
IDMWORKS
Identity & Access Management Specialists
Zero Trust Identity Journey
identiverse
#identiverse

Abhi Sarmah

Director, Technical Solutions

IDMWORKS

What is Zero Trust

"Zero Trust is an information security model that denies access to applications and data by default. Threat prevention is achieved by only granting access to networks and workloads utilizing policy informed by continuous, contextual, risk-based verification across users and their associated devices." – **Forrester Research**

"Zero Trust is strategically focused on addressing lateral threat movement within the network by leveraging micro segmentation and granular enforcement based on user context, data access control, location, application and device posture." – **Forrester Research**

"Zero trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated. Zero trust architecture is an end-to-end approach to enterprise resource and data security that encompasses identity (person and non-person entities), credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure." – **NIST SP 800-207**

"Zero trust is a security paradigm that explicitly identifies users and devices and grants them just the right amount of access so the business can operate with minimal friction while risks are reduced." – **Gartner**

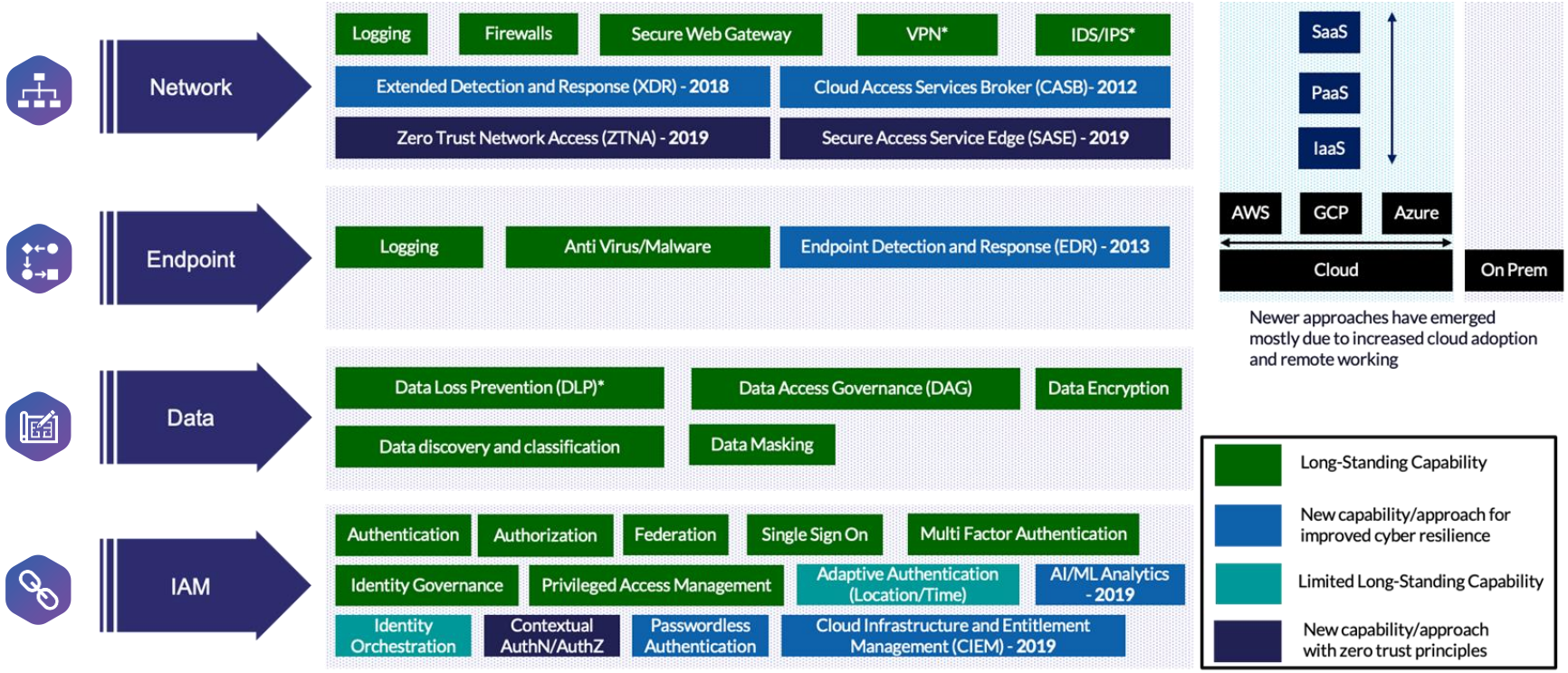
Key Tenants of Zero Trust

- ❖ Default deny
- ❖ Access by policy only
- ❖ Least privilege access
- ❖ Security monitoring and Incident response
- ❖ Continuous risk-based verification and contextually aware dynamic policy enforcement

Current Cyber Capabilities and Transition to Zero Trust

Legacy and Emerging Capability Map

Several cyber security capabilities have existed for years. Vendors have innovated and introduced new capabilities to address new threats emerging due to the increased cloud migration and increasingly remote workforce, some of these new capabilities have been designed with Zero Trust principles at its core.

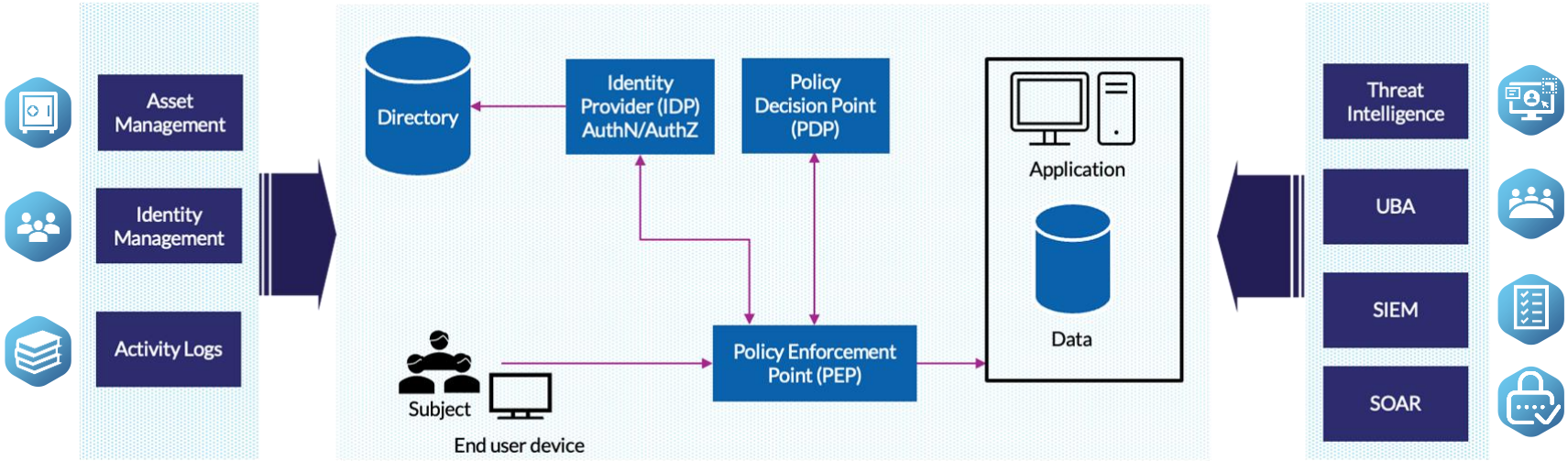


*Some modern solutions combine these capabilities

*Some modern solutions combine these capabilities

Zero Trust Reference Architecture/ Ecosystem

Orchestration capabilities are required for both incident response and enforcing access policies based on contextual awareness



- Knowing your users and assets is fundamental to enforcing Zero Trust principles, as such strong Identity Governance and Asset Management capabilities are required
- Orchestration capabilities are required for adding more context to dynamic policy enforcement for access decisions
- Orchestration is required for monitoring activities to improve the incident response capabilities and improving the effectiveness of SOC operations

Identity as Key Enabler of your Zero Trust Journey

Identity Capabilities and Support for Zero Trust

Identity and Access Management capabilities are critical in supporting the enforcement of Zero Trust principles. Mature Identity operations are critical in enforcing least privilege and in ensuring that legitimate and authorized users are accessing information assets.

IAM Area	Functional Capability	Capability Status	Zero Trust Prerequisite Supported	PEP Function Supported
IGA	Use Lifecycle Management	Long-Standing	Know your users	Authentication
	Automated Provisioning and Deprovisioning	Long-Standing	Know your users and their access	
	Role Management	Long-Standing	Least privileged access	Authorization
	Access Certification	Long-Standing	Know your users and their access	Authorization
Access Management	MFA	Long-Standing	Additional factor for authentication	Authentication
	Adaptive Authentication	Long-Standing	Contextual authentication	Authentication
PAM	Privileged Account Password Vaulting	Long-Standing	Improved cyber security	N/A
	JIT Access	Long-Standing	Never trust	N/A
	Session Recording and Monitoring	Long-Standing	Never trust	N/A

Zero Trust Capability Journey

Organizations need to evaluate current gaps in capability for enforcing Zero Trust principles, acquire missing capabilities and focus on maturity of overall cyber resilience and take incremental steps to enforce Zero Trust.

Legacy Security

- Focused on Perimeter-based controls
- ✓ VPN
- ✓ Firewall
- ✓ Intrusion Detection
- ✓ Network-based authentication
- ✓ Limited or lack of automation for IAM

Stage 1: Add Capability	Stage 2: Mature Capability
❖ Automate user lifecycle processes and provisioning	❖ Integrate critical application for automated provisioning
❖ Add privileged access management capabilities	❖ Improve role management using modern approaches
❖ Integrate PAM with IGA for MFA	❖ Improve cloud access visibility
❖ Add cloud-based access management capability with MFA	❖ Expand PAM coverage to all critical infrastructure and applications
❖ Add information asset management capabilities	❖ Implement ongoing privileged account discovery and just in time access
❖ Improve threat intelligence capabilities	❖ Manage third party privileged access
❖ Add Identity Analytics and orchestration capabilities	❖ Integrate critical applications with cloud-based authentication solution
❖ Add application specific access models such as ZTNA/SASE	❖ Start implementing adaptive authentication policies

Zero Trust Security

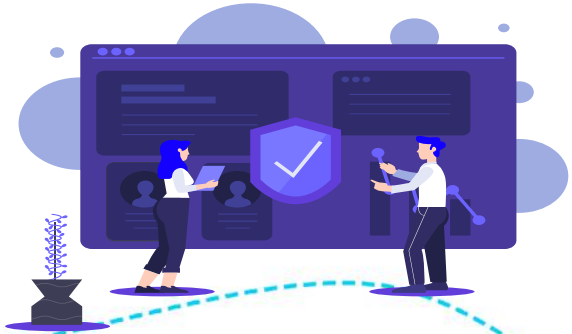
- Focused on Identity-based controls
- ✓ Per connection-based authentication
- ✓ Per application-based authentication
- ✓ Contextual authorization
- ✓ Continuous risk evaluation and access policy enforcement

Where Should I Start?

- Know and manage your **users** (enterprise, partners, customers, vendors)
- Know and manage your **critical information assets** (applications, data) and their users
- **Build foundational capability** that may not exist in various layers (Network, endpoint and IAM) – most capabilities exist now to position you on your journey to zero trust
- Map all your **use cases** specific to subjects (users) accessing resources (application and data) - this includes assets, subjects, business processes, traffic flows.
- Work with your business to identify use cases for **pilot implementation**
- Re-evaluate your security policies, zero trust approaches will likely make enforcement of various policies more automated and will likely **remove exceptions**

Conclusion

- It is important to balance security, usability, and user experience
- No single solution will enforce zero trust end to end, as such, various capabilities will need to co-exist and must be able to share relevant information with other solutions through a robust API
- Orchestration capabilities will need to be developed in-house or use vendor provided solutions for adding additional context for making risk based dynamic access decisions
- Technology specifications will likely change and, in some cases, will require significant updates- such as endpoint health for federated connections




THANK YOU!
IDMWORKS
identiverse
#identiverse