TRUEFORT™

SOLUTION BRIEF

Mapping TrueFort to the DoD Pillars of Zero Trust

The use of legacy cybersecurity technology stacks such as Antivirus, Network-based Firewalls, Host- and Network-Intrusion Prevention, Vulnerability Scanners, Patch Management, and Malware Sandboxes is a "rear-view-mirror" approach.

The ever-growing list of known indicators of compromise / attack and identified vulnerabilities that are added to the catalog of cyber threats, not counting those that are unknown, or Zero-Day threats, increases every day. Agencies and teams struggle with preventing or patching every known cyber threat. Employing a reactive, defensive mindset challenges achieving mission assurance. What is required is moving toward a proactive, predictive model that detects deviations against the known good state of a heterogeneous application workload environment.

When referencing the pillars of Zero Trust, as described by the DoD Zero Trust Model document on page 20[1], **there are key areas TrueFort provides deep knowledge:**

1. the ability to secure application and workload.
2. the ability to detect and respond to supply chain attacks.

Secure applications and workloads:

TrueFort assists with the ability to go beyond network-based controls to monitor and control process, identity, application, and the operating system in real-time by generating a behavioral baseline of application dependencies in order to deploy and maintain autonomously produced micro-segmentation policies in dynamic, and often hybrid, compute environments.

Detect and respond to supply chain attacks:

TrueFort truly understands all behaviors in the application environment including third-party software. The TrueFort Platform addresses supply chain attacks like SolarWinds/ Sunburst, Okta, and Zero-Day vulnerabilities such as Log4Shell, by combining behavior baselining, real-time anomaly detection and response across all applications and workloads.

TrueFort maps to various controls contained in every pillar in the following ways:

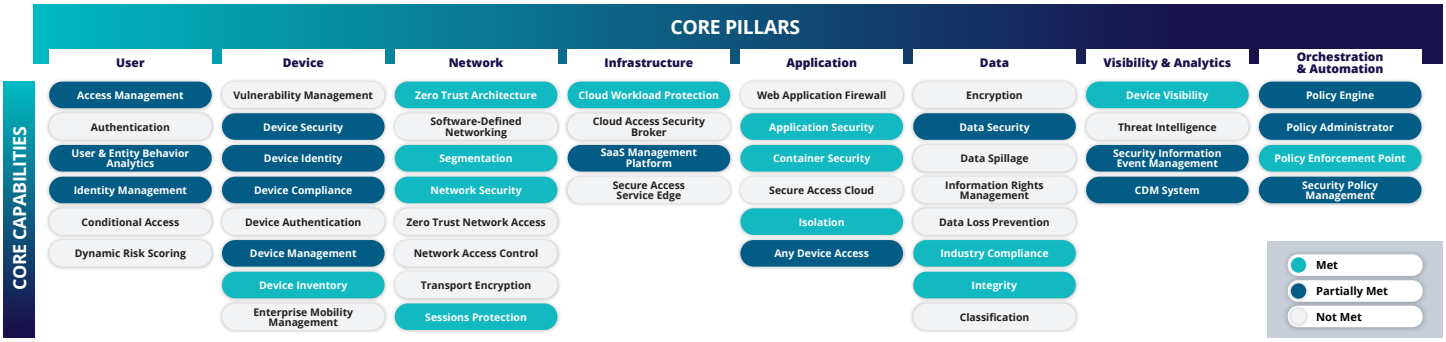


FIGURE: TrueFort's Zero Trust Capability Model

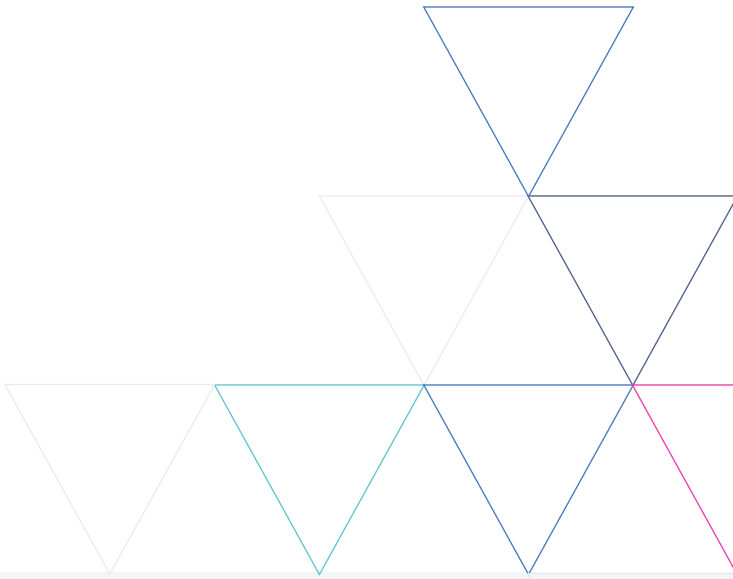
1 - Department of Defense (DOD) Zero Trust Reference Architecture

The TrueFort Platform provides this depth of broad support by applying Zero Trust to applications and workloads. Helping agencies and teams achieve success in their Zero Trust journey is accomplished by TrueFort's unparalleled visibility, even where no agent is deployed. Simply stated, agencies and teams can not manage what they do not see and understand. The journey toward implementing a Zero Trust framework starts with the ability to visualize your critical applications and environments.

Agencies and teams struggle to fully understand the dependencies within their application landscape. Change Management Databases are out of date the minute they are created. Infrastructure operators need to continuously monitor the changing behaviors of applications, both pre and post deployment. They must be able to classify, prioritize and visualize their applications, the dependencies between them and to automate the creation of the required operational controls. Added to that challenge are the differing security capabilities and requirements that come with legacy vs. modern OS's, bare metal, virtual, containerized, hybrid and cloud workloads. It becomes critical that application dependency maps are infrastructure-agnostic and are updated automatically and dynamically. Clear visibility and dependency maps form the foundation used to categorize and classify the environment and are key to building policy and enforceable segmenting controls based on least user privilege to prevent lateral movement.

Whether access is granted by accident or controlled unclassified information (CUI) is maliciously accessed, visibility is the key to security. Without the ability to see what's happening on all workloads and knowing when behavior deviates from a known good state, malicious actors can evade existing security controls, resulting in a costly and damaging breach or loss of mission assurance.

The TrueFort Platform delivers continuous real-time telemetry across network, process, identity, and software behavior which analyzes within milliseconds. The platform generates comprehensive real-time alerts and workflow-driven responses to ensure that unknown or deviant behavior is immediately identified and depending on policy configuration, it is either automatically or manually stopped. TrueFort reduces business risk for security-focused customers striving for zero trust application environments. Our innovative and uniquely application-centric micro- and nano-segmentation platform delivers comprehensive real-time cloud-to-the-ground insight, protection and automated response with patented machine intelligence using either our agent or bring-your-own agent, such as CrowdStrike, eliminating the need for additional impact to the endpoint.



ABOUT TRUEFORT

TrueFort is an advanced approach to protecting data center and cloud workloads that makes zero-trust architectures possible. Our platform uses continuous monitoring to deliver real-time detection and response as soon as noisy workload behavior strays from known, understood activity. By absorbing telemetry from multiple agents, we decipher all intra-application communications and trigger suspicious activity alerts. The TrueFort Platform is the only solution instilling the confidence to protect workloads across all production environments. By reducing the impact of security incidents, we increase your overall business resilience, shrink your exploitable attack surface, and enable you to take immediate action against live attacks. We bring the single truth security and application owners need to effectively protect workloads of all forms.

For more information, visit truefort.com and follow us on Twitter and LinkedIn.

TRUEFORT™

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

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM