Fidelis Whitepaper

Zero Trust Architecture (ZTA)

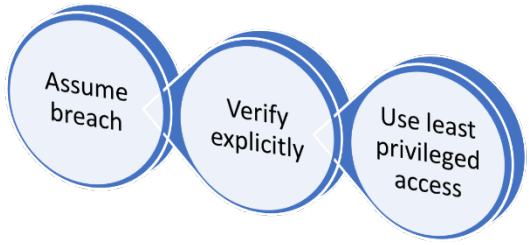
Executive Summary

As organizations with complex IT environments look to protect, defend and respond to increasingly sophisticated threat actors, the concept of a Zero Trust Architecture (ZTA) is now an imperative. As defined by the NSA, Zero Trust "embeds comprehensive security monitoring; granular, dynamic, and risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus specifically on protecting critical assets (data) in real-time within a dynamic threat environment." Following cyber intrusion events involving the software supply chain in 2020 and 2021, NSA issued guidance in February 2021 specifically recommending that US government organizations and their industry partners implement ZTA to combat active and ongoing cyber threats to systems and data.

In 2002, Fidelis began developing Elevate™ using a zero trust approach, with "inspect everything, trust nothing" as the guiding principle. Since then, the platform has evolved into a state-of-the-art eXtended Detection and Response (XDR) solution incorporating three essential data protection capabilities: Network (traffic analysis (NTA)), Endpoint (detection and response (EDR)) and Deception, fully integrated in a single cyber defense platform. This whitepaper explains that ZTA is more than overlaying identity and authentication capability, and how Fidelis Elevate helps customers achieve and realize a robust ZTA solution required to protect sensitive missions and data that peer cyber adversaries are targeting hourly.

Zero Trust Now

ZTA assumes that an intruder is already dwelling within the cyber terrain of the distributed enterprise. The premise of Zero Trust is that every person, place or thing accessing protected data is untrustworthy until proven otherwise—Assume breach, and explicitly verify the security status of identity, endpoint, network and other resources based on all available signals and data. Use least privileged access. And, once proven, verify again and again to protect data, systems and services.



Organizations adopting a Zero Trust architecture across their entire IT environment must have visibility and control to address current threats and dwell time. Moreover, compliance with ZTA must be easier and more automated than existing security measures, with the ability to verify at cyber speed that sensitive data is always protected. In short, organizations embracing ZTA must do so in a way that assures a complete view of all network activity—both authorized and not.

The Challenge

The accelerated move to the cloud, increased use of BYOD, IoT and shadow IT, and abrupt shift to "working from anywhere" in the context of escalating offensive cyber activity exponentially complicates the IT security landscape and role of cyber security. Enterprises must provide secure access to company resources from any location and device, protect interactions with business partners, and shield client-server, as well as inter-server communications. The security perimeter is constantly changing as new devices and services are added. Every connection, each managed and unmanaged device, and all new services are a potential point of vulnerability. Simultaneously, adversaries are becoming more sophisticated. They are infiltrating deeper, dwelling longer, imposing incalculable cost, and doing significantly more damage. Thus, overlaying identity and authentication enforcement alone, and calling it ZTA, does not ensure a secure cyber ecosystem.

Embracing Zero Trust Architecture

Getting to Zero Trust is an evolution, with analytics, machine learning, and automation as fundamental requirements. One approach to ZTA design is to start small and expand into broader, enterprise-wide deployment. Some opt to start the transition by ensuring that any new digital transformation initiatives are aligned with a Zero Trust framework, adding Zero Trust capabilities as they shift workloads to the cloud. Others prefer to bring Zero Trust capabilities to their most critical or sensitive systems, first. Fidelis supports any of the pure or hybrid approaches data owners elect to pursue.

Fidelis and Zero Trust Architecture

Fidelis Elevate™ eXtended Detection and Response (XDR) aligns with the NIST framework in SP 800-207 and enables the rapid transition of enterprise infrastructure to Zero Trust principles. Elevate XDR is the *only* cyber defense platform with Deception capability that is built on the "inspect everything, trust nothing" operational concept. With cyber terrain awareness, network sensors that decode sessions, transmissions and content on all ports and protocols, and powerful machine-learning analytics running against rich network and endpoint metadata collected by the platform, Fidelis-enabled networks can detect, hunt, and respond to advanced threats – in real-time and retrospectively – at every step of the kill chain. Endpoint agents monitor and respond to user and machine behavior, allowing network defenders to validate integrity and respond to IOCs automatically—at cyber speed. Most uniquely, Fidelis Elevate XDR is the only solution to provide Active Defense by combining Network and Endpoint capability with industry-leading Deception technology. This changes the hunt/detect game and enables Zero Trust against the modern threat landscape: advanced, persistent attacks from adversaries.

Visibility and Control: Where is the data going

Visibility and control—the ability to see every aspect of your environment—are foundational to an effective Zero Trust Architecture. Sensors of various types must be able to monitor all data transmission avenues within and around the distributed enterprise, including cloud and all shadow IT.

Fidelis Elevate provides deep, contextual visibility and advanced cyber terrain mapping, exposing exactly where data lives and how it moves across the environment. Elevate XDR is the only XDR platform integrating mature network, endpoint, and deception capabilities to deliver holistic visibility and control across networks, endpoints, cloud, users, and applications. Fidelis cyber terrain mapping provides a detailed inventory of all IT resources (including configuration and patch levels), the architecture, and potential exposure to external influences (such as the public internet or 3rd party organizations). Fidelis is foundational to verifying that complementary access control and authentication layers are operational and effective, a cornerstone of Zero Trust Architecture.

Data Segmentation

To secure data from loss, misuse, or unauthorized access without slowing down operations, ZTAs must be able to expose the risk and value associated with unknown connections, application and data transfers and regulate access appropriately. The ability to categorize and provide least privileged access is critical to understanding who is accessing, sending, and receiving data—and exactly what types of data. Moreover, organizations must be able to validate that data is appropriately categorized at all times as it transits via the cyber terrain, and that least privileged access is in place and functioning according to organizational policies. Fidelis does this.

Fidelis Elevate implements patented Deep Session Inspection (DSI) technology that extracts and analyzes the content of documents as well as metadata at all network layers with 300+ different attributes. The content and metadata inspection provides contextual, real-time enforcement, baseline collection and

assurance that data is being protected as envisioned in the ZTA design. It is also used in retrospective detection and threat investigations when the inevitable happens. As an integrated capability of ZTA, Fidelis Data Loss Prevention DLP provides increased data visibility, protects intellectual property and mission essential data, and validates compliance at cyber speed.

Dynamic and Continuous Risk Assessment

In a ZTA, risk assessment and trust grants happen at a much more granular level. Transactions are authorized only when trust is verified (often at various levels). A key benefit of ZTA is how it institutionalizes the continual monitoring and review of the risk environment, making it fast and easy to detect changes and maintain an overview of the complete risk management process.

Fidelis Elevate continuously inspects and decodes all transactions in the architecture. It identifies seams that may have gone unnoticed or been introduced through entropy or user/change control error, analyzing down at the transaction level. This assures adherence to ZT principles with a "watch the watchers" approach. Ultimately, Fidelis provides the enterprise with a way to validate (prove or disprove) that the ZT infrastructure is working – or not – in real-time.

Dynamic Threat Hunting

For ZTA to be effective, detection and response must be transactional in nature, application aware, and able to dynamically affect the access decision. It requires continuous scanning and threat assessment, adaptation, and ongoing trust verification in communication.

The Fidelis Elevate platform integrates intelligence feeds and anomaly detection for network, endpoint and deception defenses to deliver the holistic visibility and control required of a ZTA. As a unified XDR platform, Elevate helps to shorten mean-time-to-detection as well as illuminate attacker activity living within the inevitable seams that exist during transition or are introduced unwittingly over time. Powerful machine-learning analytics running against rich network and endpoint metadata help detect, hunt, and respond to advanced threats – in real-time and retrospectively – at every step of an attack, keeping operations and data safe.

Active Defense

Proactive, predictive, and retrospective cybersecurity defense strategies are essential complements of protective and reactive defenses. They also should be an essential part of your Zero Trust Architecture.

Major attacks such as the recent attacks on SolarWinds and Microsoft Exchange clearly demonstrate how sophisticated attackers have become adept at disguising their attacks and bypassing traditional defenses. In a Zero Trust Architecture enabled by Fidelis Elevate XDR, active defense is about defeating cyber threats at any point in the cyber kill chain.

Conclusion

Zero Trust Architecture is the clear imperative that organizations must embrace for securing networks against current and evolving cyber threats. Fidelis Elevate, built on the "inspect everything, trust nothing" operational concept, provides essential capabilities for assuring that all principles of ZTA are in place, functioning, and effective.

Appendix A: Zero Trust Security Control Mapping

The table below maps the components of Fidelis Elevate and a Zero Trust architecture in alignment with NIST's Framework for Improving Critical Infrastructure Cybersecurity (v1.1).

Fidelis Cybersecurity customers can enhance their capabilities to meet sub category control requirements and adhere to Zero Trust principles by implementing Elevate features not already in use (e.g., Deception). New customers can deploy and rely upon the Fidelis Elevate Platform as an foundational part of their migration to a **Zero Trust Architecture**.

Aligning to a MITRE-based Cybersecurity Framework v1.1			
Function	Category	Sub-category	Fidelis Capability
IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-1: Physical devices and systems within the organization are inventoried.	Fidelis Network, Endpoint and Deception
		ID.AM-2: Software platforms and applications within the organization are inventoried.	Fidelis Endpoint
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.	Fidelis Network, Endpoint and Deception
	Risk Management (ID.RA)	ID.RA-1: Asset vulnerabilities are identified and documented.	Fidelis Network, Endpoint and Deception
		ID.RA-3: Threats, both internal and external, are identified and documented.	Fidelis Network, Endpoint and Deception
PROTECT (PR)	Identity Management, Authentication, and Access Control (PR.AC)	PR.AC-1 Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	Fidelis Endpoint and Fidelis Deception
		PR.AC-3 Remote access is managed.	Fidelis Endpoint and Deception
		PR.AC-4 Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	Fidelis Endpoint
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	Fidelis Network, Endpoint and Deception
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	Fidelis Deception
		PR.AC-7 Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction	Fidelis Network, Endpoint and Deception

		(e.g., individuals' security and privacy risks and other organizational risks).	
	Data Security (PR.DS)	PR.DS-2 Data in transit is protected.	Fidelis Network
		PR.DS-5: Protections against data leaks are implemented.	Fidelis Network and Deception
		PR.DS-6 Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	Fidelis Endpoint
PROTECT (PR) ***…continued***		PR.DS-8: Integrity-checking mechanisms are used to verify hardware integrity.	Fidelis Endpoint
	Information Protection Processes and Procedures (PR.IP)	PR.IP-1: A baseline configuration of IT/industrial control systems is created and maintained, incorporating security principles (e.g., concept of least functionality).	Fidelis Network and Deception
		PR.IP-3: Configuration change control processes are in place.	Fidelis Network, Endpoint and Deception
	Protective Technology (PR.PT)	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	Fidelis Network, Endpoint and Deception
		PR.PT-4: Communications and control networks are protected.	Fidelis Network and Deception
DETECT	Anomalies and Events (DE.AE)	DE.AE-2: Detected events are analyzed to understand attack targets and methods.	Fidelis Network, Endpoint and Deception
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	Fidelis Network, Endpoint and Deception
		DE.AE-5: Incident alert thresholds are established.	Fidelis Network, Endpoint and Deception
	Security Continuous Monitoring. (DE.CM)	DE.CM-1: The network is monitored to detect potential cybersecurity events.	Fidelis Network, Endpoint and Deception
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	N/A
		DE.CM-4: Malicious code is detected.	Fidelis Network, Endpoint and Deception
		DE.CM-5: Unauthorized mobile code is detected.	Fidelis Network, Endpoint and Deception
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.	Fidelis Network, Endpoint and Deception

		DE.CM-7 Monitoring for unauthorized personnel, connections, devices, and software is performed.	Fidelis Network, Endpoint and Deception
		DE.CM-8: Vulnerability scans are performed.	Fidelis Endpoint
	Detection Processes (DE.DP)	DE.DP-5: Detection processes are continuously improved.	Fidelis Network, Endpoint and Deception
RESPOND	Mitigation (RS.MI)	RS.MI-1: Incidents are contained.	Fidelis Network, Endpoint and Deception
		RS.MI-2: Incidents are mitigated.	Fidelis Network, Endpoint and Deception