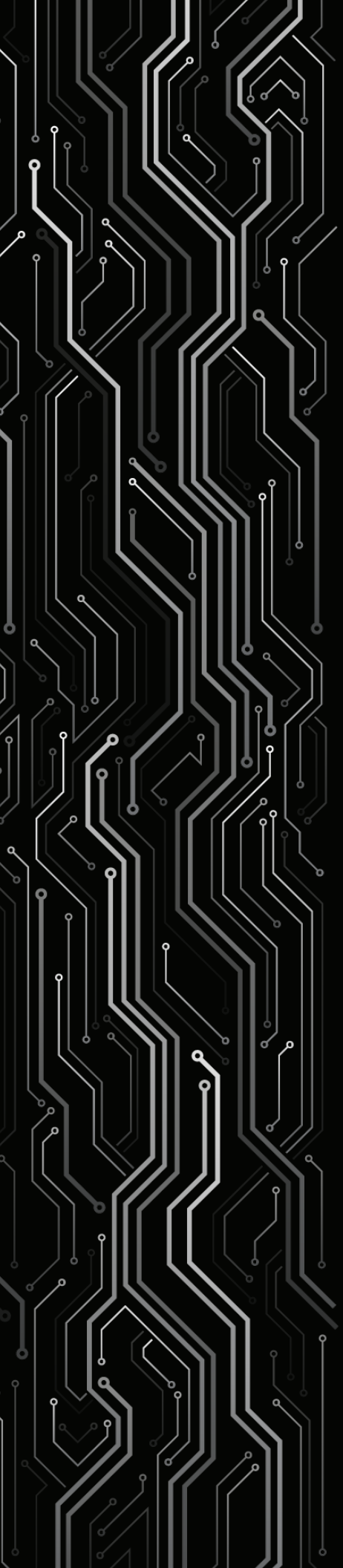
Gregg Garrett, CISSP, CISM, PMP
Vice President, Cybersecurity

Peraton



ZERO TRUST: CYBERSECURITY CONCEPTS TO SOLUTIONS

THE CYBER EO: ZERO TRUST MANDATE

The Executive Order (EO) on Improving the Nation's Cybersecurity (May 12, 2021) marks a renewed commitment for the U.S. federal government on cybersecurity modernization. According to the Cybersecurity Infrastructure Security Agency (CISA) Zero Trust Maturity Model (June 2021) the new cyber EO embraces zero trust (ZT) as a desired cybersecurity concept and tasks all U.S. federal government agencies with modernizing their current programs, services, and capabilities to be fully functional with cloud-computing environments with a zero trust architecture (ZTA). Specifically, the cyber EO requires all Federal Civilian Executive Branch (FCEB) agencies to develop migration plans for ZTAs. A typical ZTA migration plan will assess an agency's current cybersecurity state of policies, plans, architecture, systems, and software and then plan for a fully implemented ZTA as a future desired state.

UNDERSTANDING ZERO TRUST

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 on zero trust provides the following definitions of ZT and ZTA:

- **Zero Trust (ZT)** provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.
- **Zero Trust Architecture (ZTA)** is an enterprise's cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies.

The publication states that "the goal is to prevent unauthorized access to data and services coupled with making the access control enforcement as granular as possible." Said simply, ZT presents a paradigm shift in thinking for information security professionals, from a location-centric model to a more dynamic data-centric model allowing for more detailed levels of information security controls between users, devices, network systems, data, and assets that change over time.

KEY CONCEPTS OF A ZERO TRUST ARCHITECTURE

According to Forrester Research there are five key concepts to make a ZTA actionable:

1. All resources must be accessed in a secure manner
2. Access control is provided on a need-to-know basis
3. Do not trust people and verify what they are doing
4. Inspect all log traffic coming in on the network for malicious activity
5. Design networks from the inside out

THE SEVEN DESIGN TENETS OF ZTA

NIST SP-800-207 states that zero trust should strictly adhere to a set of seven design tenets that regulate user access and data management across all enterprises. These include:

1. **Rigorously enforce authentication and authorization:** all resources require mandatory authentication, often paired with technologies such as multifactor authentication (MFA), before granting access
2. **Maintain data integrity:** enterprises measure and monitor the security and integrity of all owned and associated assets, assess their cyber vulnerabilities, patch levels, and other potential cybersecurity threats
3. **Gather data for improved security:** enterprises should collect current information from multiple sources, such as network infrastructure and communication, to regulate and improve security standards
4. **Consider every data source and computing device as a resource:** enterprises should consider any device with access to an enterprise-level network as a resource
5. **Keep all communication secured regardless of network location:** physical network locations alone should never imply trust. People connecting via enterprise and non-enterprise networks must undergo the same security requirements for resource access
6. **Grant resource access on a per-session basis:** enterprises should enforce a least privilege policy—a user should only be granted the minimum privileges required to complete a task. Every access request requires evaluation and, when granted, does not immediately provide access to other resources
7. **Moderate access with a dynamic policy:** enterprises need to protect resources with a transparent policy that continuously defines resources, accounts, and the type of privileges linked to each account

HOW A GOVERNMENT AGENCY SHOULD IMPLEMENT A ZTA

Based on our experience in successfully implementing ZTAs for numerous U.S. public sector customers, we recommend an inside-out approach using the following key steps, as outlined in the GSA Zero Trust Buyer's Guide (June 2021), to implement a ZTA:

1. **Identify a protect surface:** the protect surface contains the agency's most valuable data, assets, applications, and services (DAAS), which represents the most critical elements of an agency's operation
2. **Focus on analyzing both the ingress and egress network flows in relationship to the protect surface:** understanding who the users are, which software applications they are using, and how they are connecting is the only way to determine and enforce policy that ensures secure access to the data. This independencies analysis between the DAAS, infrastructure, services, and users will reveal precisely where the agency must put controls in place and this the defines multiple micro-perimeters for each DAAS
3. **Design the micro-perimeters:** the micro-perimeters must be defined as close to the protect surface as possible and will logically move with the protect surface wherever it goes. The agency will effectively create micro-perimeters by deploying a segmentation gateway(s) to ensure only known, allowed traffic have access to the protect surface
4. **Select a data segmentation gateway as a network component:** the data segmentation gateway serves as a policy enforcement point (PEP). Zero trust policy is based on who, what, when, where, why, and how. This ZT policy determines who can transit a micro-perimeter at any point in time, preventing unauthorized user access and the exfiltration of sensitive data
5. **Continuously monitor and maintain in real-time the protect surface:** the agency must actively and continuously monitor 24x7x365 the entire protect surface with integrated, dynamic threat intelligence and rapid incident response capabilities to ensure appropriate identity, credential, and access management for an evolving threat environment

PERATON ZERO TRUST SOLUTIONS

ZT Case Study 1: Federal Defense Agency

Background and Cybersecurity Challenges:

Previously, this U.S. federal government defense agency's networks were protected by large external firewalls with anti-virus software, no internal data segmentation, no micro-perimeters, and simple password identification, and it was only passively monitored. Cyber incident data was captured electronically in data logs and batch processed for data analysis, using a basic intrusion detection system (IDS) at key monitoring points enterprisewide. Later, the information security analyst would study the cyber data logs and related data analysis and determine if a cyber incident ticket(s) needed to be released. Unfortunately, this passive/reactive method of monitoring does not provide timely cyberattack remediation, does not block or mitigate cyberattacks, and does not notify security analysts when an active cyberattack or abnormal user behavior occurs.

Peraton Recommended ZT Solution

Peraton recommended a customized ZT solution for the U.S. federal government defense agency, which allows them to move away from a reactive/passive method of cybersecurity towards a proactive ZTA approach using a combination of systems and tools which deploy micro-perimeters to monitor internal network traffic and Palo Alto Network's XDR extended endpoint detection and response system, fully integrated with advanced data analytics using security orchestration and automated response (SOAR) technology. This ZT project has been fully authorized and approved, and is being successfully implemented.

Results

This ZT project has successfully integrated next-generation firewalls to monitor the traffic inside the government agency's network which actively supports over 1,000 users. The Peraton-designed ZT solution provides advanced, proactive security from device to device, adds a micro-perimeter (site firewall) for each site, provides access control and proactively manages information flow, and integrates SOAR technology to provide automated incident response playbooks for rapid cyberattack remediation. See Appendix 1: Zero Trust Architecture.

ZT Case Study 2: Federal Civilian Agency

Background and Cybersecurity Challenges:

A large FCEB agency was searching for a way to provide a new approach to the Trusted Internet Connection (TIC) 2.0 program implementing a ZTA. Peraton initiated an Independent Research and Development (IRAD) project in 2020 to integrate a ZTA into the TIC 2.0 program.

Peraton Recommended ZT Solution

Peraton, working with its technology partner Zscaler, designed a ZTA solution using a secure access service edge (SASE) technology approach (see Figure 2), which securely connects users to internally and externally managed software applications including Ssoftware as a service (SaaS) and internet destinations, regardless of device, location, or network. This cloud-based architecture is built on a FedRAMP certified cloud infrastructure.

Results

This new ZT solution has been tested via a proof of concept and is now able to inspect all information system traffic, including encrypted traffic, and enforce security policy for identity, access, and control in a dynamic manner with continuous monitoring and analysis. Peraton has incorporated this new ZT solution into eight different government agency proposals. This ZT-based solution can modernize and improve cybersecurity for a government agency while supporting cloud adoption and a remote/mobile workforce.
See Appendix 2: Zscaler Federal Platform.

ZT Case Study 3: County Government

Background and Cybersecurity Challenges:

A large county government wanted support to guide them through the process of planning and implementing a secured multifactor authentication (MFA) capability for the expanse of their heterogeneous enterprise and support infrastructure for over 18,000 employees. The county government provides a wide-range of citizen services including medical, financial, administrative, motor vehicles to several million citizens. The intention of the County Information Technology (IT) leadership was to grant limited user access to specific software applications on a need to use basis, providing software-based data segmentation and true identity access and control, which are key design tenets of ZT.

Peraton Recommended ZT Solution

The Peraton-designed ZT solution provided an identity profile-driven access management of all software applications and associated environments for three distinct groups—county staff, county third-party, and support staff/vendors. As a result of the implementation of this initial Peraton-ZT solution, the county's software applications were secured via a robust MFA, no matter where—behind a firewall or in a public cloud—the applications are running.

Results

Peraton developed the initial ZT solution and successfully implemented it for the county government in 2018. In 2020, after the initial impact of COVID-19, a unified effort for defining an enhanced security roadmap was established with the county and principals. Peraton recommended and led the systems integration of an enhanced ZT solution for the county government leveraging an Akamai Enterprise Architecture Approach to implement a ZT model based on the principle of maintaining strict access controls that no longer gave default access—even to those already inside the network perimeter. The Peraton ZT solution provided for enterprise-wide Akamai identity management and access for county business applications and their Office 365 tenants. **See Appendix 3: Known/Unknown Users**.

SUMMARY

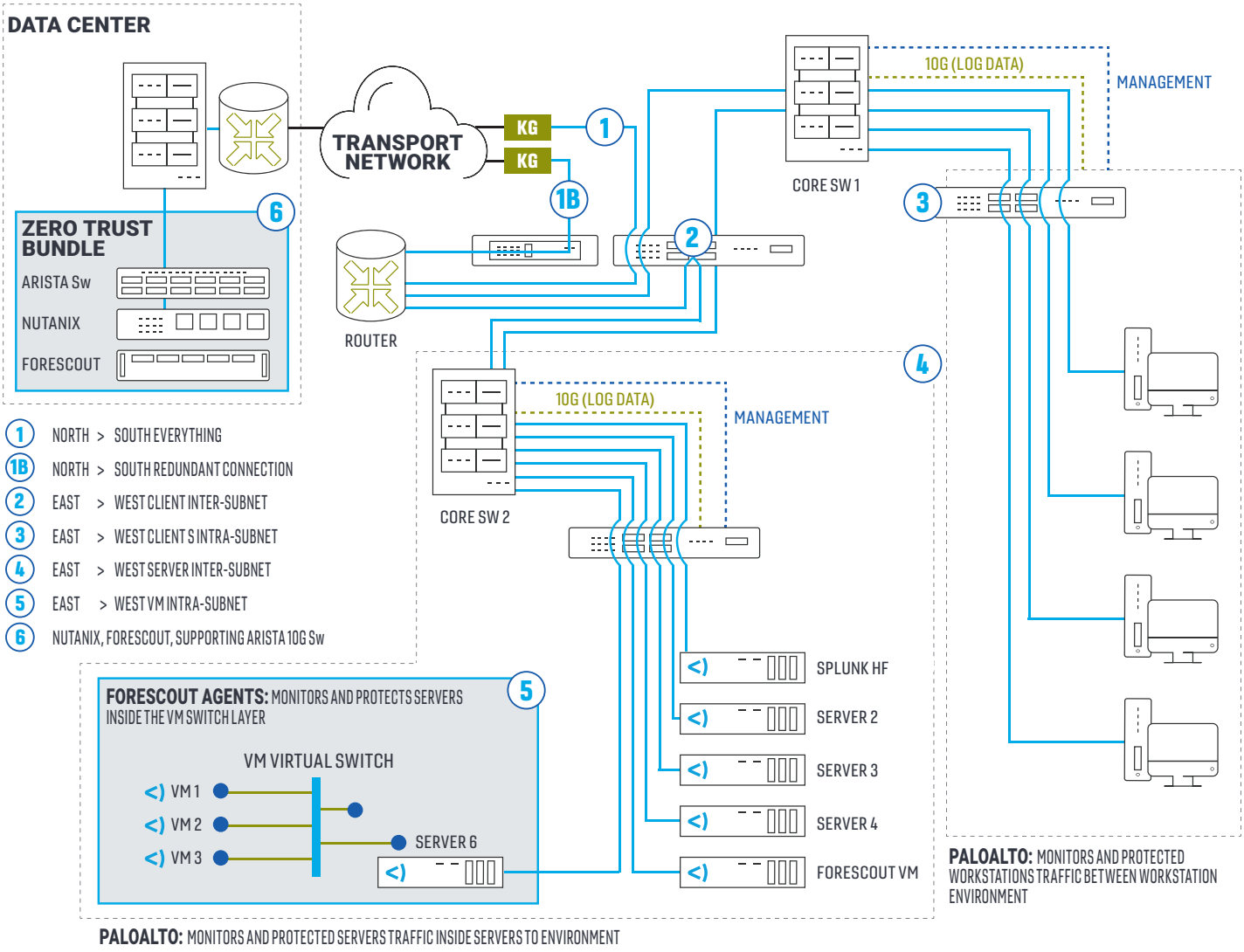
ZT is a cybersecurity set of concepts, which can drive policies, processes, and architecture based on the simple premise of "never trust, always verify." As discussed within this whitepaper, the ZT concepts are built upon a set of foundational pillars, which apply to identity/user, device, network, infrastructure, application, data, visibility and analytics, security orchestration and automation, and information governance.

There are five key steps that are essential when building a ZTA for a government agency and as demonstrated by the three Peraton ZT case studies, there are numerous ways to successfully design and implement a ZT solution.

The real key to success in transforming ZT cybersecurity concepts into actual solutions is always understanding each government agency's unique technical and business challenges, recognizing the evolving cyber threat environment, and selecting, and then integrating the right technology systems and tools for the government agency's specific requirements. ZT is not an all or nothing proposition for government agencies—Peraton is ready to work with agencies to develop customized cybersecurity ZT solutions that fit their unique information security posture.

APPENDIX 1

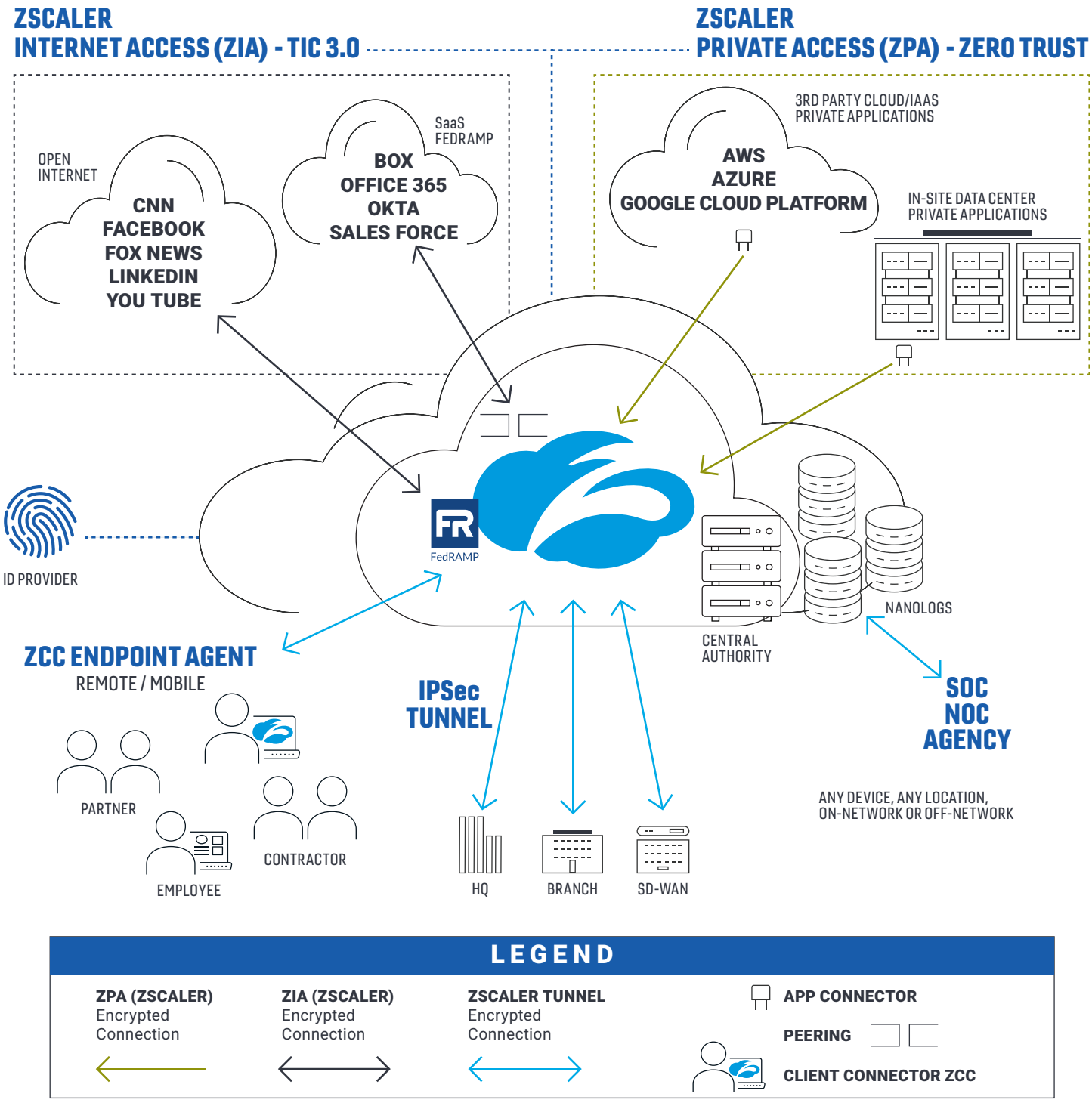
ZERO TRUST ARCHITECTURE



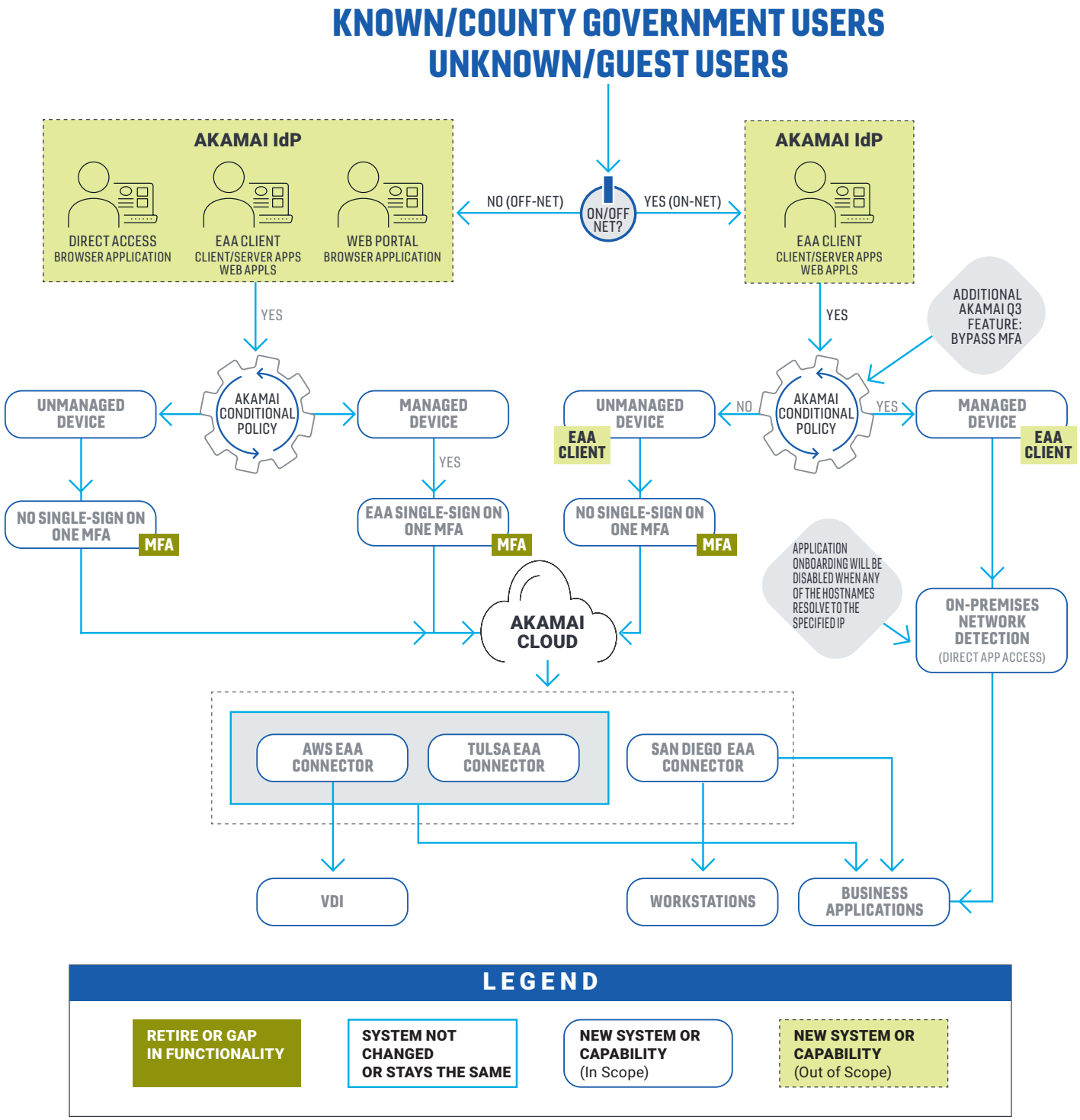
APPENDIX 2

ZSCALER FEDERAL PLATFORM

Bypass the TIC secure policy-based access to applications, internet, and SaaS services over encrypted connections



APPENDIX 3


KNOWN/COUNTY GOVERNMENT USERS
UNKNOWN/GUEST USERS
AKAMAI IdP
DIRECT ACCESS
BROWSER APPLICATION
EAA CLIENT
CLIENT/SERVER APPS
WEB APPLS
WEB PORTAL
BROWSER APPLICATION
NO (OFF-NET)
ON/OFF NET?
YES (ON-NET)
AKAMAI IdP
EAA CLIENT
CLIENT/SERVER APPS
WEB APPLS
YES
YES
ADDITIONAL AKAMAI Q3 FEATURE: BYPASS MFA
UNMANAGED DEVICE
AKAMAI CONDITIONAL POLICY
MANAGED DEVICE
YES
UNMANAGED DEVICE
EAA CLIENT
NO
AKAMAI CONDITIONAL POLICY
YES
MANAGED DEVICE
EAA CLIENT
NO SINGLE-SIGN ON ONE MFA
MFA
EAA SINGLE-SIGN ON ONE MFA
MFA
NO SINGLE-SIGN ON ONE MFA
MFA
APPLICATION ONBOARDING WILL BE DISABLED WHEN ANY OF THE HOSTNAMES RESOLVE TO THE SPECIFIED IP
ON-PREMISES NETWORK DETECTION
(DIRECT APP ACCESS)
AKAMAI CLOUD
AWS EAA CONNECTOR
TULSA EAA CONNECTOR
SAN DIEGO EAA CONNECTOR
VDI
WORKSTATIONS
BUSINESS APPLICATIONS
LEGEND
RETIRE OR GAP IN FUNCTIONALITY
SYSTEM NOT CHANGED OR STAYS THE SAME
NEW SYSTEM OR CAPABILITY (In Scope)
NEW SYSTEM OR CAPABILITY (Out of Scope)

Peraton

ABOUT PERATON

Peraton drives missions of consequence spanning the globe and extending to the farthest reaches of the galaxy. As the world's leading mission capability integrator and transformative enterprise IT provider, we deliver trusted and highly differentiated national security solutions and technologies that keep people safe and secure. Peraton serves as a valued partner to essential government agencies across the intelligence, space, cyber, defense, citizen security, health, and state and local markets. Every day, our employees do the can't be done, solving the most daunting challenges facing our customers.

Scan to learn more at
peraton.com/**capabilities/cyber**