AVERTIUM

ZERO TRUST NETWORK SERVICES

PRECISE TRUST, FOCUSED DEFENSE

Expanding endpoints and cloud computing environments have decimated the perimeter, a process accelerated by a rapid transition to work-from-anywhere. Gone are strictly on-premises solutions, making way for complex architectures that can allow a single trusted but compromised device unfettered access.

The time to act is now.

Zero Trust Network Access (ZTNA) stops malicious traffic at the edge before it can discover, identify and target enterprise servers, cloud services or remote devices.

Zero Trust avoids flaws typical of other solutions like split-tunnel VPN that leave an environment open to attack by combining the rigor of secure connectivity with device security posture assessments and centralized identity access management.

TACKLE THE IMPLEMENTATION CHALLENGES

Engineering a rigorous ZTNA architecture involves significant effort and commitment, a factor that may affect your plan for adoption. Avertium works alongside you to tackle the challenges of applying an effective solution, enabling quicker implementation:

- Identifying and organizing sensitive systems and data for proper segmentation
- Ensuring legacy and/or existing system and process compatibility over peer-to-peer, hybrid cloud, and decentralized operations that break the least privilege model
- Understanding which data needs to be accessed, how it should be accessed, and by whom

OUR ZERO TRUST SERVICES

No matter where you are in your Zero Trust journey, Avertium is ready to help with a range of consulting services:

- Readiness Assessment
- Architecture and Design
- Implementation (Incremental or Full)
- Fully Managed Turnkey ZTN-as-a-Service

THE AVERTIUM ADVANTAGE

Avertium applies decades of combined experience to implement an end-to-end software based ZTNA architecture to new or existing environments. No network hardware replacement is required to bulk up secure access for more rigor, more responsiveness and more relevance.

More Rigor

» Enhanced data protection

» Accelerated cloud migration

» Fully enforced least privilege

More Relevance

» Reduced complexity

» Enhanced containment

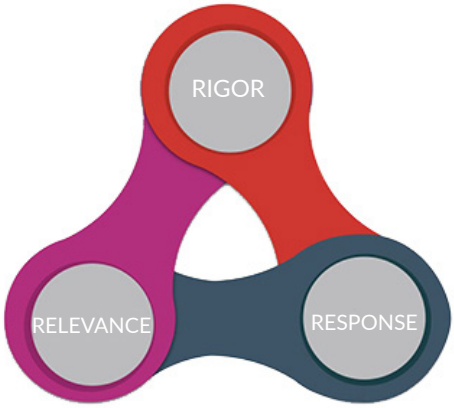
» Elevated user experience

More Responsiveness

» Faster breach detection

» Superior response

» Built-in need-to-know



HOLISTIC XDR

ZTNA is a key component of Avertium's rigorous approach to providing extended detection and response (XDR) to give our customers more visibility into data across networks, clouds, endpoints and applications. In addition to Zero Trust, we offer these XDR-related services:

- TruSOC Managed Security Services
- Endpoint Detection and Response
- Vulnerability Management
- Compliance Consulting

ABOUT AVERTIUM

Avertium brings enterprise-level security to mid-sized and larger organizations challenged by the cybersecurity talent shortage, rapidly evolving threat landscape and budgetary constraints. The company's acclaimed show-no-weakness approach to extended detection and response (XDR), governance and compliance, and strategic advisory services is redefining the managed security services category. From financial services and manufacturing, to technology and healthcare, more than 2,500 companies rely on Avertium's more rigorous, more relevant, and more responsive delivery of cybersecurity services. Backed by growth equity firm Sunstone Partners, Avertium operates CyberOps Centers of Excellence in Arizona, Colorado, and Tennessee.

+1 (877)-707-7997 | hello@avertium.com | www.avertium.com