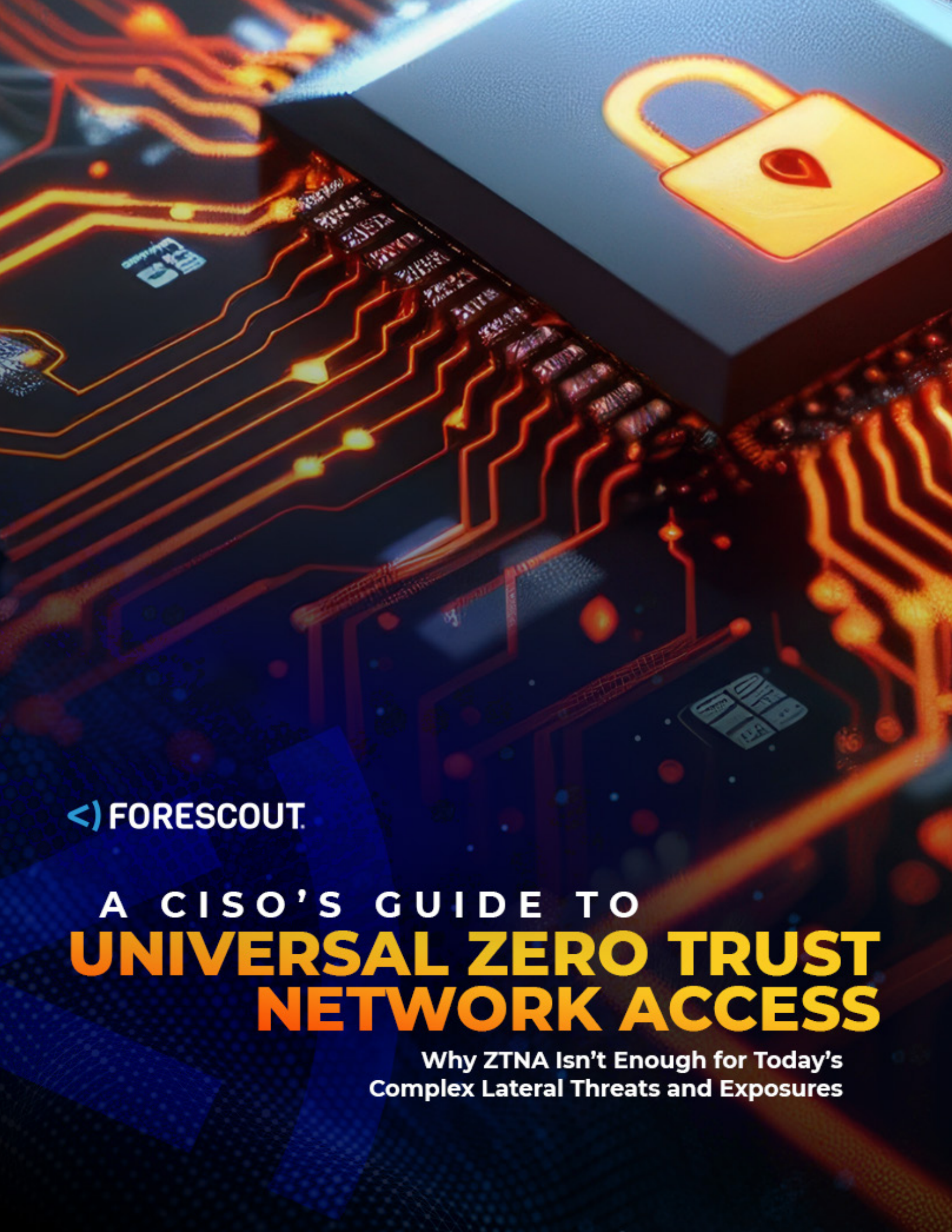


FORESCOUT

A CISO'S GUIDE TO UNIVERSAL ZERO TRUST NETWORK ACCESS

Why ZTNA Isn't Enough for Today's Complex Lateral Threats and Exposures

FORESCOUT

A CISO's Guide to Universal Zero Trust Network Access

Why ZTNA Isn't Enough for Today's Complex Lateral Threats and Exposures

TABLE OF CONTENTS

INTRODUCTION:
A Necessary Evolution in Zero Trust

Universal Zero Trust Network Access, or UZTNA, is the logical evolution of ZTNA solutions which primarily focus on mobile or remote off-network assets. Universal ZTNA offers a unified approach regardless of a user or device's physical location or asset type — covering IT, operational technology (OT), Internet of Things (IoT), and Internet of Medical Things (IoMT) environments.

Unfortunately, too many vendor-centric definitions of UZTNA are confusing the market. This is nothing new in Zero Trust. "The term 'Zero Trust' has become excessively used and misapplied, leading to significant confusion among organizations. For many security leaders, it has become a source of frustration due to inconsistent messaging and aggressive marketing tactics." finds Gartner®. [i]

Despite the recent introduction of UZTNA, some vendors have already done a disservice by doing one or more of the following:

- Defining traditional ZTNA as Universal ZTNA
- Minimizing UZTNA's importance by identifying it as a subset of Secure Access Service Edge (SASE)
- Promoting the routing of all traffic through a single cloud, creating a single point of failure
- Suggesting architectures that introduce significant network latency
- Ignoring industrial control systems and other operational technologies (ICS/OT)

This guide explains in clear terms: what Universal Zero Trust Network Access is, why it is needed, how to reach a best-in-class version, and the gaps you can close in today's ZTNA.

What is UTZNA?

UZTNA defines and enforces network access policies from real-time context and continuous risk assessment, so organizations can protect all assets while meeting regulatory and business requirements, not just the remote or mobile ones. UZTNA offers a better approach to adapt to real-world threats and operational requirements than ZTNA..

Seven Reasons Why Organizations Need UZTNA

The foundational goal of UZTNA is to accurately discover, classify, and govern all assets that touch the corporate network within a security context. When implemented properly, it enables CISOs to ensure seven critical aspects of cybersecurity:

1. Deliver consistent user experiences regardless of location

UZTNA improves user experiences by providing consistent, fast, and seamless access to applications and data from anywhere, thanks to a unified security policy that verifies users, devices, and machines in real-time. This optimizes productivity, regardless of location

2. Enforce policies for all assets: managed, unmanaged IT, OT, IoT, and IoMT

The increasing growth of unmanaged IoT/OT devices creates additional vulnerabilities beyond the perimeter that often lead to audit failure, breaches, and loss of sensitive data.
Most IT teams lack the ability to assess, in real time, all asset types, managed and unmanaged, to confirm they comply with their organization's security framework.

UZTNA enables security leaders to accurately discover, classify, and inventory all assets—including managed, unmanaged, legacy, and headless devices across IT, OT, IoT, and IoMT environments. This granular visibility ensures that no device or endpoint operates outside the scope of security controls.

> ***"Security and risk management leaders responsible for Zero Trust should evaluate vendors whose Zero-Trust capabilities extend across hybrid environments, covering on-premises, multicloud and cyber-physical system (CPS)/operational technology (OT) environments, ensuring integration with threat detection and response platforms allowing for continuous control of zero-trust posture." – Gartner*** [ii]

3. Implement identity-based, location-agnostic access policies

People and devices now operate in a wide range of locations:

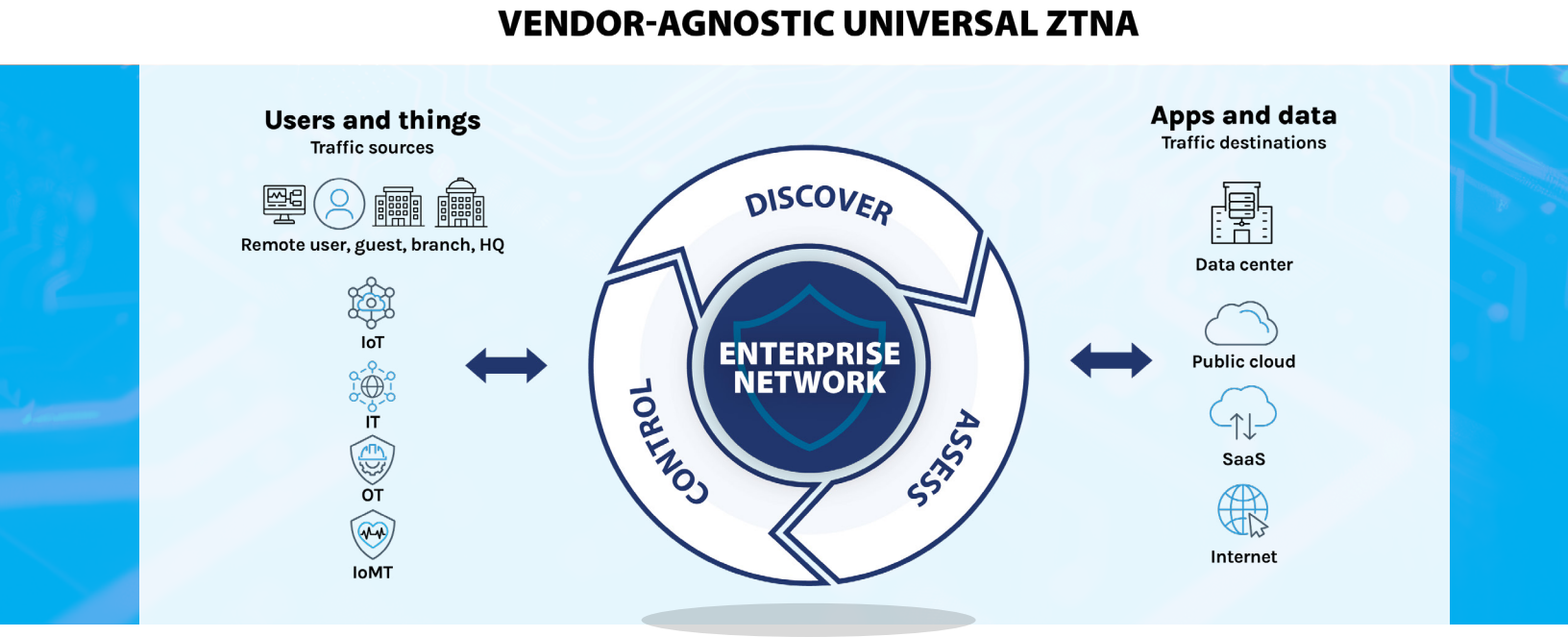
- On campus networks
- In branch offices
- In factories and OT/ICS environments
- From home or on the road

UZTNA continuously identifies all connected assets, assesses their posture and compliance and enforces zero trust access policies across heterogeneous networks. In short, it's meant to secure the connected lifecycle of an asset.

4. Extend Zero Trust policies across campus, branch, OT, remote assets, and users

Modern environments are highly distributed, and attackers exploit any weak link. Zero Trust only works when every domain is covered. Not only the data center or cloud environment.

If Zero Trust stops at one boundary, attackers simply target the unprotected areas. The 'universal' coverage part of UZTNA ensures consistent protection everywhere users or devices connect.



5. Enable adaptive access controls based on user/device risk

Adaptive access controls advance from traditional perimeter-based security models to dynamic cybersecurity. Organizations that follow a UZTNA approach can establish asset visibility and intelligence—and emphasize continuous improvement and agility through six key phases:

1. **Address visibility gaps:** Address the gaps in network visibility with asset discovery and classification for all asset types – IT, IoT, OT, ATMs, servers, and headless endpoints.
2. **Integrate device trust:** Account for posture validation, hygiene, and certificates as part of least privilege access policies
3. **Control lateral movement:** Apply microsegmentation everywhere.
4. **Unify risk visibility:** Establish continuous monitoring and adaptive policies to keep pace with evolving threats and vulnerabilities.
5. **Automate:** Leverage closed-loop controls for automating policy enforcement and asset management across all environments.
6. **Tune:** Continuously optimize security policies based on integrated system feedback.

This prescriptive and sequenced approach significantly reduces the risk of exploitation by attackers without overwhelming existing systems and resources.

6. Apply policies to devices that do not have an associated user

Increasingly, new lines of IoT and OT devices and systems operate autonomously, with no human using the device. Using Universal ZTNA, organizations can account for and treat these systems and devices in the same manner they do for people and all other device types.

7. Eliminate visibility gaps caused by fragmented security solutions

UZTNA works best when an organization can leverage the security tools already in place. Not only does this minimize disruption in the transition to UZTNA, but it also better positions the organization to take an adaptive approach to the fast-evolving threat landscape. Leveraging a vendor- and tool-agnostic approach to UZTNA enables CISOs to work with a wide variety of networking vendors, device vendors, and security tools with a best-in-class approach.

Taking advantage of UZTNA to do each of these seven things will progress an organization toward a high level of maturity in the context of their cybersecurity stance and the Zero Trust Maturity Model v2.0. Moreover, it aligns them with standards bodies and regulators on Zero Trust today.

What Standards Bodies and Training Institutes Say About Zero Trust

The National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Agency (CISA) have published positions to which Universal ZTNA aligns very well. Moreover, these positions align across the two standards bodies.

NIST

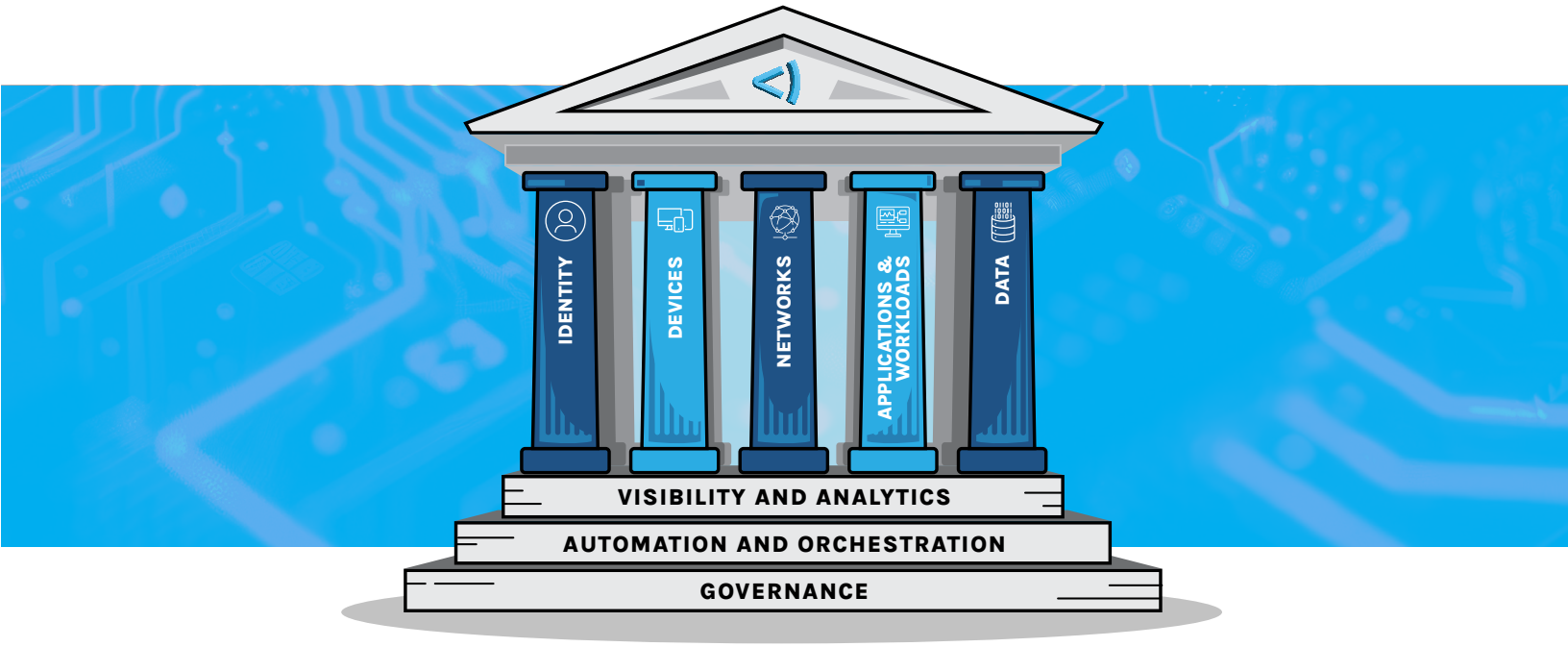
Published in 2010, NIST SP 800-207, entitled “Zero Trust Architecture,” is a foundational NIST publication that defines a modern cybersecurity model, shifting focus from traditional network perimeters to verifying every user, device, and application request, embodying the principle “never trust, always verify.”

NIST SP 800-207:

- All data sources and computing services are considered resources.
- All communication is secured regardless of network location.
- Users are granted access to individual enterprise resources on a per-session basis.
- Access to resources is determined by dynamic policy.
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
- Dynamic resource authentication and authorization are strictly enforced before allowing access.
- The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.

CISA

The Cybersecurity and Infrastructure Agency (CISA) leverage the points from NIST to provide a Zero Trust Maturity Model (ZTMM) that helps guide priorities. It focuses on five distinct pillars – Identity, Devices, Networks, Applications & Workloads, and Data. Cross-cutting capabilities include Visibility and Analytics, Automation and Orchestration, and Governance (see below).



NIS 2 Directive

The European Union (EU) has established a law for cybersecurity—the NIS 2 Directive—that targets critical infrastructure and digital services in the EU and is legally binding with mandatory compliance and fines for noncompliance. In Preamble 89 of the Directive, The EU requires continuous verification, least privilege access, strong authentication, and monitoring, aligning with Zero Trust's "never trust, always verify" model to protect against modern threats by assuming breaches and verifying every access request, regardless of location.

SANS Institute

The SANS Institute for SysAdmin, Audit, Network, and Security has also recognized the need to assume breaches and to verify every access request in its definition of Zero Trust Architecture: "Zero Trust Architecture (ZTA) is a security model based on the principle of least privilege. This principle specifies that users and devices receive only the permissions necessary to perform their tasks."

Maturity Model Gaps in Traditional ZTNA

Unlike UZTNA, traditional ZTNA leaves significant gaps in the Zero Trust Maturity Model as defined by the standards bodies and training institutes.

Blind Spots in Locations and Assets

Covered First, with traditional ZTNA, enforcement is tethered to the cloud, and since the cloud has traditionally focused on IT, it lacks security controls for other asset types, especially cyber-physical systems, including OT devices and systems. With cyber-physical systems, a security service must account for both agent-based enforcement and agentless capability to ensure it incorporates all system and device types, including those that do not accept an agent. In addition, ZTNA has not evolved to span campus and branch locations.

ASSET TYPES ● *Covered* ◑ *Partial Coverage* ○ *Not Covered*

IT	ZTNA	Universal ZTNA
Managed Endpoints (Laptops, Mobile, VDI)	●	●
Cloud Virtual Machines (IaaS)	●	●
SaaS Applications	●	●
Web Applications (HTTP/HTTPS)	●	●
Internal Web Apps & APIs	●	●
BYOD & Contractor Devices	◑	●
Wireless Access Point	◑	●
Servers & VMs	◑	●
Domain Controller	◑	●
Firewall	○	●
Router	○	●
Intelligence Platform Management Interface (IPMI)	○	●

ASSET TYPES ● *Covered* ◑ *Partial Coverage* ○ *Not Covered*

OT	ZTNA	Universal ZTNA
Core Controllers (PLCs, RTUs, DCS)	○	●
SCADA, HMI & Control Servers	○	●
Safety & Instrumented Systems (SIS)	○	●
Robotics, CNC & Assembly Systems	○	●
Industrial Sensors, Actuators & Drives	○	●
Power, Utilities & Energy Control Systems (UPS, Gateways)	○	●
Building & HVAC Control Systems (BMS)	○	●
Physical Access Control Systems	○	●
Industrial Historians	○	●

ASSET TYPES ● Covered ◑ Partial Coverage ○ Not Covered

IoT	ZTNA	Universal ZTNA
Network Attached Storage	◑	●
Printers, Wireless APs & Conference Systems	◑	●
Physical Security (IP Cameras, Badge Readers)	○	●
Point of Sale (PoS), Kiosks & Digital Signage	○	●
Smart Facilities (Lighting, Meters, BMS)	○	●
Network Video Recorder	○	●
VoIP Systems	○	●

ASSET TYPES ● Covered ◑ Partial Coverage ○ Not Covered

IoMT	ZTNA	Universal ZTNA
Healthcare Workstations (Clinical Endpoints)	●	●
Medical Information Systems	●	●
Clinical Imaging Infrastructure (PACS, DICOM Workstations)	◑	●
Patient Monitoring Systems & Smart Beds	○	●
Networked Life-Critical Devices (Infusion Pumps, Controllers)	○	●
Imaging & Diagnostic Systems (MRI, CT, X-Ray, Ultrasound)	○	●
Medication Dispensing Systems	○	●
Laboratory Equipment & Diagnostic Analyzers	○	●
Electrocardiograph (ECG/EKG) Systems	○	●

Speed & Latency Issues

Another major ZTNA weakness is its reliance on cloud performance and impact from cloud latency. ZTNA solutions perform more slowly than required in certain situations, especially in critical infrastructure where seconds can mean lives or massive operational disruption. OT systems (I.e., SCADA, PLCs, RTUs, sensors, actuators, etc.) have very different performance constraints than IT systems. For example, many of them use the following:

- Low-latency, deterministic communication loops
- Polling cycles of 10–250 milliseconds
- Protocols that are sensitive to jitter (e.g. Modbus, DNP3, OPC UA)
- Local loop control that must not be delayed

If an organization plans to route this type of OT traffic through a cloud-based Zero Trust platform for inspection, it can introduce several performance issues:

- Round-trip latency to the nearest cloud PoP
- Inspection latency
- Potential jitter due to variable routing conditions

For some OT processes, adding just tens of milliseconds of delay can disrupt the process. For users located in branch or campus locations, cloud performance variables including distance, network hops, and congestion cause slow application performance. User experience suffers due to frozen screens, stuttering video, delayed data, and more. All these things hamper productivity, especially in the use of real-time apps.

Real-Time Applications Hurt by Poor Cloud Performance

- AI and machine learning inference
- Virtual desktop infrastructure
- IoT
- Industrial automation
- IoMT in healthcare
- Voice over IP and video conferencing
- Augmented reality and virtual reality

Single Point of Failure

Typically, ZTNA providers want your data to run only through its cloud service, introducing a single point of failure. According to the Atlantic Council's "Critical infrastructure and the Cloud: Policy for Emerging Risk" publication: "The cloud is unique in how deeply it concentrates risk for hundreds and thousands of entities by stacking that risk on a few specific technology nodes." [iii]

The cloud risk assessment underscores how organizations that delegate control and visibility to cloud services lose visibility into the operations and failure modes of cloud's technology systems, putting their organization at risk.

Gartner states that, "Cloud concentration risk has come about because many organizations have opted to focus their IT efforts on a handful of strategic providers in order to reduce IT complexity, and therefore also risk, cost and skill requirements." And "There are three main potential consequences of this risk, according to Gartner experts." [iv]:

- **Wide incident "blast radius"**
  The more applications (and business processes) depend on a particular cloud provider, the greater the potential breadth of impact of a cloud service issue, which may heighten business continuity concerns.
- **High vendor dependence**
  Concentrated dependency on a particular vendor can reduce future technology options and allow vendors to exert significant influence over the organization's technology future.
- **Regulatory compliance failures**
  Organizations may be unable to meet regulatory demands to address concentration risk across different regulatory bodies, which may have different approaches to concentration risk.

Difficulty Orchestrating Best-in-Class Technologies

In designing the original concept of Zero Trust, NIST intended for organizations to pursue a vendor-agnostic approach. This would allow organizations to flexibly leverage best-of-breed security solutions that encompass the entire organization or extended enterprise.

Originating as a single-vendor cloud solution, ZTNA has traditionally proven to be a poor choice for orchestrating disparate technologies from multiple vendors. ZTNA has not provided a vendor-agnostic path to Zero Trust.

ZTNA capabilities are siloed for two main reasons. First, they were never intended to be a solution or framework to address the security of everything connecting to the enterprise network. It was not designed as a multi-vendor, universal framework.

Secondly, ZTNA has a limited focus in secure access to applications for remote users (initially driven by remote user needs during the COVID pandemic). Even today, ZTNA solutions continue to have limited integration with threat detection, security posture assessment platforms, and remediation tools.

Universal ZTNA Closes the ZTNA Gaps

UZTNA raises the bar in Zero Trust by improving upon the areas where it has traditionally focused — expanding the scope, accounting for greater context, and introducing a dynamic aspect to security postures.

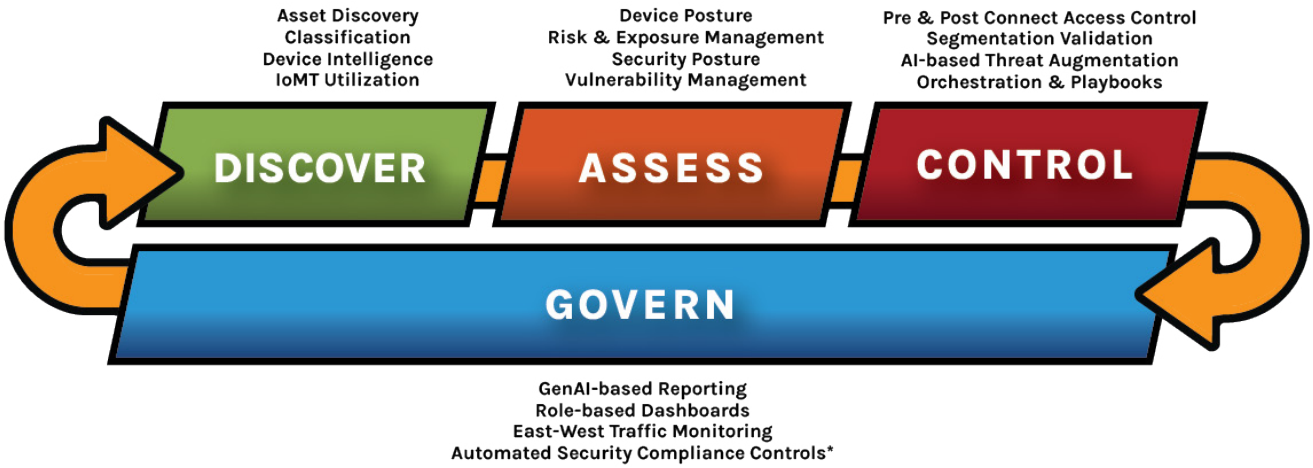
1. Asset Identification Across All Asset Classes: The foundation of UZTNA is the ability to accurately discover, classify, and inventory all assets—including managed, unmanaged, legacy, and headless devices across IT, OT, IoT, and IoMT environments. This granular visibility ensures that no device or endpoint operates outside the scope of security controls.

2. Never Trust, Always Verify Model: Each connection is linked to a continuously verified identity, evaluating posture, behavior, and context in real time so that trust is constantly reassessed.

3. Least Privilege Access: UZTNA enforces least privilege access by dynamically granting only the permissions and network access required for each asset's function. Today, a user identity determines what they have access to yet is insecure due to the prevalence of compromised credentials. UZTNA's risk-based approach minimizes the attack surface and limits lateral movement. When proper segmentation is applied, it greatly reduces exposure (aka: blast radius) to both malware and insider threats.

4. Continuous, Contextual, and Dynamic Access Evaluation: Rather than relying on static policies, UZTNA continuously assesses the risk posture of each asset and session. Access rights are dynamically adjusted in real time based on contextual factors such as user behavior, asset health, location, and the prevailing threat landscape. This ensures that trust is never assumed and is always verified.

UZTNA operates through a process flow that begins with comprehensive asset discovery and classification. Every device is identified and profiled. Whether it's traditional IT, OT, such as PLC's and RTU's, or IoT including printers and badge readers, or a connected medical device. Access policies are



then orchestrated based on the device's identity, context, and security posture, including risk score, behavior, and compliance. These policies are applied dynamically, leveraging integrations with native and third-party security tools to enforce segmentation, quarantine, or remediation actions as needed.

Continuous monitoring and threat intelligence further ensure that access remains appropriate as context evolves, delivering a Universal Zero Trust posture across the entire organizational landscape.

References

[i] Gartner, Predicts 2025: Scaling Zero-Trust Technology and Resilience, Charanpal Bhogal, Wayne Hankins, et al., 21 March 2025.

[ii] Ibid.

[iii] Tianjiu Zuo et al (2023). "Critical infrastructure and the cloud: Policy for emerging risk," Atlantic Council.
Accessed December 5, 2025 from the following source:
Critical infrastructure and the cloud: Policy for emerging risk - Atlantic Council.

[iv] Gartner Press Release, Gartner Says Cloud Concentration Now a Significant Emerging Risk for Many Organizations, October 30, 2023
https://www.gartner.com/en/newsroom/press-releases/2023-10-30-gartner-says-cloud-concentration-now-a-significant-emerging-risk-for-many-organizations/

FORESCOUT

See how we can help your organization implement UZTNA at
https://www.forescout.com/

About Forescout

For over 25 years, organizations and governments worldwide have trusted Forescout to secure their networks. From pioneering Network Access Control (NAC) to delivering Universal Zero Trust Network Access (UZTNA), Forescout leads the evolution of enterprise network security across IT, OT, IoT, and IoMT environments. The Forescout 4D Platform™ delivers comprehensive asset intelligence, continuous risk assessment, and dynamic control, over all managed and unmanaged assets, enhanced by the proprietary threat intelligence research of Vedere Labs. Leveraging agentic AI workflows with human-in-the-loop actions, Forescout continuously analyzes threats, orchestrates response, and integrates seamlessly with 180+ security and IT products.

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com