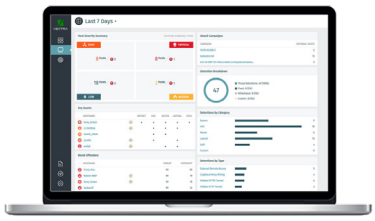
Supporting the Federal Government's Zero Trust Strategy with Data Science and AI



Whether you are on the Zero Trust Architecture (ZTA) bandwagon or feel we've been driving to this for years under a different name, the November 2022 release of the Department of Defense (DoD) Zero Trust Strategy is a welcome breath of unified direction. Every branch, mission partner, civilian agency and Defense Industrial Base (DIB) has their own interpretation of ZTA and its strategy. It is hoped that the well-mapped strategy provides industry and the government alike with a mutual plan to work towards — a common goal that ultimately allows the stakeholders from government and industry to focus on a well-established plan and timeline. Certain capabilities and subsequent industry engagements warrant more rapid acceleration vs. those later in the process — taking a phased strategy with dependencies to engage various tools and integrations is critical for success.

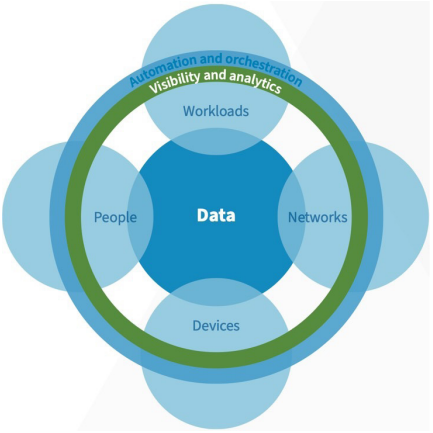
Align with DoD Zero Trust Strategy Pillars:

- Visibility
- Analytics
- Automation
- Orchestration

Aligning Zero Trust Deployments with DoD Strategy

Two significant themes within Zero Trust are to assume a hostile environment and to presume breach. Yet, at the same time, users need to access data wherever they work. ZTA allows this access by ensuring users and non-person entities (NPEs) are authorized and authenticated from wherever they reside. This model implements security by dynamic policy, observable user state and continuous monitoring. Other benefits of ZTA include increased network visibility, reduced attack surfaces by appropriate network controls, damage containment from early detection capabilities, and rapid recovery from advanced persistent threats (DoD) within the edge, data center or the cloud.

As agencies begin and continue their ZTA deployments, the industry can assist by investing its efforts in products and services that align with the department's goals. To that end, and within this analysis of the DoD ZTA Strategy and Architecture documents, Vectra has found close alignment with select pillars. This document will focus on the Visibility, Analytics, Automation, and Orchestration pillars. These pillars arc across the core pillars of People, Workloads, Networks, and Data.



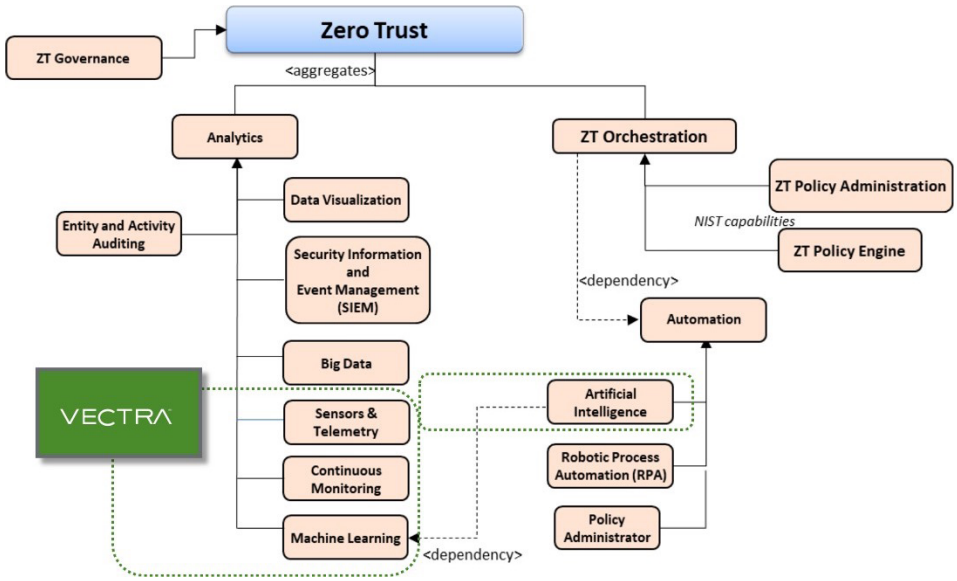
Visibility and Analytics

Analytics is all about context. Context provides an understanding and visibility into anomalous behavior. This allows the environment to make dynamic changes to security policies and real-time access decisions (DISA, NSA). Sensor data and telemetry assist in building an image of what is happing in the environment so teams can investigate and respond to threats. Coupling all these elements with purpose-built AI and ML enhances accuracy and reduces operator error during threat investigation. Rational outcomes from the contextual AI engine can be forwarded to SOAR tools for automated remediation. More than simply looking for anomalous behavior is required to provide the efficacy of detections to creation automation. The visibility and analytics components must allow the operators to trust the outcomes based on the contextual learnings of the environment.

Vectra continuously monitors the behaviors of accounts, hosts and services while applying supervised and unsupervised AI models to score these behaviors for threat, certainty and risk prioritization. As a result, Vectra delivers a continuous real-time assessment of privilege. This empowers security teams with the right information to anticipate what assets will be targeted by attackers and to rapidly act against malicious use of privilege across the edge, data center or the cloud. By doing so ensures that the visibility is continuously evolving to provide the right analytics vs. compliance or a snapshot in time, which is paramount to ensuring trust in the system by the operators and the tools leveraging the actionable intelligence.

Automation and Orchestration

The Automation and Orchestration pillar considers the benefits of automating manual security processes by replacing them with policy-based actions. Therefore, it is essential to leverage tools that implement standardized APIs to ingest data from and send data to Policy Enforcement Points (PEPs) and Policy Decision Points (PDPs). Vectra's AI correlates threat behaviors to a host or account and prioritizes them into one of four severity rankings: Critical, High, Medium and Low. This ranking is based on Vectra's scoring model's understanding of how aligned the collective attacker behaviors are to a real escalating attack. These successive attacker behaviors create detections indicative of an adversary, which allow an analyst to review and respond.



AI-generated detections can be automatically forwarded to a SOAR system for an immediate response and integrated into SDWAN for disconnected dynamic routing and endpoint tools for host and account lockdown and remediation. For example, suppose a detection meets a threat and/or risk threshold. In that case, an event is generated in a SOAR, which instructs an EDR to lock a host or a ticketing system to start a workflow, which generates the ticketing system with the related PCAP, forensics and incident response data. Additionally, Vectra has a robust REST API where tools can harvest useful information to view and manage hosts, accounts, detections, notes and more.

Plan Your Journey Logically

Wherever your organization is along the Zero Trust journey, understanding how to provide the visibility, analytics, orchestration and automation up front is a key requirement. Vectra has a proven history within the IC, DoD and CIV sectors along with the DIB to help the process move smoothly. Understanding the full view of users, hosts and services into a singular 'host container' is necessary for correct visibility. Being able to do so across disconnected enterprise networks, high-side enclaves, and Gov and TS cloud environments and SaaS identity workloads can accelerate the journey and alleviate manual process and lengthy evaluations of environments.

DISA, NSA. "Zero Trust Reference Architecture version 2.0." July 2022. https://dodcio.defense.gov. 9 December 2022.
DoD. "DoD Zero Trust Strategy." 7 November 2022. https://dodcio.defense.gov. 9 December 2022.

About Vectra

Vectra® is the leader in Security AI-driven cyber threat detection and response for hybrid cloud. Vectra's patented Attack Signal Intelligence™ detects and prioritizes threats across public cloud, SaaS, identity, and networks in a single platform. Vectra's Attack Signal Intelligence goes beyond simple anomaly detection to analyze and understand attacker behavior. The resulting high-fidelity signal and deep context enables security operations teams to prioritize, investigate and respond to cyber-attacks in progress sooner and faster. Organizations worldwide rely on the Vectra platform and MDR services to stay ahead of modern cyber-attacks. Visit www.vectra.ai.

Email: federal@vectra.ai | Vectra.ai/federal