITH CONFIDENCE

The journey to zero trust starts with evaluating an organization's cybersecurity against a maturity assessment model and then designing, developing, and deploying solutions that are fit for purpose. Along the path to maturity, organizations may find certain zero trust capabilities already in place and can leverage near-term opportunities to make headway without significant investment. For more substantial zero trust efforts, there is the ability to request funding via the Technology Modernization Fund (TMF).

Importantly, security leaders can look to zero trust efforts at other agencies to glean lessons learned. For instance, the Defense Information Systems Agency (DISA) is developing a scalable prototype of a zero trust security solution known as Thunderdome. Also, the Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute for Standards and Technology (NIST) have recently published several pieces of zero trust guidance. As organizations leverage the growing body of federal guidance on zero trust and share lessons learned, U.S. national and economic security is sure to benefit.

- Agencies are drafting zero trust implementation plans to meet specific zero trust security mandates by the end of fiscal year 2024.
- The path to developing tailored solutions for zero trust starts with evaluating the current state of the enterprise's capabilities and gaps. Armed with a threat-centric understanding of where an organization is along the spectrum, it's possible to set future targets that help drive down operational risk and give rise to new solutions for pressing needs.
- Three notable areas of focus for cyber and data practitioners are dealing with data, identity management, and smart, efficient handling of logs and data.

EMPOWER PEOPLE TO CHANGE THE WORLD®

Trusted to transform missions with the power of tomorrow's technologies, Booz Allen Hamilton advances the nation's most critical civil, defense, and national security priorities. We lead, invest, and invent where it's needed most—at the forefront of complex missions, using innovation to define the future. We combine our in-depth expertise in AI and cybersecurity with leading-edge technology and engineering practices to deliver impactful solutions. Combining more than 100 years of strategic consulting expertise with the perspectives of diverse talent, we ensure results by integrating technology with an enduring focus on our clients. We're first to the future—moving missions forward to realize our purpose: Empower People to Change the World℠.

BOOZALLEN.COM