TRUEFORT™

E-BOOK

WHAT YOU CAN LEARN FROM

The DOD's Take on Zero Trust

+1 201 766 2023 | sales@truefort.com

TRUEFORT.COM

In April of last year, the DOD published their Zero Trust Reference Architecture, which confirms their commitment to the Zero Trust approach as an important strategy for protecting the country's most sensitive information. The document defines the purpose, motivation, guidelines, and constraints for implementing a Zero Trust (ZT) security strategy and framework throughout the Department of Defense Information Network (DODIN). DOD mission owners, people responsible for managing and accomplishing the operational goals inside the agency, will consult the reference architecture (RA) as they work toward an interoperable ZT end state.

For other readers looking to make sense of the reference architecture, this review will introduce the basic principles and capabilities of ZT as presented in the document and highlight some essential ZT concepts.

What is Zero Trust?

A ZT strategy refers not to a pre-determined product suite, but a shift in security mindset. ZT assumes all person and non-person users, whether inside or outside an organization's network cannot be automatically trusted. They must be authenticated and authorized continually for all access requests. A ZT architecture applies to on-premises, cloud, and hybrid environments. Because ZT security assumes any actor can be a threat, it monitors all activity and limits user access to controlled segments of the network, ensuring that if malicious actors or malware get in, they won't be able to jump from one system to another.

Five Tenets of Zero Trust

The DOD reference architecture enumerates five major tenets of ZT, which define the ZT mindset. These tenets drive the selection and implementation of new and updated security capabilities that organizations will need as they transition toward a ZT framework.

- **Assume a hostile environment.** All users, devices, and networks/ environments are treated as untrusted.
- **Presume breach.** Operate with the assumption that an adversary has presence in your environment.
- **Never trust, always verify.** Deny access by default and apply the principle of least privilege to all entities.
- **Scrutinize explicitly.** Apply security policy consistently and use multiple attributes to determine conditional access to resources based on user action and confidence levels.
- **Apply unified analytics.** Log all transactions to support analytics for all data, applications, assets, and services.

Together, these tenets describe a security posture in which no entities are trusted automatically. ZT capabilities constantly authenticate, authorize, and validate network activity against security policies optimized for individual network segments, applications, workloads, and data. They carry out security assessments for the entire range of users, such as persons, internet-connected hardware, applications, and service accounts.

With ZT, organizations aim to follow the principle of least privilege by granting only as much access as any user is authorized for based on

- user roles, attributes, and credentials,
- device authentication and authorization,
- and security policies for specific resources, applications, and data.

Zero Trust Pillars and Capabilities

For most organizations, moving from a traditional location-centric security model to the more data-centric approach of ZT requires implementing new capabilities, revising and creating access policies, and reviewing workflow. As the DOD is planning a transition to ZT, the reference architecture helps define the capabilities required and provide some understanding of how they interact in a ZT framework. The reference architecture organizes these capabilities into seven categories or pillars.

Microsegmentation solutions that include automated dependency mapping provide complete results faster, cheaper, and more accurately than manual approaches. Look for solutions that help pinpoint intra-application and cross-application relationships, while offering real-time views at the account, network, and process levels in legacy and cloud-native environments. This level of detail and automation will provide a single source of truth for security engineers, incidence response, and DevSecOps teams to assess the application landscape and home in on security hotspots.

User

Capabilities in the User pillar authenticate users, including persons and non-person entities (NPEs), such as applications, email systems, management programs, databases, or device firmware. These capabilities also make an initial determination about whether users have authorization to access requested resources, applications, and data. User authentication and authorization will be used in conjunction with finer-grained authorization decisions which assess user credentials against security policies for resources, applications, data, and network segments to determine the final access decision.

Device

Capabilities in the Device pillar identify, authenticate, authorize, inventory, isolate, secure, remediate, and control any hardware asset that can connect to a network, including computers, cell phones, laptops, tablets, and internet-connected equipment (IoT). Capabilities in this pillar enforce pre-determined security policies for each device. For example, if a computer does not have the latest security patches installed, it may be denied access until it's updated.

Zero Trust Pillars and Capabilities

Network/Environment

Capabilities in the Network/Environment pillar logically and physically segment, isolate, and control the on- and off-premises network and environment with granular access restrictions. Users are limited to the data, applications, and resources they requested because security policies preclude moving from one part of the system to another without further scrutiny. Segmenting the network this way helps minimize damage should one part of the network become compromised.

Applications and Workload

Capabilities in the Applications and Workloads pillar monitor all systems, programs, and services that execute in on-premises and cloud environments across the complete application stack. This pillar includes the ability to discover applications and understand their relationships and dependencies. It also involves monitoring data to develop workload and application behavior baselines which help identify malicious activity and launch a prompt response. This pillar also includes the ability for DevSecOps teams to vet common libraries and source codes for more secure application development.

Data

The Data pillar includes capabilities to protect information on devices, in applications, and on networks. Data is categorized by its value to the organization, compliance regulations, and malicious actors. Data is tagged for security levels and access requirements; it's also tracked and inventoried.

Visibility and Analytics

The Visibility and Analytics pillar includes the capability to capture and monitor security processes across other pillars for broad observability, which improves anomaly detection, supports dynamic policy updates, and enables real-time access decisions. Behavioral analysis of the normal actions that occur in the network is especially important for developing a baseline of activity against which unexpected and possibly suspicious actions are easier to catch.

Automation and Orchestration

The Automation and Orchestration Pillar includes capabilities to automate policy-based actions across the enterprise for increased scale and decreased response time. Capabilities in this category also help security teams analyze breaches and identify vulnerabilities to prevent future incidents.

Deeper Dive Into Important ZT Capabilities

DOD's document is intended to help the agency transition to a ZT framework. As a result, it covers dozens of relevant concepts and capabilities. Some of these capabilities are particularly important for ZT success, especially with respect to the control and protection of applications and workloads.

Deny Access by Default with Microsegmentation

In a ZT framework, the principle of "Never trust, always verify" or denying access by default is most effective when an organization can apply granular security policies through microsegmentation. With microsegmentation, organizations define security policies customized for applications, workloads, machines, and other resources. Requests to any workload or application, for example, may be granted or denied based on the business attributes, compliance requirements, and data sensitivity of that resource.

Attaching security policies to applications and workloads also ensures that if the programs move from one environment to another, their policies move with them. For effective microsegmentation, organizations need the capability to discover all the applications in their network, map dependencies between them, and use behavioral data to help optimize the security policies.

Behavioral Analytics for Non-Person Entities

Behavioral analytics uses machine learning and artificial intelligence on the actions any person or NPE executes in the network. Analytics programs identify patterns of normal behavior, track trends of behavior shift, and with continuous monitoring, capture anomalies that might indicate suspicious actions. This information is used to build a positive security model and inform security policies.

It's crucial that an effective ZT framework run behavioral analytics on NPEs as well as persons. NPEs may need access to sensitive data to do their work. Or they may connect with other parts of the network, making them an attractive way in for malicious actors. If organizations have visibility into NPE behavior and a baseline of normal behavior, it's much easier to spot bad actors and respond appropriately.

Application Authorization

Traditional security frameworks have little visibility into the application behavior, which makes it harder to detect suspicious actions. But for ZT architectures, organizations should add application-level security policies both for restricting access to applications and for detecting breaches in the application layer. Based on application mapping and behavior baselines, organizations can

- establish an authorization decision point prior to allowing any user access to an application,
- detect application-level activity that falls outside normal behavior,
- and automate responses to questionable operations.

Learn More About the DOD Zero Trust Reference Architecture

For additional details about the DOD recommendations for enabling Zero Trust security or for details on how these recommendations relate to other federal technical architecture and design documents, consult the full report here.

About TrueFort

TrueFort provides real-time visibility, application intelligence, and immediate response to global enterprises that have seen traditional security approaches fail in today's threat environment. We help customers quickly and seamlessly implement essential capabilities of Zero Trust, such as cloud workload protection, behavior analytics, and file integrity monitoring for the cloud.

- **Cloud Workload Protection and Microsegmentation**
  With TrueFort, companies capitalize on existing infrastructure for day-one microsegmentation. TrueFort Cloud coordinates with deployed EDR agents to secure on-premises, hybrid, and cloud environments. The platform provides environment-wide observability, and behavior analytics speed the development of optimal security policies for each workload.
- **Service Account Behavior Analytics**
  Service accounts are often the forgotten vulnerabilities that may give attackers unrestricted access to move laterally across environments. But for companies moving toward a ZT end state, service accounts are hard to find and manage. TrueFort solutions automatically locate and track service account behavior, map their dependencies and interactions, automate least privilege access, and trigger real-time notifications of unexpected service account behavior.
- **File Integrity Monitoring**
  Most FIM applications don't provide the details needed to track cloud workloads and identify the specific changes taking place in a file. TrueFort's FIM solution monitors fine-grained details about file updates, such as versions, modification dates, and content updates, and compares changes against a model of expected behavior to identify suspicious deviations. If a problem is detected, the system automates responses in accordance with business, compliance, and security priorities.

To learn how TrueFort can help you implement Zero Trust in your organization, contact us HERE.

TRUEFORT™

3 West 18th Street
Weehawken, NJ, 07086
United States of America

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM