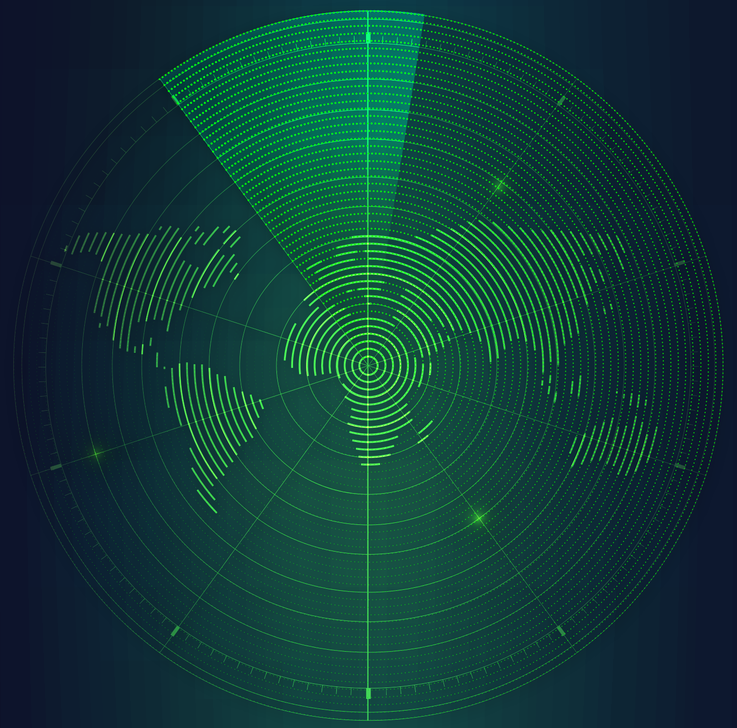
NTT DATA

Navigate the Labyrinth of National Cyber Defense

Where to begin for a clear and simple path
to zero trust for cybersecurity in government

What You Will Find Here



Introduction

The highest levels of the U.S. Department of Defense (DoD) recognize that for the United States to sustain its military advantage, it must treat cyberspace as a mission-critical battlespace. In recent years, we've seen how cybersecurity affects modern warfare and business alike, such as when Ukrainian organizations were hit by a destructive malware called *Whispergate* in early 2022.[1] *Whispergate* also crippled Ukraine's ability to access critical information required to make timely battlefield decisions. In February 2022, the "Russian invasion of Ukraine marked the first time that cyberattacks were used at this level in a full-scale war."[2]

Cyber warfare is fought on many fronts, and it also impacts the overall security of our nation. A May 2022 Cybersecurity and Infrastructure Security Agency (CISA) joint Cybersecurity Advisory indicated that threats to U.S. critical infrastructure are coming from both state-sponsored and criminal threat actors.[3] We predicted this battlespace change, and have developed and deployed cybersecurity plans, roadmaps and strategies for military components and government agencies.

However, those tasked with creating holistic approaches have found the required collaboration initiatives produce large, intricate and expensive plans. One example is the DoD Zero Trust Capability Execution Roadmap.[4] Another is the DoD Zero Trust Strategy.[5] Both are exceedingly detailed for decision-makers who need to see the bigger picture and aren't necessarily cybersecurity subject-matter experts. The result: difficulty finding a focused path to implementation, which may create accidental complications that blunt the effectiveness of the overall solution.

Our adversaries will seek out and exploit these issues. Because of that, we're still in need of clear, fast and simple practical solutions. Unfortunately, cybersecurity has been anything but simple for the past couple of decades.

Lost in a siloed cybersecurity complexity maze

Although inclusive, holistic and thorough, the cybersecurity plans developed over recent years have combined distinct siloed approaches that have evolved autonomously over decades. This evolution has left leaders with the difficult task of determining what works well across silos.

As the NTT 2023 Global Threat Intelligence Report states, "To mitigate the risks and minimize the potential impact of attacks, it is crucial for organizations and governments to invest in cybersecurity measures and raise awareness of cyberthreats. Doing this, however, cannot be a siloed effort."[2]

These silos and complex plans make it difficult for individual mission leaders to determine how to begin, how to prioritize among everyday real-time risks, and how to respond with specific solutions quickly and effectively.

Speed is also of the essence. In its roadmap, the DoD acknowledges the need for speed, "…aggressive approach that pushes start dates to the left as much as possible," but also admits that the plan, "**Does not** proscribe specific solutions to achieving the activities required." Thorough plans are essential to ensure adequate protective coverage and policies. Nevertheless, a maze of complicated cybersecurity approaches is slowing progress and inhibiting specific solutions.

Leaders need a straightforward approach and tactical solutions to reduce risk. The chosen tactic also must be implemented quickly and measured effectively. This eBook walks you through the maze to find the clear, effective and rapid solutions you need to protect the mission.

Three paths through the complexity maze

A zero trust architecture (ZTA) can provide tactical focus. It has both the best statistically proven methods to reduce cybersecurity risk and the required security at the current level of granularity needed for existing cloud-based IT environments.

Enterprise implementations aren't a simple undertaking, but the basic tools are available for simplification. The U.S. National Institute of Standards and Technology (NIST) created the now well-known ZTA conceptual framework and in Special Publication (SP) 800-207 describes the seven tenets required to design and deploy a ZTA.[6] These tenets can be summarized and simplified into three major categories:

- **Authentication** — the ability to identify and trust people, devices and locations
- **Monitoring** — the ability to see and learn from the IT environment and react appropriately
- **Authorization** — the ability to match access to trust in finer and finer granularity

These three categories offer viable paths through the cybersecurity complexity maze. They're the foundational basis of any ZTA and can guide a simplified enterprise implementation with technology maturity and continuous improvement capabilities.

A ZTA that uses simple, efficient and strong actions within these categories will create a solid starting point to help organizations move beyond the complexity and silos. At the DoD, it will allow the department to effectively protect our national security interests in cyberspace while allowing any planned strategies and roadmaps to progress for the long term. These actions will provide leaders with contextual understanding, visibility and control of the progress made toward their full cybersecurity goals.

Authentication path

The ability to authenticate, to identify and sort friends from foes, is always difficult in a complicated battlespace. It's doubly so in cyberspace, where both friend and foe operate freely. We must identify trusted team members correctly so they can accomplish their mission. At the same time, we must prevent untrusted actors from accessing sensitive information. The "never trust, always verify" authentication of identity must be reliable, user-friendly, seamless and robust.

Strong authentication is the best way to avoid attacks. Most cyberattacks don't come from an expert hacker or artificial intelligence, but from well-known methods and common vulnerabilities. Strong authentication easily disrupts these exact methods. Studies such as Microsoft's Digital Defense Report have shown that more than 90% of compromised accounts weren't protected with strong authentication and that basic security hygiene still protects against 98% of attacks.[7] However, only identifying people is insufficient to protect sensitive resources.

NIST SP 800-207 explains the relevant tenets for authentication apply not only to people but to all data sources, computer services, networks and resources. The DoD's Zero Trust strategy and plans acknowledge this, too. We must authenticate the device as well as the connection and location. Luckily, we have access to the most advanced and mature technology, and it's easy to implement.

Combining several common security protocols will achieve effective and efficient authentication. Multi-factor authentication for people, a cloud-based private access network for devices and connections, and a source signal tracker for location (such as IP address verification) will provide trusted authentication. This user-friendly combination offers a seamless, reliable path out of complexity and a solid basis for trust decisions. Much like the proverb "an apple a day keeps the doctor away," effective authentication can make a huge difference in stopping ransomware and other attacks.[8]

With each path, a stasis solution should be avoided. Our adversaries aren't going to keep to the same attack methods; therefore, dynamic solutions and continuous improvement must be included in all components. Dynamic authentication means that if any of the elements of authentication change, then all the authentication decisions will be reevaluated and the connection to resources cut off. In practice, dynamic authentication prompts the person to resubmit information and discontinues the process if the authentication fails. It's also an opportunity to learn what happened and how to improve the security environment. The key to a successful ZTA implementation is continuous improvement.

Monitoring path

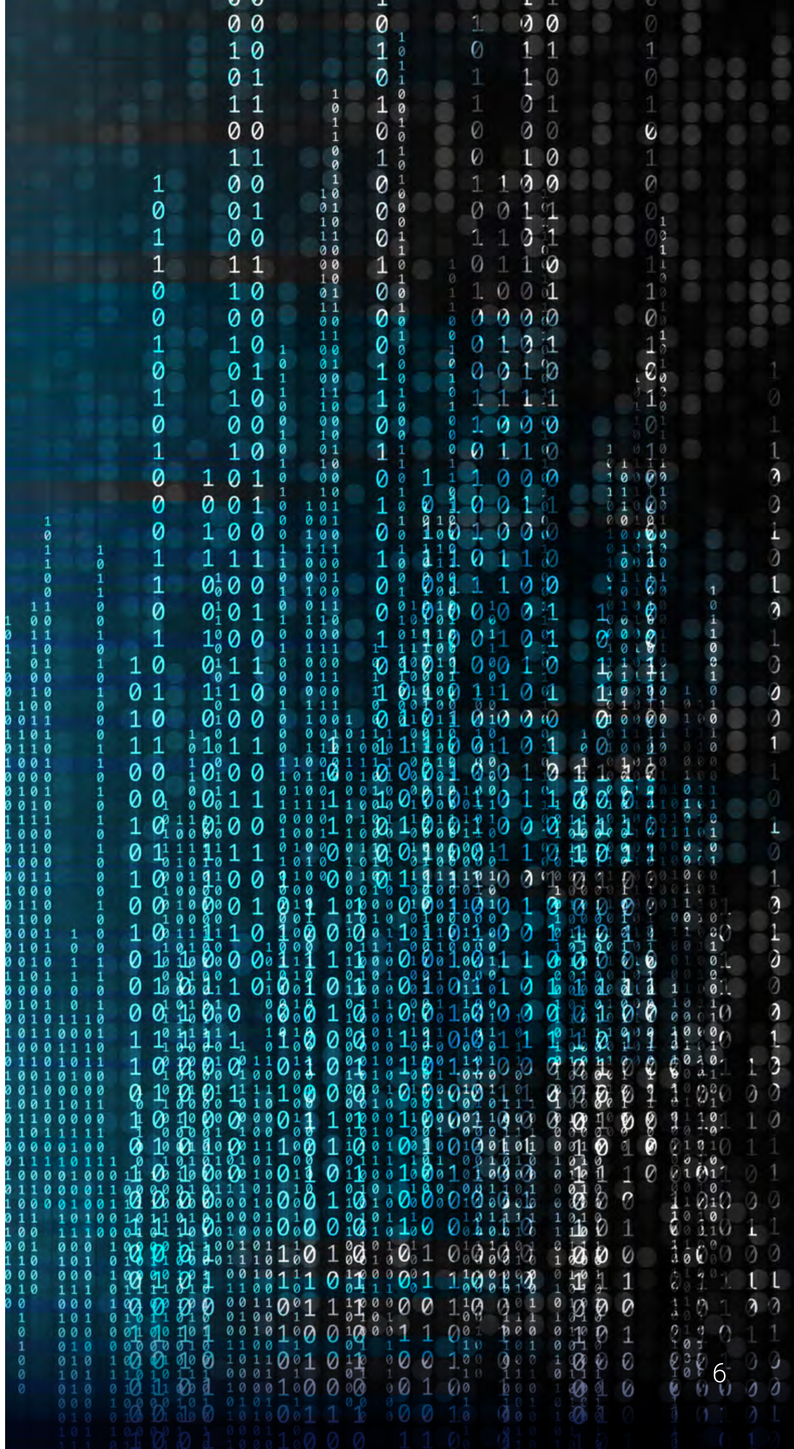
You can’t protect what you can’t see. Having insight into what’s happening is a force multiplier for mission effectiveness. Using sophisticated monitoring tools to keep tabs on the IT environment is a crucial component of maintaining the organization’s security. Technologies for monitoring have evolved to a sophisticated level in recent years. They’re now capable of tracking what’s happening on all trusted devices, providing new opportunities to observe and evolve.

The relevant NIST SP 800-207 monitoring tenets apply to all assets associated with the IT environment and require collection of as much information as possible.

Effective and efficient monitoring connects people, devices and places with events (such as attempted logins, downloads and probes). All collected data can be effectively evaluated with industry-leading tools.

Security information event management (SIEM); security orchestration, automation and response (SOAR); and extended detection response (XDR) cybersecurity incident management tools as well as data loss-prevention tools produce better tactical decisions, enabling a stronger defense protocol. These user-friendly tools provide the needed perspective for effective decisions and allow the organization to take appropriate and effective protective actions.

As with the previous path, the risk of stasis must be mitigated. Therefore, monitoring must include dynamic solutions and continuous improvement. Dashboards and other tools that provide insight into what’s going well and what needs improvement feed continuous improvement processes and inform those decisions. Often, investigating incidents also helps develop a list of lessons learned that can improve security processes.



Authorization path

Of the three paths, authorization is the most difficult to both deploy and implement. Authorization is the ability to dynamically match access to trust in finer and finer granularity in real time. The relevant NIST SP 800-207 authorization tenets include guidance for very fine-grained access and more complex control. The guidance recommends using dynamic policies with behavioral and environmental attributes (based on privileges granted at a point in time that can change at any time). They're continually dynamically evaluated and adapted due to altered conditions or requirements.

Most organizations today rely on role-based access control (RBAC) for authorization, where a role is associated with a group of people, all of whom are given the same access privileges. But RBAC is too problematic for national defense because it creates three significant issues:

- **Role accumulation,** where people accumulate roles over time and end up with more access than they need for their position
- **Role explosion,** where the organization creates more and more roles to achieve a finer grain of access control
- **Application brittleness**, where applications change, allowing access where it isn't allowed

There are also issues in finding where sensitive resources are located and if the appropriate access controls exist to protect those resources, called resource sprawl. The sensitive information and automation resources need fine-grain controls but are spread throughout the IT environment in unexpected or unknown places. To apply fine-grain access control, you need to know where that information is stored, how to classify it and how to associate the appropriate access. Additionally, you must map multiple instances of sensitive resources and numerous team members with each other correctly.

This combination of poorly fitted technology for the situation (RBAC) with inherent resource sprawl creates multiple opportunities for risk and abuse. We do know how to manage these types of issues in compartmentalized spaces. That said, those processes are arduous and expensive, and you can't generalize them to apply to this larger amount of information in cyberspace. We must search for a simpler, more cost-effective solution.

There are some interesting differences between the tenets associated with authorization that we didn't see with authentication and monitoring. For authorization, dynamic access control is part of every tenet and inherent in all authorization decisions. Given the limitations, we can see that RBAC isn't the best fit for authorization. However, two other excellent dynamic access control technologies will work much better for this path.

The best option currently available is Conditional Access control (CAC). Pioneered by Microsoft, CAC provides the ability to use information from monitoring and authentication to impact authorization decisions. This approach allows other attributes, such as geography, time of day and security readiness level, to impact authorizations. For example, if a trusted laptop with a strongly authenticated team member were to access the IT environment from a foreign country without prior authorization, it's possible to use CAC to deny access automatically.

The secret to good authorization is this combination of monitoring and authentication to inform the decision. With the right set of attributes, you can implement many dynamic controls that mitigate risk.

The other excellent authorization option using access control technology is called attribute-based access control (ABAC). ABAC allows for even finer-grain access control because it can use a wide range of attributes from enterprise systems to inform the authorization decision automatically. As an example, if a team member moves from one region to another, their access to information in the first region would automatically be unavailable because they no longer have the correct attribute, while access to resources in the new region would be granted automatically based on the new attribute.

Continuous dynamic improvement is baked into authorization more than either of the other two paths, but it will require more time and effort to evolve. Technologies developed to help with the resource sprawl issue continue to be refined. Those technologies help to discover sensitive information or resources and categorize them based on criteria established within the enterprise. As an example, technologies can now scan a SharePoint site collection and uncover all instances of unlabeled security information and then label it appropriately. Using that labeling technology with either CAC or ABAC can provide an effective mechanism for limited access.

Moving forward

It's essential that all the capabilities (or paths) are dynamic, fully integrated and connected to each other. As IT environments get more complex, the ability to detect that something has changed and automatically take appropriate actions will be ever more important. As important as identifying team members with outdated laptops or employees traveling to foreign countries is detecting a compromised device or intent behind unusual behavior, be it malicious or unintentional.

The dynamic component of ZTA is truly the hardest and the most likely to cause difficulties in an organization. Any time responses to changing conditions are automated, it creates both intentional and unintentional repercussions. The key is to keep constantly refining the processes, tools and methods to minimize any unintentional negative impacts.

For those entrusted with the security of an organization's information systems, a balance of achieving cybersecurity while not breaking the bank is essential.

The ZTA paths and actions detailed here provide a way to focus on those solutions that will produce the greatest impact at a moderate cost. They provide a framework for understanding and a place to start in implementing what's necessary for an adequate level of cybersecurity.

Finally, creating an organization with a continuous improvement cycle based on strong protection, in-depth monitoring and constant evaluation is the best way to stay ahead of threats today and in the future.

Visit **our site** to learn more about NTT DATA's cybersecurity solutions for government.

Sources

1 Microsoft Digital Security Unit (DSU), Microsoft Incident Response, Microsoft Threat Intelligence. "Destructive malware targeting Ukrainian organizations." Microsoft Security Blog. January 15, 2022.

2 NTT Security Holdings. "2023 Global Threat Intelligence Report." May 30, 2023.

3 Cybersecurity and Infrastructure Security Agency. "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure." Cybersecurity Advisory (Alert Code: AA22-110A). May 9, 2022.

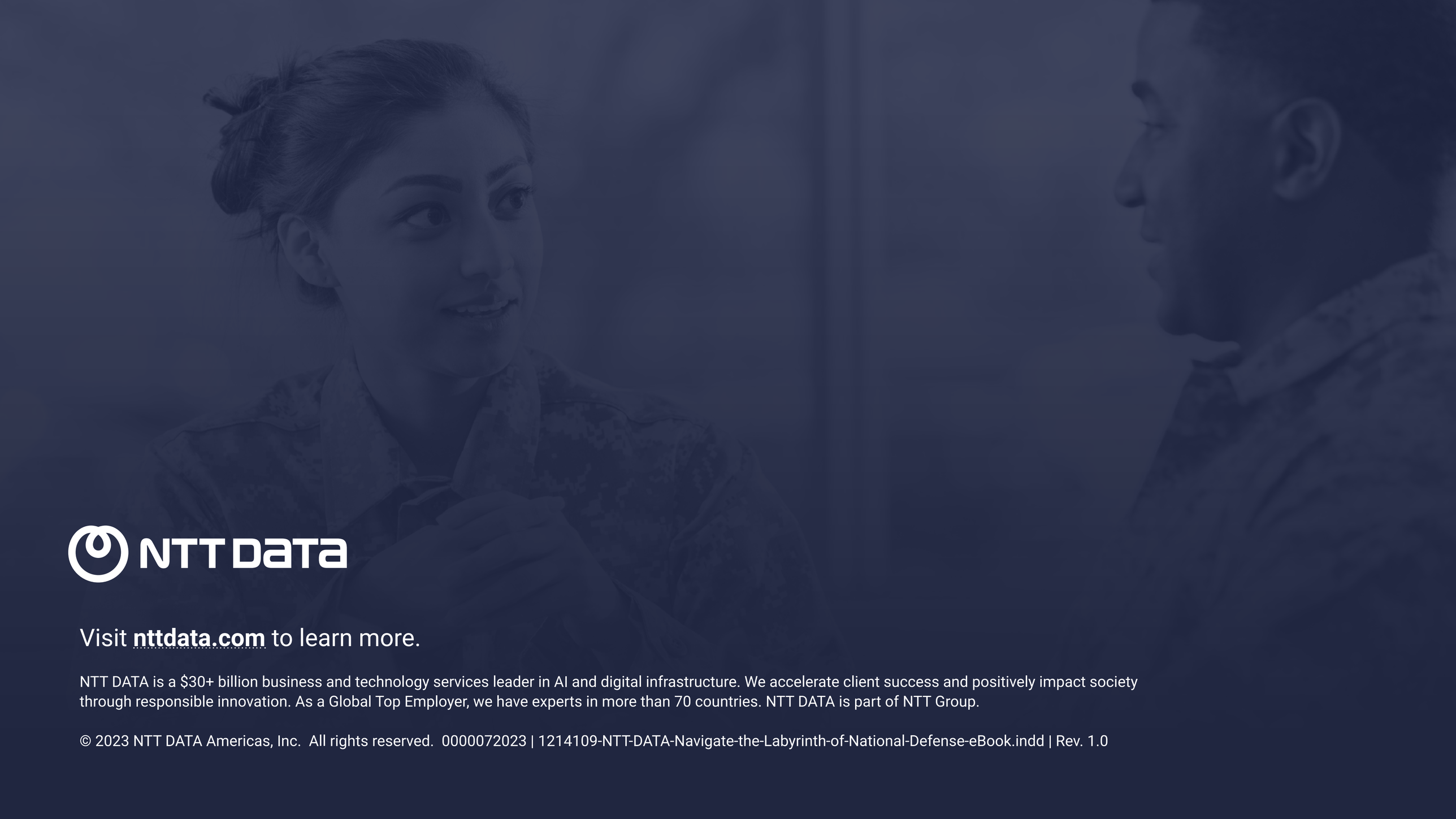
4 U.S. Department of Defense, Office of the Chief Information Officer. "DoD Zero Trust Capability Execution Roadmap (COA 1)." January 6, 2023.

5 U.S. Department of Defense, Office of the Chief Information Officer. "DoD Zero Trust Strategy." October 21,2022.

6 Scott Rose, Oliver Borchert, Stu Mitchell and Sean Connelly. "NIST Special Publication 800-207: Zero Trust Architecture." U.S. National Institute of Standards and Technology. August 2020.

7 Microsoft Corp. "Microsoft Digital Defense Report 2022: Cyber Resilience." Microsoft Security. 2022.

8 Nat Bongiovanni and Marta Czarnecki. "An A.P.P.L.E. a Day Keeps the Ransomware at Bay." 2023.



NTT DATA

Visit **nttdata.com** to learn more.

NTT DATA is a $30+ billion business and technology services leader in AI and digital infrastructure. We accelerate client success and positively impact society through responsible innovation. As a Global Top Employer, we have experts in more than 70 countries. NTT DATA is part of NTT Group.