ZERO TRUST ARCHITECTURE (ZTA) IMPLEMENTATION AND TRANSFORMATION
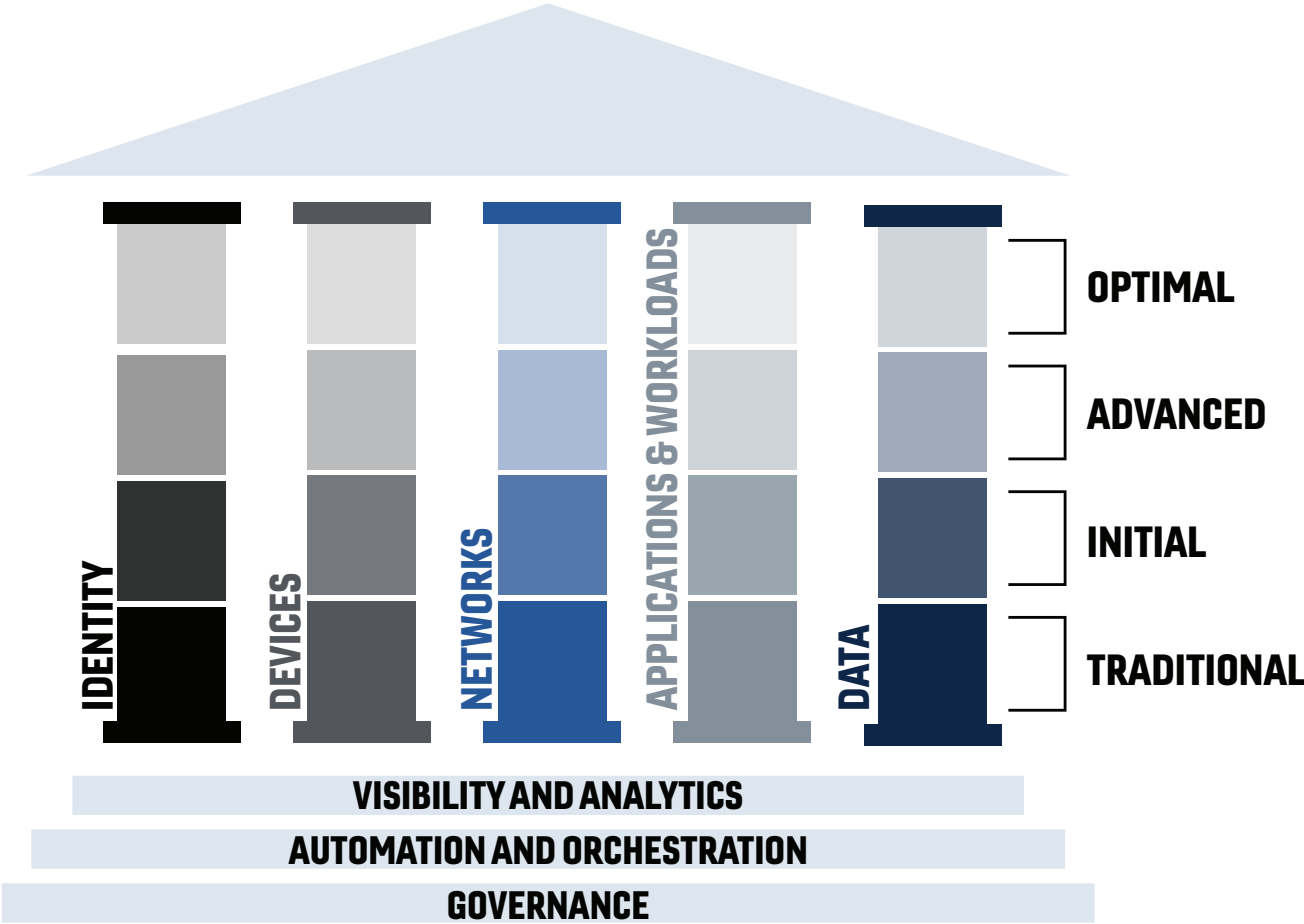
INTEGRATING SECURE ZT SOLUTIONS WHILE EHANCING MISSION

The digital transformation, characterized by cloud adoption, ubiquitous connectivity, and the proliferation of mobile devices, has fundamentally altered the security landscape. Traditional perimeter-based security models, reliant on the notion of a trusted internal network, are increasingly ineffective against sophisticated threats that exploit the inherent trust within these boundaries.
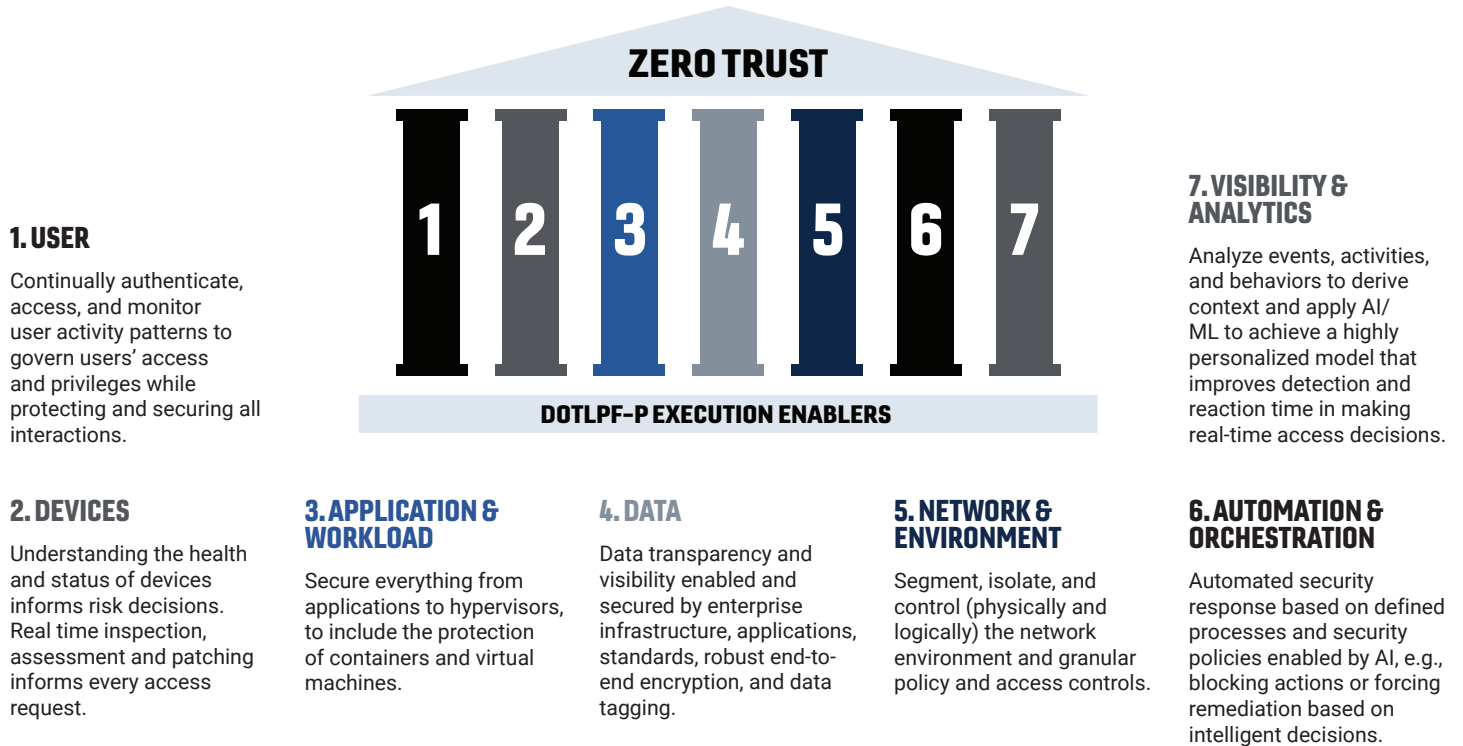
This whitepaper presents a practical, phased approach to zero trust (ZT) implementation aligned with the Department of Defense (DoD) and the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency's (CISA) Zero Trust maturity models, empowering organizations to navigate this evolving threat landscape and build a resilient and secure cybersecurity architecture.

Evolving Threat Landscape:

- The demise of the perimeter: Employees, partners, and customers access resources from diverse locations and devices, blurring the lines between internal and external networks and making the traditional network perimeter "castle-and-moat" security doctrine obsolete

- Sophisticated threat actors: Cybercriminals are increasingly sophisticated, employing advanced techniques—ransomware, supply chain attacks, and social engineering—to bypass traditional security controls

- Data-centric security: Data is the primary target of cyberattacks. Protecting sensitive data, at-rest and in-transit, is paramount

Figure 1A: CISA Zero Trust Maturity Model

ZERO TRUST

DOTLPF–P EXECUTION ENABLERS

1. USER

Continually authenticate, access, and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions.

2. DEVICES

Understanding the health and status of devices informs risk decisions. Real time inspection, assessment and patching informs every access request.

3. APPLICATION & WORKLOAD

Secure everything from applications to hypervisors, to include the protection of containers and virtual machines.

4. DATA

Data transparency and visibility enabled and secured by enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging.

5. NETWORK & ENVIRONMENT

Segment, isolate, and control (physically and logically) the network environment and granular policy and access controls.

6. AUTOMATION & ORCHESTRATION

Automated security response based on defined processes and security policies enabled by AI, e.g., blocking actions or forcing remediation based on intelligent decisions.

7. VISIBILITY & ANALYTICS

Analyze events, activities, and behaviors to derive context and apply AI/ML to achieve a highly personalized model that improves detection and reaction time in making real-time access decisions.

Figure 1B: DoD Zero Trust Reference Architecture

ASSESS
- Identify protect surface and data locations
- Perform assessment against maturity model
- Conduct gap analysis from as-is to to-be states
- Identity current in-flight projects

OPERATE
- Transition to operations
- Update baseline configuration and SOC monitoring capabilities
- Create SOPs/playbooks
- Update policy and guidance documents

ZERO TRUST

ASSESS

PLAN

BUILD

OPERATE

PLAN
- Prioritize high value data and systems
- Create roadmap to close gaps
- Update cybersecurity guidance, security plans, and enterprise architecture
- Update system architectures and designs

BUILD
- Modernize infrastructure and systems, partner with zero trust technology providers
- Deploy and test solutions/proofs of concept
- Document for change boards and ATOs
- Integrate into enterprise environment

Figure 2: Peraton's ZT Integration Approach

ZERO TRUST: DEFENSE-IN-DEPTH TURBOCHARGED

Zero trust is not a product or technology but a strategic security philosophy that assumes no implicit trust, regardless of location or network.

Arranged in pillars and cross cutting capabilities in Figures 1A and 1B, Peraton's approach focuses on enhancing specific capabilities and depth of cyber defenses across the enterprise.

Peraton uses a four-step approach to apply and mature ZT capabilities within your organization. We can provide a baseline assessment and compare your ZT journey progress against targeted ZT goals (DoD Target and Advanced or CISA's Optimal Levels). If you have an established baseline, we can work with key partners/preferred vendors to plan, build, and/or operate solutions to mature specific ZT capabilities as shown in Figure 3.

PERATON'S ZT VALUE PROPOSITION

- **Partnerships with preferred ZT security solutions vendors:** As a systems integrator with experience deploying preferred ZT security solutions in complex and challenging environments, Peraton leverages and empowers partnerships with Zscaler, ServiceNow, Microsoft, Amazon Web Services, Splunk, Crowdstrike, and Okta

- **Maximize exisiting investments:** Peraton knows how to help customers maximize their existing product and licensing investments

- **Established playbooks:** Our established playbooks for deployment scenarios across a multitude of technical reference architectures enable rapid value delivery and shorter mean time to deploy (MTTD) cycles

- **Proven performance:** We have a proven track record of achieving and exceeding target ZT maturity levels in DoD and civilian government agencies
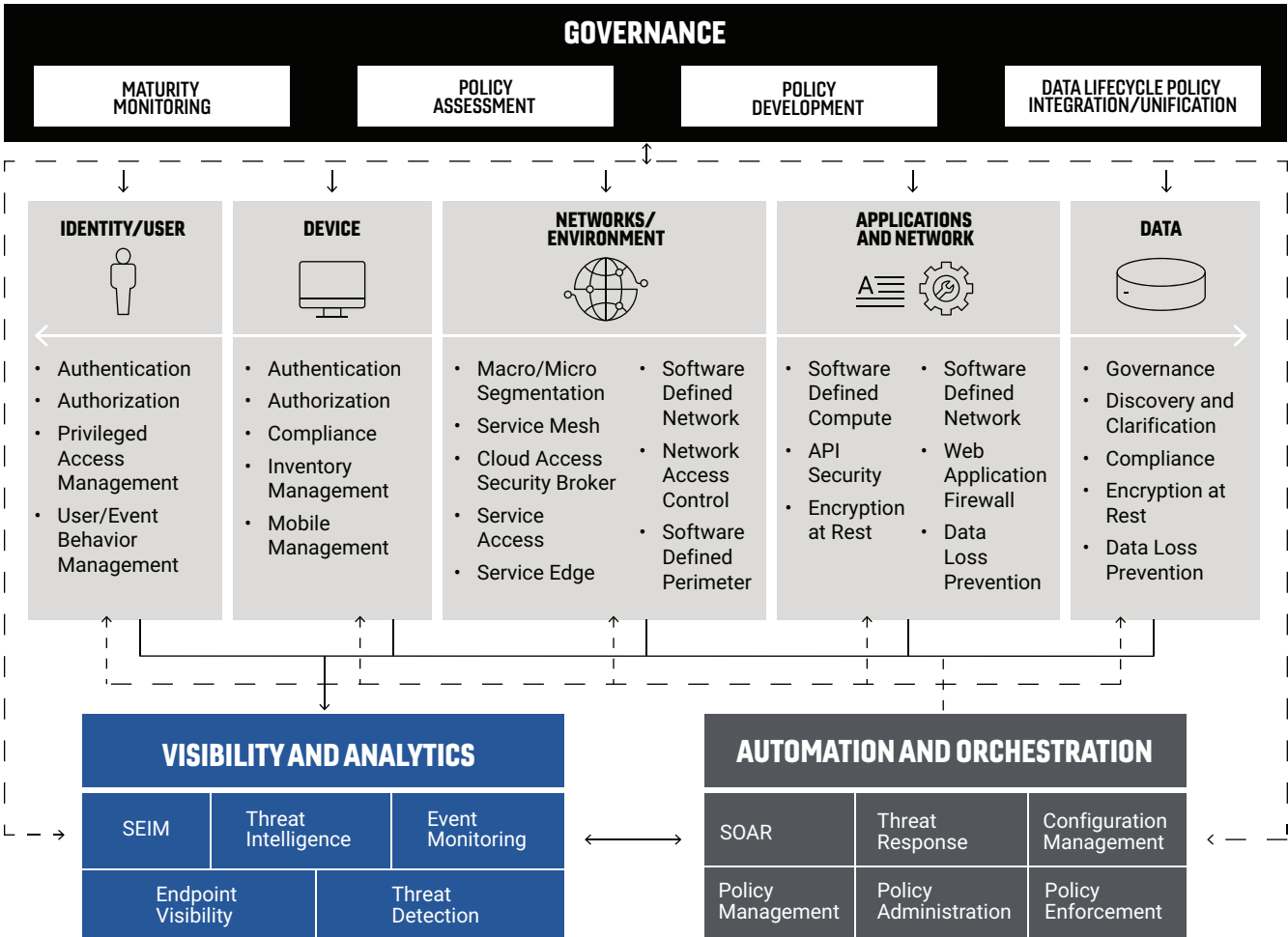
GOVERNANCE

MATURITY MONITORING	POLICY ASSESSMENT	POLICY DEVELOPMENT	DATA LIFECYCLE POLICY INTEGRATION/UNIFICATION

IDENTITY/USER	DEVICE	NETWORKS/ENVIRONMENT		APPLICATIONS AND NETWORK		DATA
• Authentication • Authorization • Privileged Access Management • User/Event Behavior Management	• Authentication • Authorization • Compliance • Inventory Management • Mobile Management	• Macro/Micro Segmentation • Service Mesh • Cloud Access Security Broker • Service Access • Service Edge	• Software Defined Network • Network Access Control • Software Defined Perimeter	• Software Defined Compute • API Security • Encryption at Rest	• Software Defined Network • Web Application Firewall • Data Loss Prevention	• Governance • Discovery and Clarification • Compliance • Encryption at Rest • Data Loss Prevention

VISIBILITY AND ANALYTICS

SEIM	Threat Intelligence	Event Monitoring
Endpoint Visibility		Threat Detection

AUTOMATION AND ORCHESTRATION

SOAR	Threat Response	Configuration Management
Policy Management	Policy Administration	Policy Enforcement

Figure 3

CASE STUDY 1: DOD ZT ASSESSMENT AND ROADMAP— PERATON'S ASSESS AND PLAN

Peraton conducted an extensive ZT assessment across multiple IT and cyber programs for a DoD customer that involved reviewing all current technology investments and existing security architecture implementations to establish a baseline against the DoD Zero Trust Maturity Model.

Our mandate was to provide a modernization and innovation plan that recommends new, emerging, and disruptive technology and processes, schedule, and cost to improve the operational effectiveness and efficiency of the agency's C5ISC infrastructure. This resulted in the delivery of a detailed roadmap to achieve the target FY27 goals and beyond.
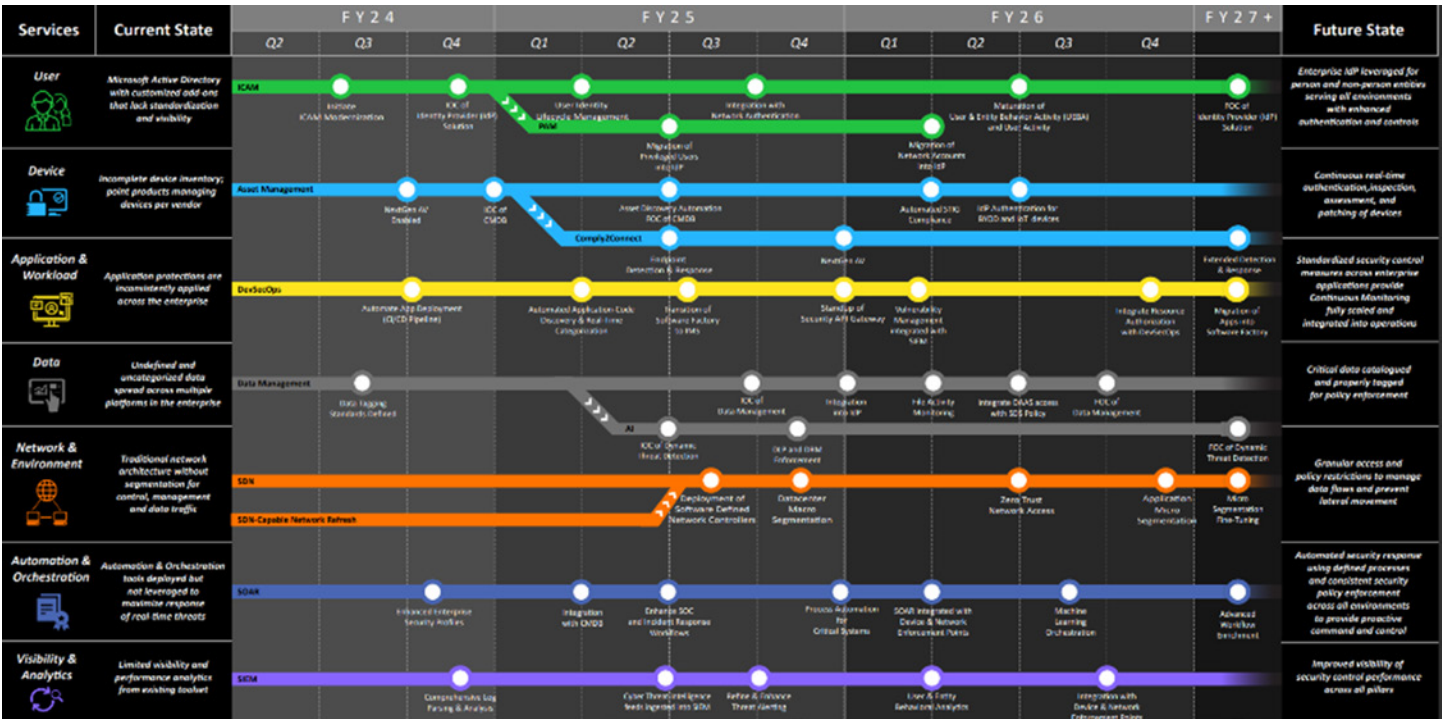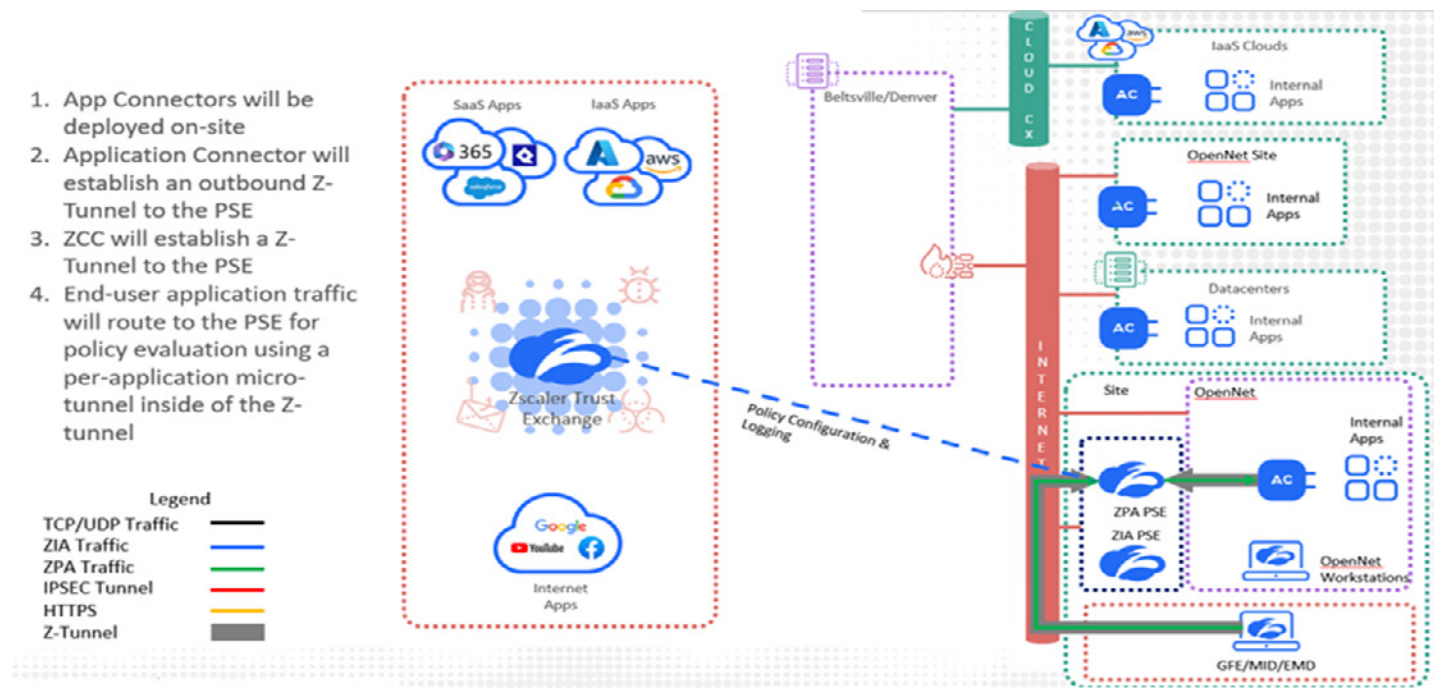

Figure 4

CASE STUDY 2: FEDERAL CIVILIAN ZT IMPLEMENTATION (PERATON'S BUILD, OPERATE)

Peraton worked with a federal civilian agency to build and operate Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) ZT solutions to establish a Zero Trust Exchange (ZTE) using a cloud-based security platform. From a ZT perspective, this helped mature pillar capabilities against the CISA Zero Trust Maturity Model 2.0, specifically Network, Device, and Data pillars.

From a mission perspective, we were able to reduce the bandwidth utilization for internet and local site traffic—greatly improving the user experience—by offloading that traffic using Zscaler's client connector. With this solution, internet traffic does not have to backhaul through the corporate WAN that was traversing overseas back to CONUS before being sent back, creating high latency and delayed webpage load time.

1. App Connectors will be deployed on-site
2. Application Connector will establish an outbound Z-Tunnel to the PSE
3. ZCC will establish a Z-Tunnel to the PSE
4. End-user application traffic will route to the PSE for policy evaluation using a per-application micro-tunnel inside of the Z-tunnel

Legend

TCP/UDP Traffic	
ZIA Traffic	
ZPA Traffic	
IPSEC Tunnel	
HTTPS	
Z-Tunnel	

Figure 5
Source: Zscaler

ABOUT PERATON

Peraton is a next-generation national security company that drives missions of consequence spanning the globe and extending to the farthest reaches of the galaxy. As one of the world's leading mission capability integrators and transformative enterprise IT providers, we deliver trusted, highly differentiated solutions and technologies to protect our nation and allies from threats across the digital and physical domains. Peraton supports every branch of the U.S. Armed Forces, and we serve as a valued partner to essential government agencies that sustain our way of life. Every day, our employees do the can't be done by solving the most daunting challenges facing our customers. Visit peraton.com to learn how we're safeguarding your peace of mind.