Fidelis Cybersecurity

WHITE PAPER

Trusting Your Zero Trust Architecture

Learn why Active XDR from Fidelis Cybersecurity® is an essential foundational element of a Zero Trust Architecture

Fidelis Cybersecurity

Table of Contents

What Is Zero Trust?

An imperative

The accelerated move to the cloud, increased use of BYOD, IoT and shadow IT, and an abrupt shift to working from home have exponentially complicated the IT security landscape. Cybersecurity professionals must provide secure access to company resources from any location and asset, protected interactions with business partners, and shield client-server and inter-server communications from malicious or unauthorized usage.

At the same time, adversaries are more sophisticated and targeted in their approach. As a result, they are infiltrating deeper, dwelling longer, imposing an incalculable cost, and doing significantly more damage.

As organizations look to defend increasingly complex IT environments against more sophisticated threat actors, the concept of a Zero Trust Architecture (ZTA) is growing in prominence and prevalence. Several high-profile cyber intrusion events involving the software supply in 2020 led NSA and DISA to issue guidance specifically recommending that US government organizations and their industry partners implement ZTA to combat active threats to systems and data. The White House recently issued similar guidance.

Zero Trust architectures protect critical assets (data) in real-time within modern, dynamic threat environments by fortifying data access controls. This architectural approach is built on the assumption that an intruder may already be on the network. Specifically, Zero Trust takes the position that every person, place, or thing accessing the network and services is untrustworthy until proven otherwise. The strategy assumes every access request is an attempted breach. Zero Trust requires explicit verification of the security status of identity, as well as proof of authorization for access to endpoints, networks, applications, and other resources, based on all available signals and data, including potential risk. And, once trusted access is established, a Zero Trust Architecture continues to verify to safeguard data, systems and services by continuous and pervasive visibility and monitoring coupled with detection and response to threats. Implemented properly, ZTA can help reduce breach risk and speed detection times, ease compliance auditing, and better protect company data.

To accomplish the goals of ZTA, trust is granted at a much more granular level than in traditional access architectures. Transactions, including direct user and programmatic authorization and access requests, are allowed to proceed only after identity and authorization is verified, and verification happens repeatedly. ZTA tactically employs continuous monitoring and review of the risk environment by implementing multiple access control points and authorization challenges beyond session initialization. This re-verification process helps detect changes in the context of each request and maintains a running risk analysis throughout each access session. This is where Fidelis Cybersecurity can really help.

Get Started

Zero Trust's appeal lies in its ability to keep pace with continually evolving threats and risks. Therefore, ZTA has become a digital transformation imperative across companies of all sizes, and from every industry. Whether you implement ZTA alongside a new project or take a critical-projects-first perspective, overlaying identity and authentication enforcement alone does not lead to a secure Zero Trust-based IT ecosystem.

To capitalize on the full benefits of ZTA, you must have exceptional visibility and control, enterprise-wide. You also need sensors in the path of all avenues in and out of your enterprise — including endpoint, cloud, and all shadow IT. A comprehensive ZTA strategy ensures that new and evolving systems and workloads are inventoried, interrogated, and validated against your security standards. A comprehensive, enterprise-wide ZTA also includes continuous risk assessment, dynamic threat monitoring, comprehensive data governance, and a proactive cyber defense strategy that keeps you ahead of the threat.

Zero Trust in Action

In today's agile, fast-moving, widely distributed, and ephemeral environments, including multi-cloud and containerized data management and application environments, the continuous nature of access monitoring employed by ZTA is a critical component of threat management. New and emerging threats take advantage of modern infra-structures that aren't protected by Zero Trust controls. Some of the common threat scenarios that ZTA helps secure include:

Insider Threats: Traditional identity and access management strategies operate on the idea of least privilege access, where a user who is authenticated inside the firewall is generally considered safe. However, the biggest threat to cybersecurity is your employees. Nearly 70% of enterprises state that they are worried about an inside cyberattack. ZTA handles the insider threat by continually verifying a user's access to the system and challenging each request to data and applications to ensure roles and authorization.

Data Loss Prevention (DLP): As more data is stored in the cloud and on endpoint devices, and data growth compounds exponentially, companies need effective strategies for monitoring data at rest, in use, and in transit, along with handling requests that come from both within and outside the corporate firewall. When it comes to detecting data loss, suspicious user behaviors and anomalous access patterns are your primary indicators of threat. An effective ZTA strategy monitors each data access request, even after a user or process has been authenticated, and tracks usage patterns, so anomalies are detected in real-time. With actionable threat- and behavior-based analytics, you can detect attacks earlier in the attack lifecycle with greater confidence.

Changing Risks: Cyber threats are a constantly evolving and shifting landscape, and your ZTA needs to be flexible enough to handle changing risks. Malware, vulnerabilities, phishing attempts, and more add new elements and adversaries that need to be detected, caught, managed, and eradicated before they can damage your environment or steal your data or IP. Stopping outside or anomalous attacks are only half of the strategy; ZTA must also account for viruses and phishing attacks that take advantage of the users and accounts that have trusted and verified access to your data and applications. In these cases, it's imperative that you have automated detection of suspicious activity that alerts your SOC or system owners as it happens.

Neutralize Threats with Fidelis Cybersecurity

Full situational awareness
Gain continuous, contextual visibility.

Proactive cyber defense
Engage earlier in the attack lifecycle.

Dynamic threat monitoring
Detect and respond at line speed.

Threat-focused analytics
Identify and correlate events and their context.

Asset risk analysis
Understand the risk of an asset and user before and after trusting access.

Fidelis Cybersecurity & Zero Trust

Fidelis Elevate® is an eXtended Detection and Response (XDR) platform that aligns with the NIST framework in SP 800-207 and enables the rapid transition of enterprise infrastructure to Zero Trust principles. Fidelis Elevate is the only active cyber-defense platform that integrates Deception technologies with detection and response on endpoint, network and cloud to change the hunt/detect game and defend against modern, advanced persistent attacks from adversaries. The integrated deception technologies in this Active XDR platform enable SOC teams to continually tune defenses and neutralize threats before they can cause damage to business operations. These capabilities are critical in the Zero Trust architecture to enable monitoring and compliance functions. One of the tenets of a Zero Trust Architecture is 'Never Trust, Always Verify.' Fidelis Cybersecurity provides the verification of the Zero Trust access enforcement itself to make sure that the Zero Trust controls are working as designed and not compromised by misconfiguration, exploits, advanced attackers or insider threats.

Additionally, Fidelis CloudPassage Halo® provides continuous compliance for cloud administrative accounts, enforcing ZTA best practices in dynamic, containerized and highly agile cloud environments. Fidelis Halo monitors for weak passwords, disabled multi-factor authentication, overly permissive administrative accounts, stale accounts, and more, keeping the cloud perimeter secured at the administrative account level. As new cloud accounts come online in an environment, Fidelis Halo automatically detects and alerts on violations to the ZTA configuration standards and can automatically disable accounts until they are made secure by the SOC team.

Enterprise-wide visibility

Fidelis provides continuous, real-time visibility through an integrated security stack across and within endpoints, networks, users and cloud assets, accounts, and workloads. Fidelis Elevate features deep, contextual visibility and advanced cyber terrain mapping to show exactly where data lives and how it moves across your environment. This continuous attack surface mapping provides a detailed real-time inventory of your IT resources, including configuration and patch levels. It also details the architecture and potential exposure to external influences, such as the public internet or 3rd party organizations. Fidelis solutions complement IAM solutions with verification of access controls and identifying circumvention as well as trusted insider threats. The visibility Fidelis Cybersecurity provides play an essential role in realizing a Zero Trust Architecture.

Continuous risk assessment

Fidelis Elevate ensures user and asset risk verification is done continuously to identify coverage gaps that may have gone unnoticed or that are introduced through entropy, configuration changes, or access control errors introduced in the environment. Fidelis Elevate assures adherence to Zero Trust principles by enabling a "watch the watchers" approach that repeatedly inspects and decodes all user access requests in the architecture. Additionally, Fidelis employs log-based intrusion detection and multiple layers of threat management for focused analytics that help identify and correlate suspicious and anomalous events and provide context surrounding the events. Ultimately, Fidelis provides an enterprise with a way to validate that the Zero Trust infrastructure is working—or not—at real-time cyber speed.

Fidelis Halo offers an additional layer of protection with continual log-based intrusion detection and file integrity monitoring, configuration monitoring, and vulnerability management. By watching access points and assets, security teams can protect IT infrastructure from end-to-end while providing actionable intelligence for the SOC.

Transactional monitoring

Fidelis Elevate enables security teams to monitor all ports and all protocols from the network up to the application level. It allows users to monitor individual connections and transactions, decode the contents of the transaction up to the application level, and filter or block a transaction if the contents of the transaction violate network policy. For example, in traditional environments, email transactions are not well covered—users can download and send any attachment they want. If the content of an email violates DLP policy, Fidelis can block sending the email.

Dynamic threat monitoring

The Fidelis Elevate platform integrates intelligence feeds and anomaly detection for network, endpoint, and deception defenses to deliver holistic visibility and control. This unified active XDR platform helps shorten mean-time-to-detection and discovery of an attacker living within inevitable seams that exist during transition or 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 business operations and data safe.

Data governance

Fidelis Elevate adds controls for Data Loss Prevention that are part of the Data Governance function in the Zero Trust Architecture to help protect data from loss, misuse, or unauthorized access. With Fidelis Elevate, you protect data without slowing down business operation by harnessing insights from each data access request and understanding the risk and value associated with each. You'll gain a greater understanding of who is accessing, sending, and receiving data, and what types of data each user is accessing. With both user access patterns and threat-based analytics, you can better ensure least-privilege access, secure data transfers, and detect many indicators of data loss, including unauthorized access, exfiltration, and unintended or negligent data exposure.

Proactive Cyber Defense

As evidenced by major attacks, such as those on SolarWinds and Microsoft Exchange, sophisticated adversaries are adept at disguising attacks and bypassing traditional defenses. A proactive cyber defense strategy, including proactive, predictive, and retrospective cybersecurity functions, have a better chance of keeping up with emerging and evolving threats. A Zero Trust Architecture fortified by Fidelis Elevate, proactively shifts users to an active defense where they can detect and respond to cyber threats earlier in the attack lifecycle and before significant damage can be done.

Zero Trust architectures are critical to better safeguarding your environment. Fidelis solutions (including Fidelis Elevate and Fidelis Halo) are essential foundational elements of any Zero Trust Architecture.

Learn more about Fidelis Cybersecurity

Fidelis Elevate Bolsters your Zero Trust Architecture in Three Ways

Predictive Defense

- Identify interesting events and activities to help focus and direct threat hunter activities where they should be looking. Threat intelligence keeps these threat hunters and automated attack detection rule sets current.
- At the same time, frameworks like MITRE ATT&CK help analysts string together seemingly random events and put them in the context of a broader attack campaign.

Proactive Defense

- Adding smart Deception in your environment with decoy assets and users.
- Gaining pervasive and continuous visibility on your terrain with identification and tracking of assets as well as assessment of risk on the terrain.
- Enabling threat hunting within your environment through the lens of an attacker — to detect, investigate, analyze, mitigate, and track anomalous activity for threats that might have breached perimeter defense.

Retrospective Analysis

- Apply threat intelligence based on newly identified threats against historical metadata—automatically and continuously to flag a past compromise. Security analysts can then apply proactive defense and response techniques to eradicate the attacker.

About Fidelis Cybersecurity

Fidelis Cybersecurity, the industry innovator in proactive cyber defense solutions, safeguards modern IT environments with unparalleled detection, deception, response, cloud security, and compliance capabilities. We offer full visibility across hybrid environments via deep, dynamic visibility and asset discovery, multi-faceted context and risk assessment. These features help minimize attackable surface areas, automate exposure prevention, threat detection, and incident response, and provide the context, accuracy, speed, and portability security professionals need to find and neutralize adversaries earlier in the attack lifecycle. With Fidelis, organizations emerge stronger and more secure. Fidelis is trusted by many top commercial, enterprise, and government agencies worldwide. For more information, please visit **www.fidelissecurity.com**

Fidelis Cybersecurity