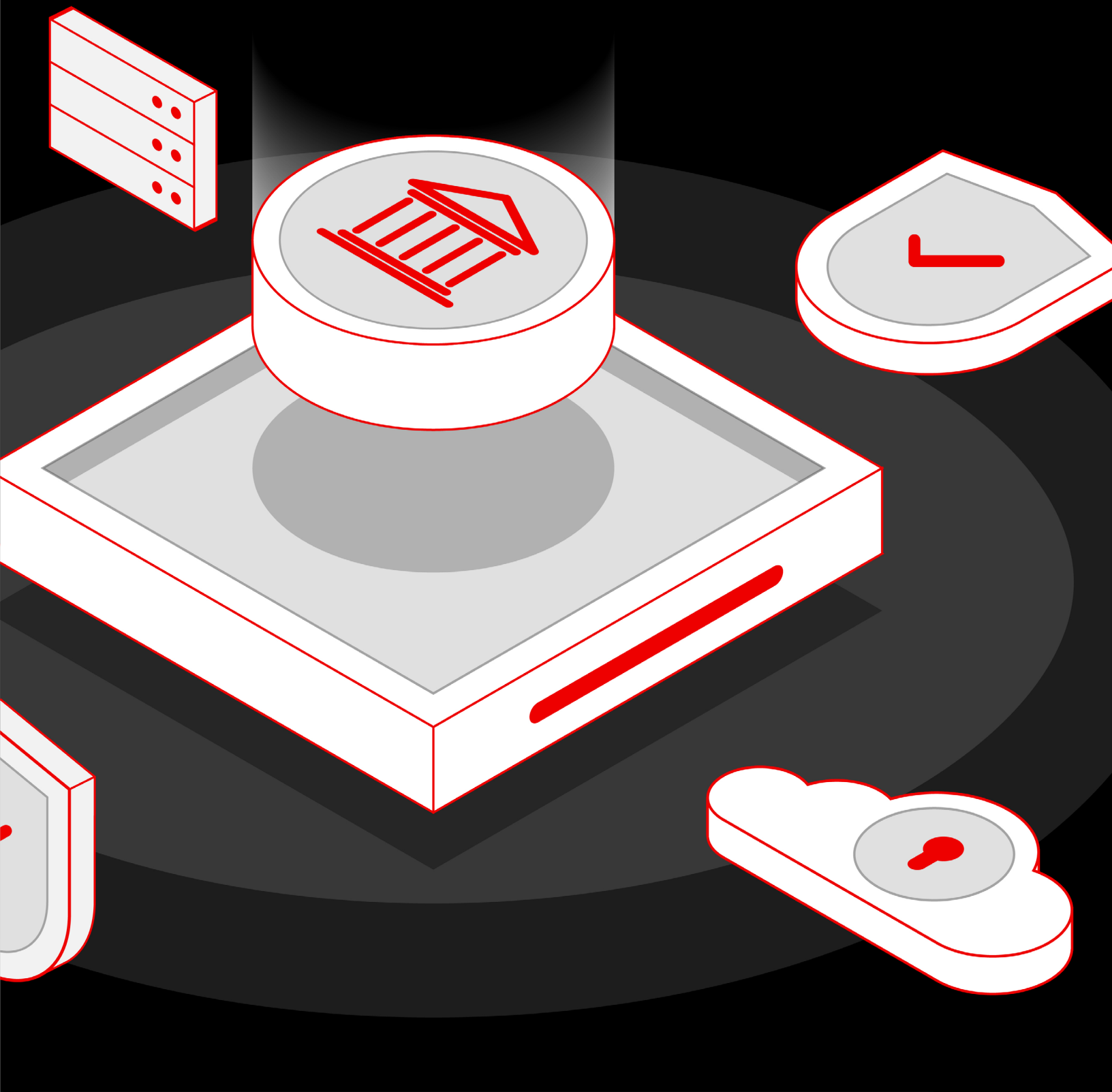
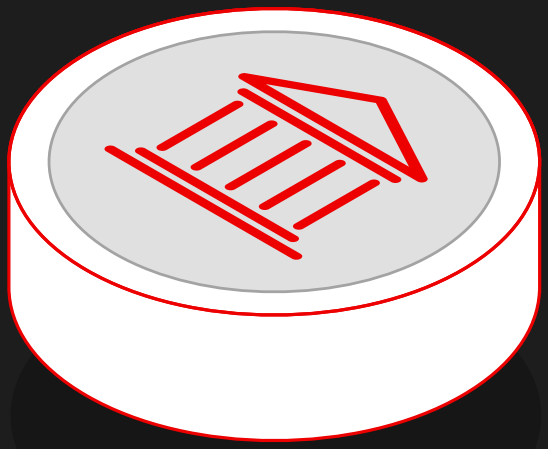
Red Hat

Zero trust security
for government agencies

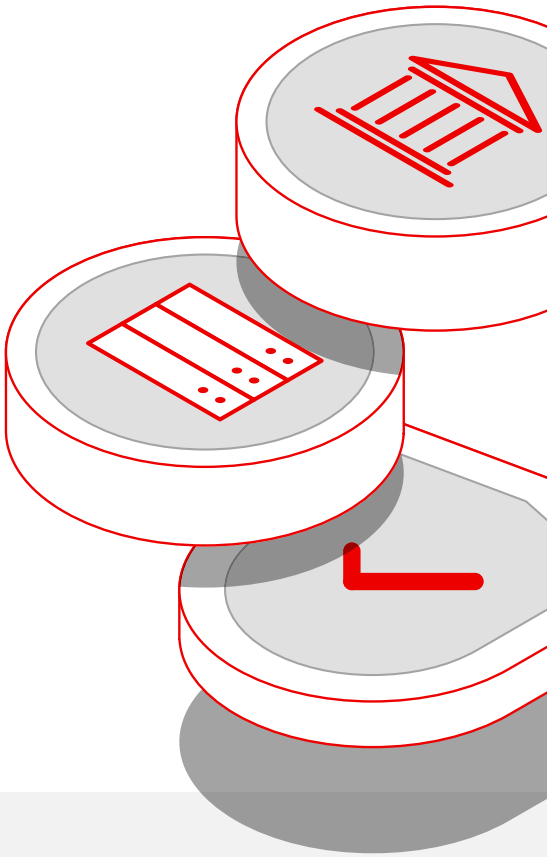


Contents



Introduction

What is a zero trust approach and why does it matter for IT security?



In the evolving landscape of IT security, government agencies face increasingly sophisticated cyber threats that traditional security models are not equipped to address.

Traditional perimeter-based approaches rely on a strong outer defense to protect internal resources, have proven inadequate in the face of modern risks like advanced persistent threats, insider attacks, and the proliferation of mobile and cloud computing. Recent examples of security breaches include the US public sector as well as high profile breaches at well-known organizations such as Disney, AT&T, Helsinki City Council, and JPMorgan Chase.[1]

In 2021, the White House recognized these challenges and issued an Executive Order mandating that a zero trust (ZT) security approach be adopted across all federal agencies. This directive marked a major shift in how government agencies must approach cybersecurity, emphasizing the need for a more resilient and adaptive security posture.

After the Executive Order was released, in order to accelerate the adoption of the full set of zero trust capabilities, the Department of Defense (DoD) released the strategy and Course of Actions (COAs) in winter of 2022. The DoD COA includes the DoD Zero Trust Capability Roadmap which describes how the Department currently envisions achieving the capability-based outcomes and activities sequenced over time to achieve the DoD Target Level ZT and Advanced ZT maturity levels.

[4] Drapkin, Aaron. "Data breaches that have happened in 2022, 2023, and 2024 so far." Itech.co news, accessed 30 July 2024.

Zero trust security defined

Zero trust is an approach to designing security architectures based on the premise that every interaction begins in an untrusted state. Instead of assuming that entities outside or even inside the network are trustworthy, zero trust operates on a simple principle: never trust, always verify.

Zero trust aims to close gaps in security architectures that rely on implicit trust models and single instance authentication. This rigorous and continuous verification process effectively addresses the weaknesses of the perimeter-based model, providing robust protection against both external and internal threats.

By addressing the vulnerabilities of traditional security approaches, zero trust can enhance the resilience and security focus of public sector IT environments, to safeguard sensitive data and critical infrastructure.

The shift to zero trust is not simply a technical adjustment but a strategic one as well. Organizations will also need to consider:

1. **How they can advance risk management from the top down** starting with business processes, such as access controls, rather than solely focusing on securing existing systems based on traditional confidentiality, integrity, and availability models.
2. **The integration of observability and contextual telemetry** into access control and business systems, so that decisions are informed by real time insights.
3. **Adopting an inventory process that is asset-oriented rather than system-oriented**, emphasizing a comprehensive understanding of every asset's role within the broader business context.

Adopting these considerations into your zero trust strategy can help federal organizations align with the wider government mandates and set new standards for cybersecurity in the public sector.

This e-book takes a closer look at the overarching principles of zero trust to help organizations become familiar with and adopt a zero trust security approach.

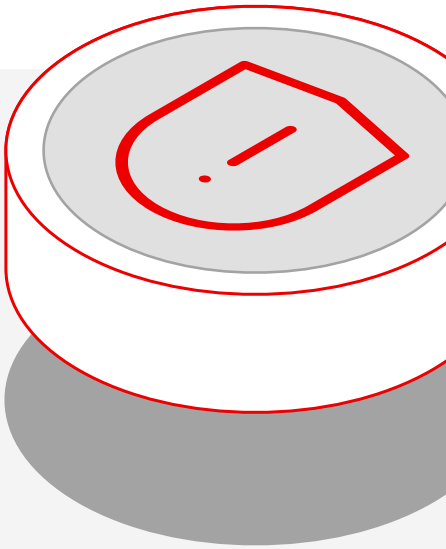
Chapter 1

An introduction to the principles of zero trust

Zero trust principles start with making security a foundational component of all projects, whether developing new products or implementing new infrastructure.

Instead of building security around network access alone, a zero trust architecture, as described by the National Institute of Security in Technology (NIST), is built into every digital interaction as a practice across the organization.

While there are different approaches to zero trust, the following 6 principles can help organizations prepare for and adopt zero trust security.



1. Protect surfaces versus attack surfaces

A government agency can have any number of areas in their IT infrastructure that need to be protected, such as data and critical systems. These areas, known as protect surfaces, will be a catalog of all assets requiring protection and is why inventorying is so critical for any size agency or organization.

Rather than trying to address the entire attack surface of a system, which will likely include vulnerabilities and attack vectors which are of low risk in the context of a particular system, the process of defining a protect surface focuses efforts on defining microperimeters that directly reduce risk.

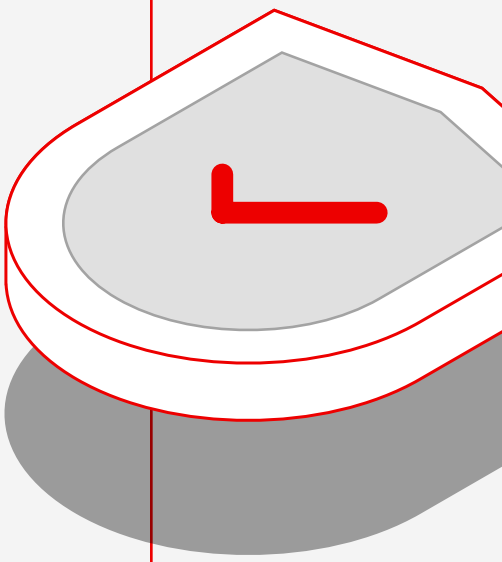
This can be much more manageable for an enterprise than addressing entire attack surfaces, which may include thousands of common vulnerabilities and exposures (CVEs) spread over many different software or hardware deployment targets and physical locations. The protect surface of a system can be defined by an exploration of the risk and sensitivity levels of each component.

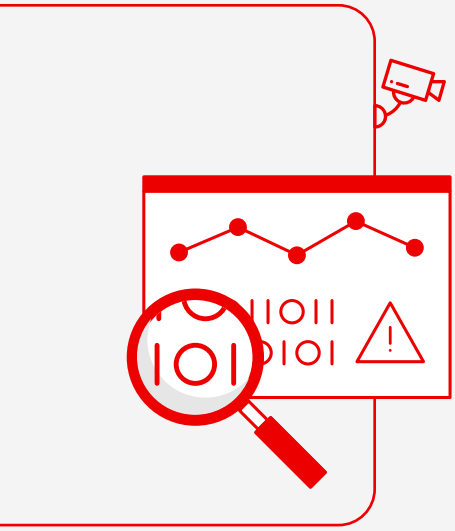
2. Assume breach

This principle assumes that an attacker is already within your defensive security perimeter and that any or all traditional perimeter based security controls are no longer effective. This means that you cannot rely on these controls to mitigate further malicious actions or reconnaissance by that attacker within the overall system or enterprise.

Hostile actors are everywhere and constantly attacking systems, with varying levels of success. Even if an enterprise is not involved in an active security breach, insiders are by definition already operating within a defensive security perimeter and can go rogue in very damaging ways because of that advantage. Most enterprises are also subject to open vulnerabilities and unpatched systems due to the time it takes to patch and update systems, which provides a target rich environment for insiders.

The goal of "assume breach" is not to keep you up all night worrying about your IT systems, but to encourage you to structure your security posture in a way that inherently reduces the impact of any new or ongoing attacks from the perspective of assuming the enterprise always has bad actors actively operating within it.





3. Never trust, always verify

Airport security never assumes, and always verifies that a flier's risk level is low, and doesn't possess prohibited items even though they have a valid ID and boarding pass. In the same way, an IT system should not make assumptions about an entity's risk level and grant access to a resource simply because of static credentials.

The risks to a system should be identified, and applicable implicit trusts eliminated, which can be many and varied. For example, the current identity and threat-level of a user, their device, the data being sent into or transferred out of a system, the connection method used to access a resource, and more.

4. Explicitly scrutinize

Any use of information in a system must be explicit, including all information dependencies. Under this principle, the idea of least privileged access applies, which is an information security concept that requires all users to be limited to only have access to the specific data, resources, and applications necessary to complete their required task. This strategy creates self-contained and complete information dependencies, improving the consistency of policy enforcement and the security posture of the system.

5. Apply unified and dynamic analytics

This principle specifies that analysis of a system must be performed completely, consistently, and continuously in order to determine the actual behavior, context, and risk for any action taken against a resource. The goal is to build a robust means of performing security analysis and incorporation of current results into your policies and enforcement points. This practice directly supports the principles of "explicit scrutiny" and "never trust, always verify" by providing the context necessary to inform those decisions.

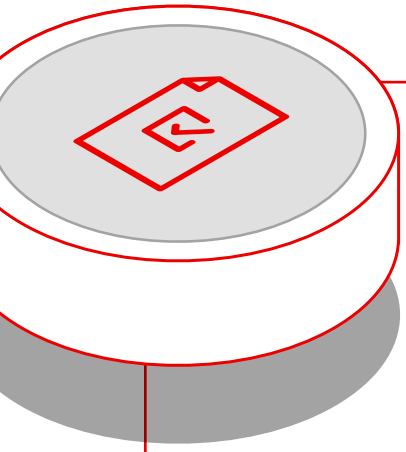
Assessing your zero trust maturity

There are many different maturity models that may represent a successful zero trust implementation, and these maturity models depend largely on the makeup of the organization.

Evaluating the maturity of your organization against a zero trust maturity model such as the Cybersecurity & Infrastructure Security Agency (CISA) model can help:

1. Provide an understanding of your current security posture and identify gaps that need to be addressed to achieve greater protection against cyber threats.
2. Extend your security evaluation to not only include technology but also policies, processes, and the cultural shift necessary to adopt a zero trust mindset.
3. Grow your team's understanding of your maturity level so you can make more informed decisions about resource allocation, prioritize initiatives, and create a roadmap for enhancing your security infrastructure.
4. Ensure compliance with Federal mandates, including the Executive Order on Improving the Nation's Cybersecurity.

To determine zero trust maturity, public sector organizations can follow 5 key steps.



Step 1

Conduct a baseline assessment

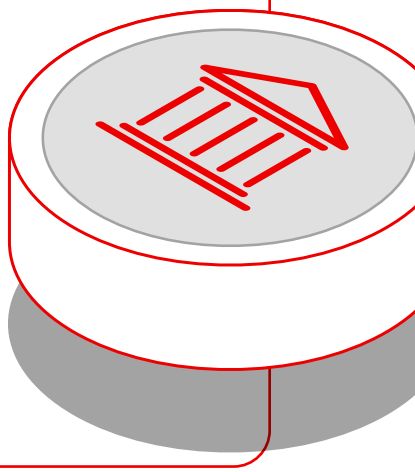
Begin by mapping your existing security architecture, policies, and practices. This involves cataloging all assets, including devices, users, applications, and data flows. Understanding your current security posture gives you a baseline to measure success over time.

Step 2

Evaluate key pillars of zero trust

Assess your organization against the core components of a zero trust architecture including: identity, device, network, application, and data security.

For each component, determine the level of integration and effectiveness of zero trust principles. For example, examine how identities are managed, how devices are authenticated, and how network traffic is monitored and segmented.



Step 3

Identify gaps and prioritize actions

Based on your assessment, identify gaps where your organization falls short or where there are inconsistencies. This might include access controls, lack of continuous monitoring, or where data encryption is not fully implemented. Prioritize these gaps based on the level of risk and potential impact they have on the organization.

Step 4

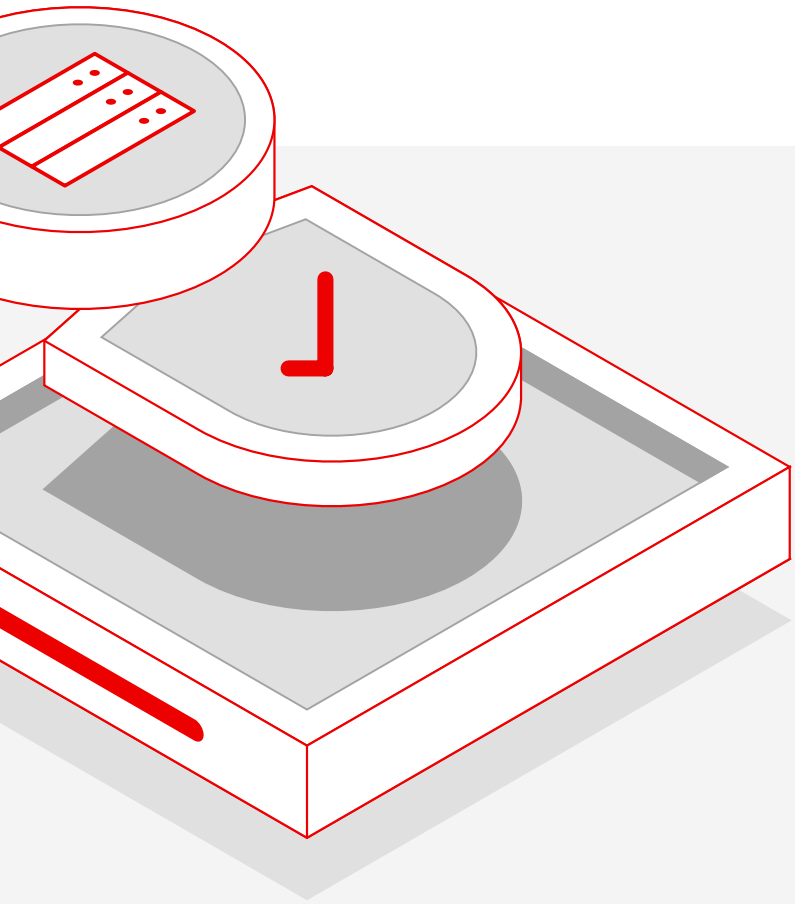
Develop a roadmap for implementation

Create a strategic plan that outlines specific initiatives to enhance your zero trust maturity. Consider where competing priorities, application and service lifecycle, and maturity of tools and infrastructure, among other considerations will factor into your implementation.

Step 5

Foster a zero trust culture

In addition to technical measures, fostering a culture of zero trust within your organization is essential. This may involve educating and training staff on zero trust principles, encouraging collaboration between teams, ensuring that security is integrated into every aspect of operations, and promoting a mindset where trust is continuously verified.



By assessing and enhancing your zero trust maturity, public sector organizations can better protect critical assets, ensure compliance with federal cybersecurity mandates, and build a resilient defense against evolving cyber threats.

Choosing the right maturity model for your organization

The US government has promoted several maturity models to measure the effectiveness of a zero trust implementation, for example the Department of Defence (DoD) security model and the CISA model in Figure 1.

CISA ZTA perspective

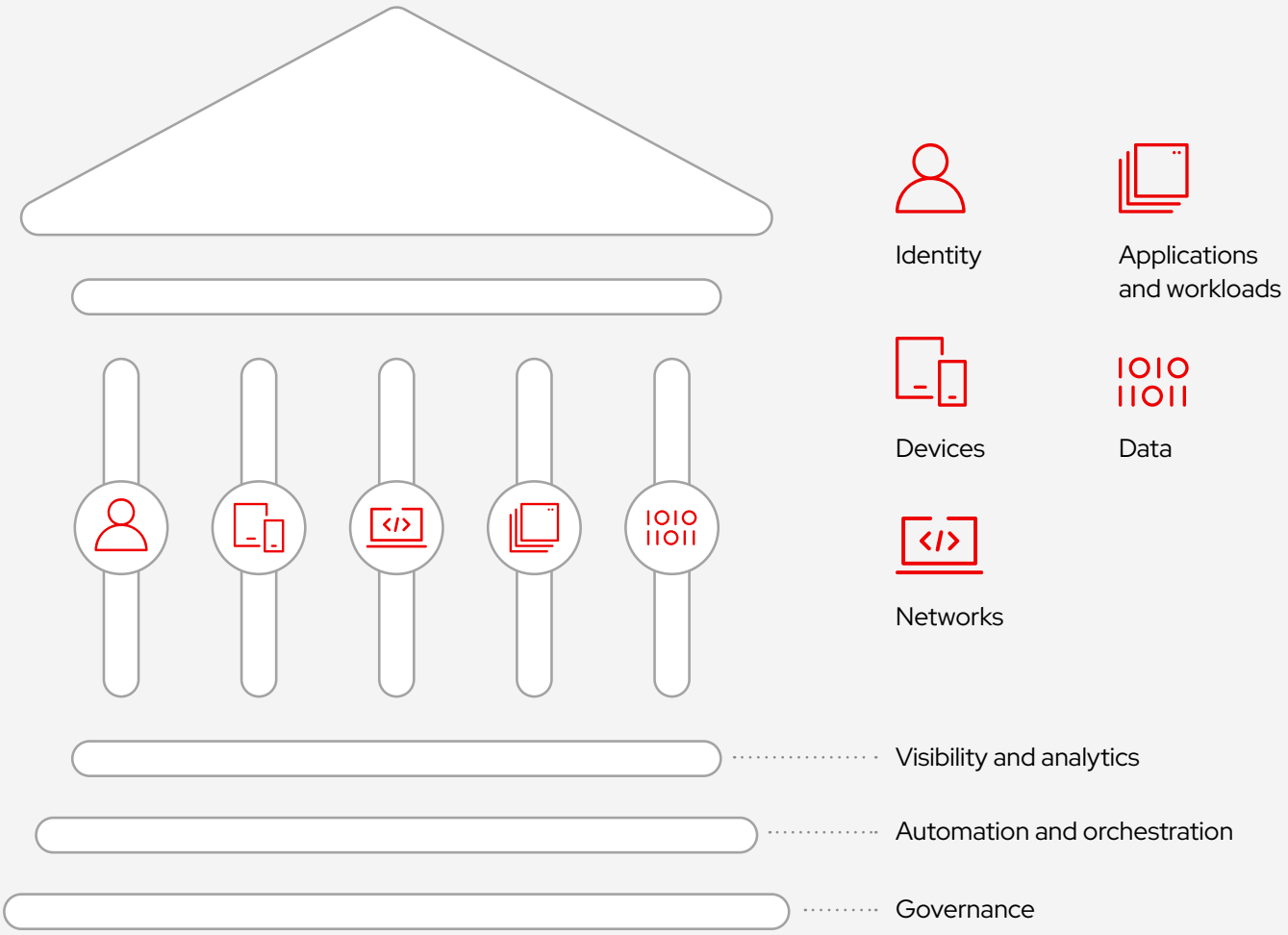
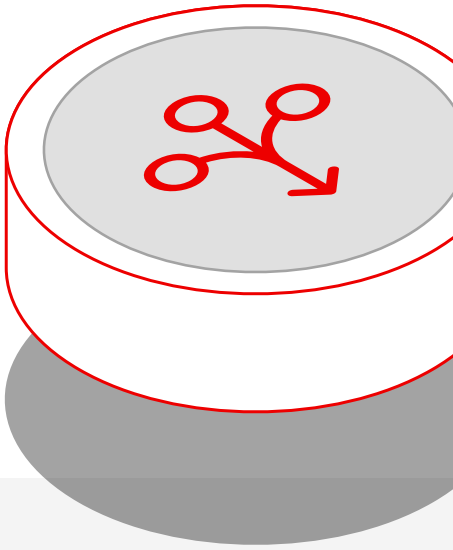


Figure 1. Zero trust maturity model for the Cybersecurity & Infrastructure Security Agency (CISA).

Chapter 2

Capabilities, architecture, and cybersecurity

To maximize the effectiveness of your zero trust security approach, it's important to understand the relationship between capabilities, architecture, and existing cybersecurity measures. Let's take a closer look at these 3 components.



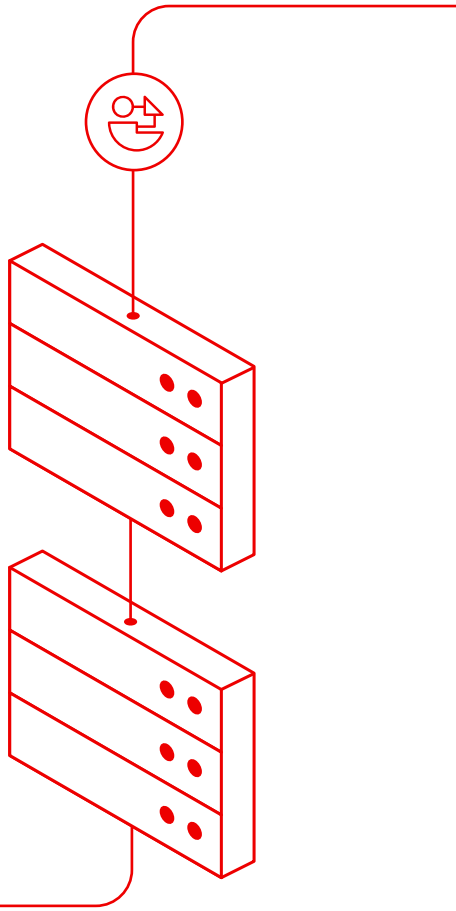
1. Capabilities

In the context of zero trust, capabilities may include tools, technologies, and processes such as identity and access management, multifactor authentication, encryption, continuous monitoring, and analytics. These capabilities still need to be used correctly and consistently with zero trust principles. While many organizations will claim they have adopted zero trust, the true value is only present when these capabilities are part of the organization's zero trust architecture.

> **What to watch out for:**
>
> It is equally important to avoid using capabilities that might be present in your enterprise that would bypass or weaken your zero trust approach, such as account credential resets that rely solely on single factor authentication like a security question or insufficiently secured central management systems which have broad access across the enterprise.

2. Architecture

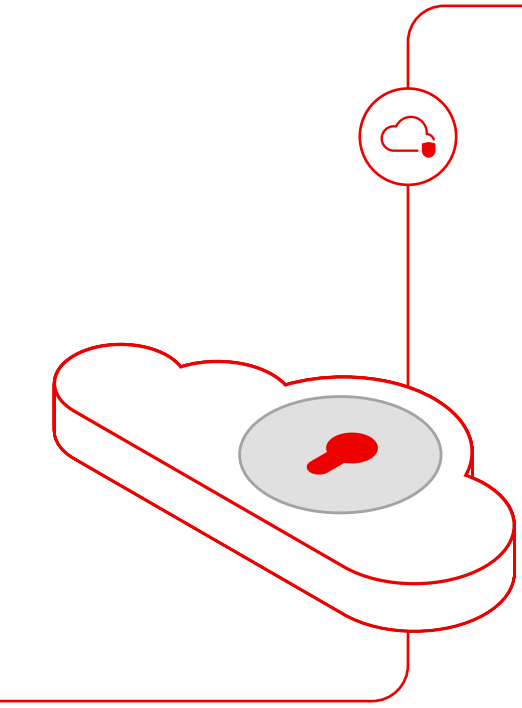
Architecture is the structural design of an organization's IT environment, encompassing hardware, software, networks, and data flows. For zero trust security, the architecture is what ensures the capabilities you have are used correctly and effectively.



What to watch out for:

Watch out for process and technology gaps. For zero trust to be implemented effectively, all interactions between entities and resources need to be mapped out and understood, with visibility and control points built into the architecture that are capable of enforcing policies at the appropriate system layer (network, application, database, etc.).

Strive for simplicity over complexity, as complexity itself can be a security liability. Try not to layer tooling on top of other tooling unless absolutely necessary, and choose tooling and platforms that inherently provide zero trust aligned capabilities versus those that need to be excessively configured and customized to achieve your goals.



3. Cybersecurity

While zero trust security represents an evolutionary approach to cybersecurity practices, traditional cybersecurity measures such as firewalls, endpoint detection and response software, and threat detection systems remain essential. These traditional elements provide foundational defenses that should contribute to the dynamic and granular protections offered by a zero trust approach.

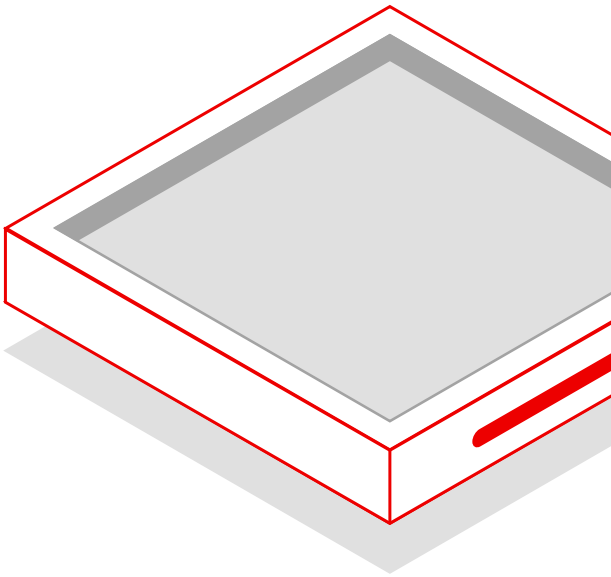
What to watch out for:

Avoid zero trust solutions that might weaken or compromise your existing cybersecurity posture and traditional cybersecurity tools that have been repackaged and reclassified as zero trust tools, and cybersecurity tools that don't offer open APIs and open standard interfaces or protocols. These solutions will lack the flexibility and interoperability needed to effectively architect an integrated zero trust ecosystem in your enterprise.

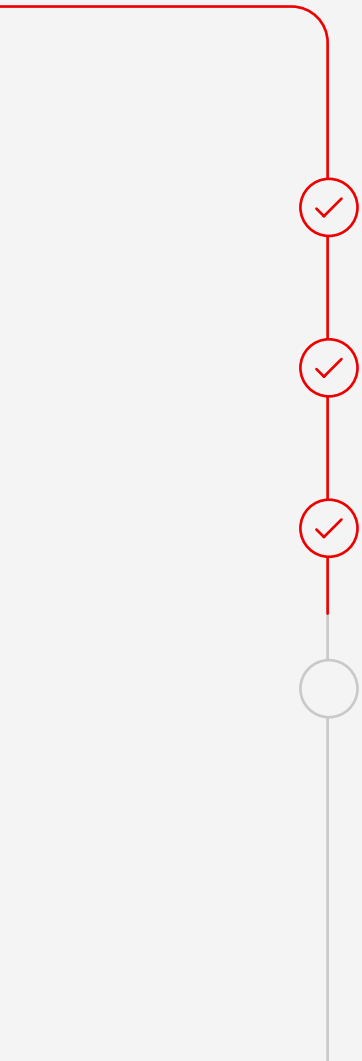
Implementing a zero trust architecture does not require a comprehensive replacement of existing networks or massive acquisition of new technologies. Instead, the framework should strengthen other existing security practices and tools.

Chapter 3

How Red Hat can help you implement a zero trust architecture



A challenge that many organizations encounter when adopting zero trust is the large number of specialized cybersecurity tools and vendors in the zero trust space that provide niche solutions and capabilities.



While these point solutions can contribute to a strong zero trust posture, they are most effective when implemented as integrated components of a cybersecurity architecture grounded in zero trust principles.

There has been a strong focus in government and industry on certain aspects of zero trust, such as network controls and identity. Zero trust maturity also requires controls within the mechanisms and infrastructure that develop, deploy, and run applications to effectively make zero trust a first class citizen in systems design. Red Hat's approach to zero trust focuses on controls within every phase of the software development lifecycle for those organizations building applications, and for all organizations, controls within the Linux® operating system up through infrastructure management and into application runtimes themselves.

As a leader in secure focused infrastructure and software development, Red Hat provides expertise and foundational technology that organizations can use to design, build, and manage applications and architectures that imbue zero trust controls and principles into new and existing infrastructures and processes. Red Hat has a long history of collaboration with ecosystem partners, and its open source software development model facilitates interoperability and compatibility with other zero trust-enabling technologies. Zero trust architectures are almost always implemented with platforms from multiple vendors, and it is important to consider interoperability when choosing new technologies or evaluating existing ones.

Advance zero trust maturity from traditional to optimal

Figure 2 illustrates a graduated zero trust model, where the 7 pillars of the architecture mature from traditional to optimal over time. Red Hat has a tailored consulting process designed to help government agencies assess their maturity with respect to zero trust in order to plan a roadmap for improving the organizational capabilities and maturity.

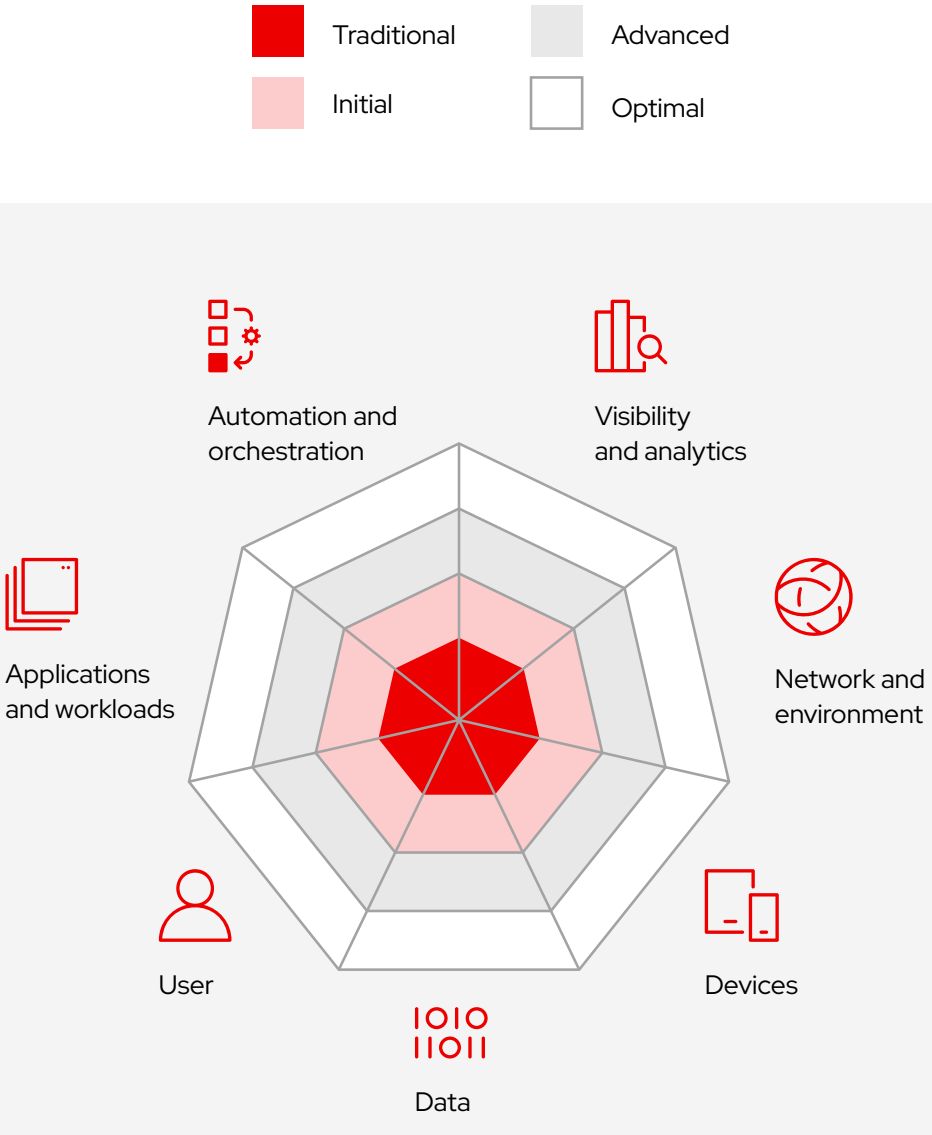
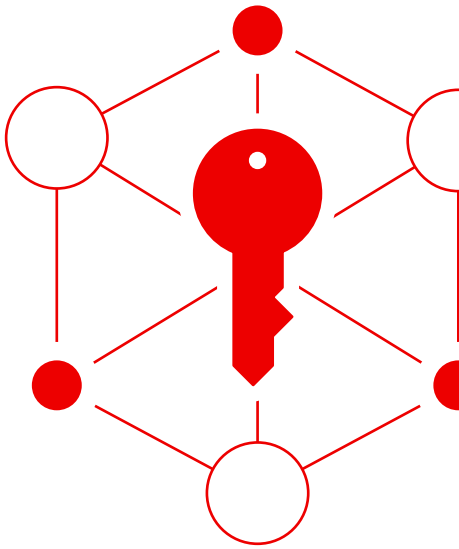


Figure 2. Zero trust maturity stages.

Assessing and implementing zero trust with help from Red Hat



To better understand how Red Hat can help government organizations adopt a zero trust security approach, let's take a look at how Red Hat solutions apply to the 7 key pillars of the maturity model in Figure 2, and how they can help advance your organization's zero trust security approach.

Red Hat® Enterprise Linux makes security a part of the infrastructure and product lifecycle from the beginning.

By taking a defense-in-depth approach that uses automation and shared intelligence, Red Hat can help government agencies mitigate the risk of being exposed to vulnerabilities.

To maintain a security-focused environment with minimal downtime, Red Hat provides live patches and remediation included with subscription. Red Hat Enterprise Linux's independently validated and certified operating system reduces compliance barriers to help organizations stay focused on security, compliance, and being audit-ready.

Red Hat Enterprise Linux provides a security-focused foundation from which you can build and scale a zero trust architecture consistently across bare-metal, virtual, cloud, container, and edge footprints.

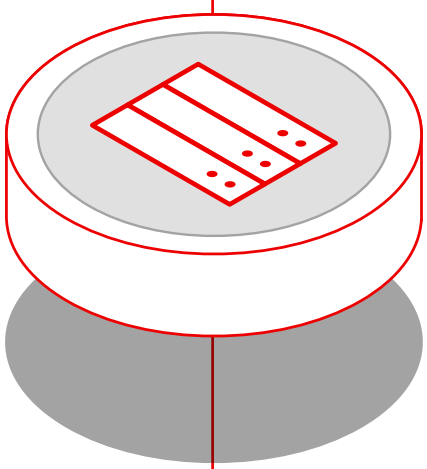
Red Hat Enterprise Linux can help advance zero trust maturity for:

- **Devices.** Gain baseline device hardening, host-resource labeling and mandatory access controls, attestation services, and hardware and application virtualization workload separation.
- **Networks and environments.** Ensure Federal Information Processing Standard (FIPS) compliant cryptography for network services.

Red Hat Ansible® Automation Platform can help government agencies achieve the automation and orchestration maturity necessary for zero trust architectures.

Automation and orchestration are foundational tenets of a mature zero trust architecture for a good reason: these capabilities are necessary to dynamically and consistently enforce multitiered compliance and access policies across complex and heterogeneous IT estates which are not as effective when hampered by manual or static processes. Red Hat Ansible Automation Platform is purpose-built as an enterprise-ready, certified, open source automation solution with documented, reproducible supply chains to help government agencies streamline daily operations and integrate security into processes, applications, and infrastructure consistently across disparate teams which are likely operating on different zero trust pillars.

This cross-collaboration and consistency is critical to allow organizations to effectively structure zero trust control sets that involve multiple systems and controls across multiple pillars, which involve multiple factors and deep context derived from the evaluation of many data sources such as user entity behavior analytics, user and system attributes, and allow lists. A robust general-purpose automation solution which can interact with all the control/enforcement components of a complex system provides the agility to meet the demands of a zero trust architecture and increase an organization's zero trust maturity.



Ansible Automation Platform can help advance zero trust maturity by:

- **Allowing cross-pillar consistency and coordination** of zero trust controls on all assets in an IT system, including multivendor end-user and server devices, network and security infrastructure, identity management solutions, multicloud infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) environments and more.
- **Adding agility and dynamism** into existing manual and static remediation, configuration management, and analytics processes to allow teams to operate quickly to meet the requirements of zero trust or trigger automations based on real time events.
- **Providing auditable and verifiable** configuration-as-code automation templates which are source-code-controlled and cryptographically signed, ensuring comprehensive observability and auditability of these mechanisms.

Red Hat OpenShift® Container Platform is a foundation for developing and deploying workloads following zero trust principles.

With the right development and hosting platforms, government agencies can adopt zero trust architecture with 'out of the box' capabilities for specific zero trust techniques and domains. For example, Red Hat OpenShift Service Mesh provides bidirectional cryptographic identities and application layer network and micro-segmentation of applications components. Red Hat OpenShift also delivers a foundation for incorporating zero trust principles early in the software development process with Trusted Application Pipelines, incorporating Software Bill of Materials (SBOM) validation, artifact signing, and more to eliminate implicit trusts within the software supply chain as "far left" as possible. OpenShift's zero trust controls also extend to deploy/run stages of the SDLC with container security/network monitoring and workload segregation provided by Red Hat Advanced Cluster Security. These and other zero trust aligned capabilities are available within Red Hat OpenShift across on-premise, managed and unmanaged public clouds, providing consistent zero trust controls which are independent from the underlying cloud service provider's offering.

Red Hat OpenShift helps you adopt zero trust by providing opinionated security controls and automated enforcement points across the application stack and development and deployment processes. Built with open standards, protocols, and APIs, OpenShift readily integrates with other components of an enterprise's zero trust architecture, connecting to zero trust control planes for access decisions and providing audit and event data streams back for behavioral monitoring and analysis used for contextually-aware decisions.

Red Hat OpenShift can help advance zero trust maturity for:

- **Networks and environments.** Red Hat OpenShift Container Platform for application software-defined network (SDN) configured with open source service mesh (OSSM) for end-to-end mutual encryption and workload identity-based access policies. Advanced cluster security also provides real-time network monitoring and control of workload component communications.
- **Applications and workloads.** Red Hat OpenShift Service Mesh provides a uniform way to connect, manage, and observe microservices-based applications. OpenShift, especially when combined with Advanced Cluster Security, also provides many inherent visibility and control points within a build, test, and run application pipeline.

Chapter 4

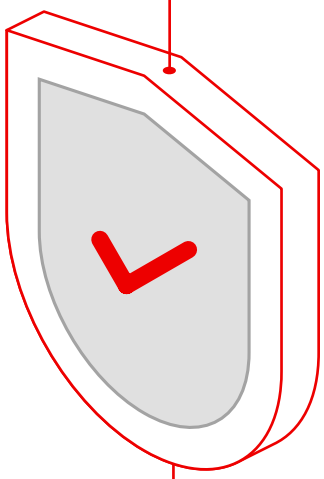
Zero trust security: How to know when you have succeeded

When adopting a zero trust security approach, it's important to think of it as an ongoing journey rather than a fixed destination.

Choosing the right maturity model that suits your organization will provide you with the framework needed to assess your current security posture, set goals, and prioritize the right actions for ongoing improvement.

Promote consistency across systems and missions

An important benefit of using a maturity model is promoting consistency across systems and how they help fulfill larger governmental security goals. Consider comparing your current security measures against the targets outlined in your model, this can help you determine where you are in your process of moving to zero trust architecture, identify inconsistencies, and plan to effectively address these gaps.

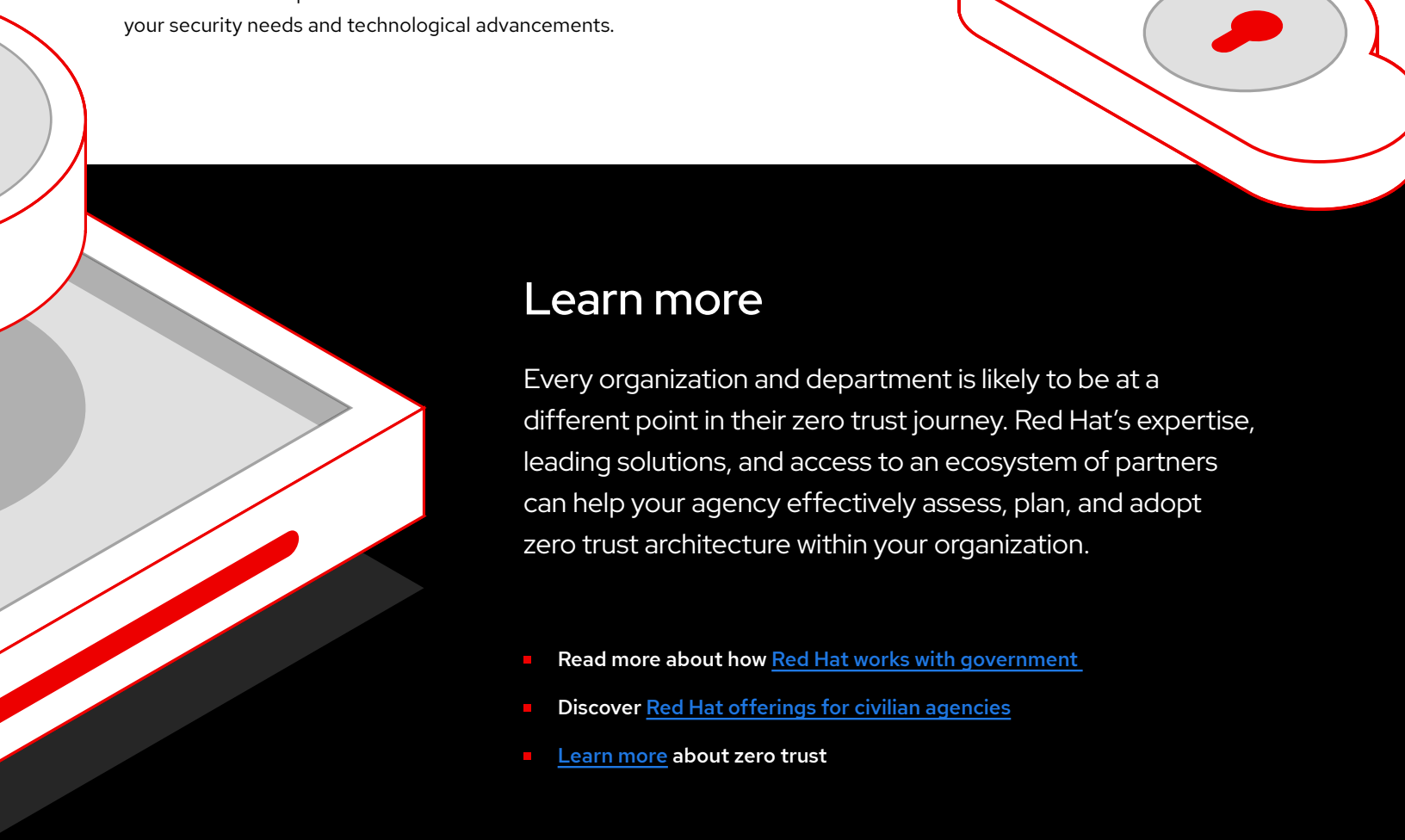


Red Hat's approach to zero trust maturity models

Having seasoned security expertise guide you on your zero trust journey can provide valuable guidance to help you prioritize goals and strategies for building zero trust architecture.

Red Hat's experts aim to use the most comprehensive maturity models available. Currently, we view the Department of Defense (DoD) model as the most complete and align our portfolio of solutions with where we expect most adopters of zero trust architectures to be, but can translate to other models like the CISA example in Figure 1. The alignment focuses on providing capabilities that support early maturity targets and address longer-term goals over time.

Our goal is to help government agencies develop a tailored roadmap that uses your existing capabilities to be as effective as possible while also planning future enhancements. Every organization will require a unique zero trust approach, and Red Hat has the expertise to build robust zero trust architectures that evolve with your security needs and technological advancements.



Learn more

Every organization and department is likely to be at a different point in their zero trust journey. Red Hat's expertise, leading solutions, and access to an ecosystem of partners can help your agency effectively assess, plan, and adopt zero trust architecture within your organization.

- **Read more about how Red Hat works with government**
- **Discover Red Hat offerings for civilian agencies**
- **Learn more about zero trust**