FORENSIC INVESTIGATIONS IN ZERO TRUST ENVIRONMENTS

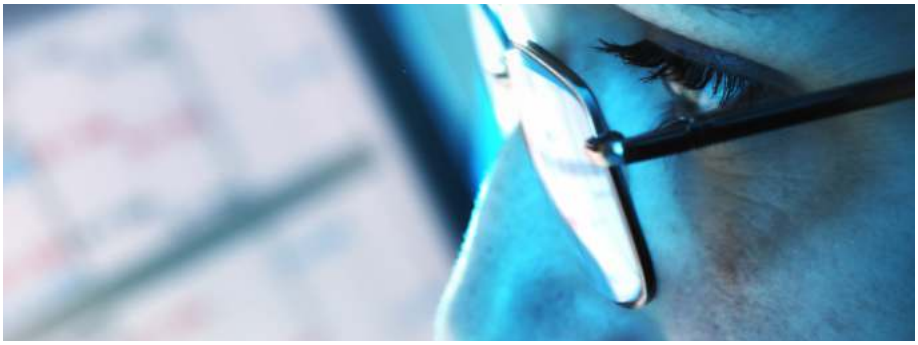
exterro®

Introduction

On January 26, 2022, the Office of Management and Budget issued a memo titled, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, articulating a major change in the federal government's cybersecurity posture. By September 2024, all government agencies and any organizations doing business with government agencies **must implement or have made significant progress toward implementing zero trust architecture**.

It's very clear that the need to upgrade the government's cybersecurity posture is pressing. After all, the federal government wouldn't undertake such a major technology initiative on a 16-month timeline unless the situation was very serious. And it is. The cyberthreat landscape is increasingly treacherous. As President Biden stated in his executive order, Improving the Nation's Cybersecurity, "Incremental improvements will not give us the security we need; instead, the federal government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life."

But while the government must take every measure possible to protect infrastructure, national security, and the economy, **other organizations in the public and private sectors are facing the same threats** and must act accordingly. It's understandable that zero trust concepts may not feel clear-cut, even to tech-savvy business and public sector leaders. The term is relatively new, and its rapid rise to buzzword status may obscure some of the key ideas involved.



What exactly is zero trust architecture? How should organizations consider implementing it? What are its implications for organizations' broader cybersecurity infrastructure? How can they conduct digital forensic investigations in zero trust environments? This whitepaper explains these concepts and offers practical advice for digital forensic professionals looking to conduct investigations in zero trust environments.

Table of Contents

Why Zero Trust?

Historically, organizations secured their IT infrastructure and data by creating and hardening a perimeter. Organizational assets, including networks, software, and data storage resided inside the perimeter, in terms of both the physical and cyber-environments. Think of ID cards or keys to enter the office, servers stored inside secure rooms with limited access, and on-premises data and applications secured behind firewalls.

If you think about corporate information architecture today, data is stored on servers, cloud data storage, on personal devices, and in SaaS software solutions. Applications too exist in multiple places: on network servers and smartphones, on laptops and in the cloud. Workers log in from offices, home, through mobile devices, and even from wi-fi networks in a local coffee shop. Threats to security arise from outside the organization—and within—in the form of bad actors, phishing attacks, and malware-infected devices. Securing the perimeter no longer protects an organization from cyberthreats.

Zero trust architecture has arisen as a response to today's de-perimeterized networks. Zero trust security exists in the form of policies as much as, if not more than, technology. It brings a mindset of continual vigilance, validation, and verification to organizations' information infrastructure, helping them minimize the risk and impact of cybersecurity threats, wherever they may originate.

What Zero Trust Is—And Isn't

"The foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted. Instead, we must verify anything and everything attempting to establish access."

- Department of Defense (DoD)
Zero Trust Reference Architecture

To understand what zero trust is, it's useful first to be clear about what it is not. **Zero trust is not**:

IS NOT **A technology or software solution**

IS NOT **A service or product you can buy**

IS NOT **A strict, highly defined network architecture**

IS NOT **Something you can "set and forget"**

Zero trust is a cybersecurity paradigm or framework, akin to a thought process. It includes technology components, but also includes policies deployed with the goal of keeping organizations' data secure by tightly regulating access to it. The zero trust mindset requires organizations, their cybersecurity professionals, and technology infrastructure to adopt a posture of constant visibility, monitoring, and auditing of its data, hardware, applications, and users.

Why Zero Trust?

Today, many elements of organizations' networks exist outside the traditional perimeter:

- → SaaS applications across multiple disciplines
- → Fileshares and off-network storage
- → Hardware endpoints
- → Users including employees, contractors, partners, and clients

Zero Trust protects all of these network nodes, in part by limiting access to the minimum amount of data or resources necessary to perform its (or their) function. Every user, process, or action taking place on a network must be authenticated, authorized, and validated. For example, users may have a company issued laptop, but lack administrative privileges to add or remove software, or they may have access to certain fileshares, but not others. This segmentation of users, applications, and devices helps minimize the risk of cross-contamination by cybersecurity threats.

Components of Zero Trust

While the federal government's definition of a zero trust environment is not definitive, as there is no single standard or accreditation, it covers the fundamentals in the following five components that agencies must implement by the end of fiscal 2024.

- → **Identity:** Enterprise-wide tracking identifies who is doing what and where, manages permissions, and includes phishing-resistant multi-factor authentication.
- → **Applications:** All applications must be considered internet-connected, routinely audited, and kept up-to-date with external vulnerability analysis and reporting recommendations.
- → **Data:** The protection of data is the primary objective, requiring visibility into, monitoring of, and reporting on data. Agencies should log, analyze, and share learnings from data incidents.
- → **Devices:** Conduct a complete and accurate inventory of all devices, then ensure the ability to prevent, detect, and respond to incidents on all devices, includes BYOD.
- → **Networks:** Encrypt all DNS, HTTP, and email services within the organization and segment infrastructure into isolated environments to reduce potential for cross-contamination.

Conducting Forensic Investigations in Zero Trust Environments

With the need to detect and respond to incidents on all devices and to log, analyze, and share learnings from these incidents, digital forensic technology is a must to maintaining a zero trust environment in compliance with the federal mandate—or simply to follow best practices for securing organizational data and assets. This means that a forensic solution must be able to:

- → Have admin access across the network
- → Deploy agents to remote devices
- → Maintain an inventory of all devices—and the ability to respond to incidents on these devices
- → Operate across platforms including Mac, Windows, and Linux
- → Image and collect data forensically across an encrypted connection
- → Remediate incidents by deleting files, closing ports, or potentially deactivating users
- → Preview endpoints to analyze files in use, programs running, and connected services in real time

FTK® Enterprise Public Site Server

FTK's public site server facilitates IT departments' ability to respond to security incidents on all devices, whether they are on the local network or remote. It resides in a secured environment on your network, and agents deployed on monitored devices can communicate with the public site server anytime they are connected to the internet.

Through instructions deployed on the public site server, remote agents can perform critical incident logging, analysis, and remediation tasks including (but not limited to):

- → Scanning, analyzing, or deleting files
- → Collecting from memory
- → Collecting forensic images
- → Closing ports
- → Deactivating users

Even if devices are not connected to a virtual network or an internal network, the **FTK** public site server allows IT to communicate with devices, and in the event of a breach or an incident, perform the necessary actions to secure that device, secure the network, and abide by the zero trust mandate. If a device is not online, administrators can queue a job on the server, and as soon as it reconnects to the internet, the server will deploy the job to the agent and perform the necessary actions.

Gain deep visibility into endpoint data to investigate a breach or employee wrongdoing

LEARN MORE

Conducting Forensic Investigations in Zero Trust Environments - *continued*

The need for forensic investigators to have full admin access to conduct investigations appears to conflict with the zero trust requirement to limit users, devices, and applications to the minimum necessary to perform their functions. The other standard business applications a forensic investigator has on his or her device, which must be treated as internet connected, would pose unnecessary security risks, obliging organizations to provide forensic investigators with two devices—one with full privileges for forensic review, another for all other business functions. Given the cost, such a solution is unlikely to be embraced. The alternative, therefore, is a forensic solution with the capabilities to conduct secure forensic review in a non-installed review platform.

FTK® Central and Portable Case

With an on-premise installation of **FTK Central**, all forensic information can be secured on a server controlled by IT, while forensic reviewers complete their tasks in a web browser interface. Additional experts involved in an investigation—for example, HR or financial specialists, can review relevant elements of the case without needing administrative access or a dedicated forensic device. **FTK Central** allows teams to sidestep the extensive software lockdowns required to minimize non-authorized access in zero trust environments.

Similarly, **Portable Case** allows investigators to use a self-contained review platform that connects with the primary case stored in **FTK**. It can be loaded on a USB jump drive or to the cloud, complete with the relevant data to be reviewed. Then the reviewer can access the application from its self-contained directory with no installation necessary. Once they've reviewed the data and provided their input, the principal investigator can sync the information back with the primary case.

Key Takeaways

Zero trust is a concept whose time has arrived. Even without the force of a federal government mandate behind it, more and more organizations are recognizing the security benefits posed by adopting the technology, policies, and mindset of continuous vigilance and validation.

Complying with the requirements of the federal mandate demands organizations to have digital forensic capabilities, such as remote device analysis and remediation. But some of these capabilities—namely the need to have wide-ranging device access—seemingly conflict with the principles of zero trust.

Advanced digital forensic solutions in the **Exterro FTK®** family provide forensic investigators with key capabilities in ways that align with zero trust environments. Key features like Public Site Server and Portable Case allow investigators to conduct their activities securely in compliance with the federal zero trust mandate and best practices for cybersecurity and digital forensics.