FORTRA

Zero Trust and the Seven Tenets

Peer Advice

Whether you are new to information security, or you're a long-time practitioner, it seems that "zero trust" is the latest initiative at the top of everyone's priority list.

This is a positive move in the InfoSec world, as many components of the zero trust approach have been implemented individually for many years but lacked overall unity as part of a holistic plan. It's encouraging that these security drivers are now collated into a formal document.

Special Publication 800-207, created by the National Institute of Standards and Technology (NIST) offers guidance for instituting a zero trust architecture. The document outlines the basic tenets that form the foundation of zero trust. For some organisations, however, the tenets of NIST 800-207 seem overwhelming.

This guide is designed to make these tenets more tangible—to ground them in practical application, enabling your organisation to take small, yet action-orientated steps towards achieving this important goal.

TENET 1

Everything is Included

All data sources and computing services are considered resources

WHY IS THIS TENET IMPORTANT?

"All data sources and computer resources, and all computer change services are resources. You need to transact data from these resources, as well as from all of the data sources irrespective of the kind of data you are exchanging or processing. **Access to any of this data by the wrong people could ultimately place your organisation at risk.**"

» **Mosopefoluwa Amao**
Cybersecurity Analyst

REAL-WORLD CHALLENGES

"**Remote work is challenging** because personal devices may not be classified as enterprise-owned resources. This could be potentially risky within the organisation because employees should not use their personal devices to access enterprise resources."

ADVICE FOR IMPLEMENTATION

"Organisations should consider, first of all, all of the data sources that are deployed either on premises or in the cloud. Organisations need to make sure that they have an inventory of all of these data sources, and they need to consider the kind of data that is being collected. They should ensure the system logs are properly monitored and reviewed. This way if anything is out of place, they can always identify it.

Organisations need to prioritize security, and they need to understand that irrespective of the device, **if it is being used to access organisational resources it must be protected.** If they're not protected, then they could potentially hurt the company."

TENET 2

Secure All Communication

All communication is secured regardless of network location

WHY IS THIS TENET IMPORTANT?

"The advice to secure all communication is an attempt to align a lifecycle management process **to adopt secure communications across all the layers of the network infrastructure.** Many organisations put a lot of time, effort, money, training, and technology into being compliant, but they are still getting breached. It's because all of the tools, and all of the effort has been focused on maintaining a minimum standard of compliance, rather than looking at the root cause of most data breaches. It's the result of absent identity and access management, poor IT service management, unpatched infrastructure, and even sometimes, insider threat."

» **Ian Thornton-Trump**
CISO

REAL-WORLD CHALLENGES

"The problem is that, for most organisations, the cost and the skill set required for a complete solution is mind-boggling. There is no single blinky box that can do this.

You can have all the encryption you desire between endpoints and web applications, but if you are still using old communication tools such as telnet, and you're still using unsecured protocols in order to manage printers within your infrastructure, you're failing.

There need to be policies to support this ideal, the ability to identify the things that are in violation of those policies, and plans that are consistent with the business to commit to these goals."

ADVICE FOR IMPLEMENTATION

"Finding out what is on your network is easy now using the technologies that we have. All you need to do is collect a bunch of network traffic, break it out by protocol, and trace which devices are using insecure protocols. Once you've eliminated all the bad protocols, you can move on towards identifying unencrypted traffic, or inadequately encrypted traffic. With all of the remote endpoints on the networks, this can become a monumental task, so **it's important to work incrementally to get to the end result.** Three components of zero trust that are super important are visibility, automation, and orchestration. Those need to be done in order."

TENET 3

Session-Only Access

Access to individual enterprise resources is granted on a per-session basis

WHY IS THIS TENET IMPORTANT?

"By granting access on a per-session basis, we make an attacker's life much harder. What we've witnessed several times in practice, are developers' workarounds bypassing the actual security needs, yet meeting compliance with "misinterpreted" security requirements. **With a per-session authorisation, we ensure that both the authentication and actual flow channels go side-by-side**, together all the way. Bypass of the initial authentication (or key verification) won't work, as this needs to be performed for every session, which is practically infeasible in a per-session structure."

» **Lefteris Tzelepis**
IT Security Director

REAL-WORLD CHALLENGES

"Lacking a central identity access management (IAM) system is an apparent roadblock. This is something that may require prior consideration. There could be resources within the systems that do not require authentication, and several functions may already be built upon this assumption or setup. Moreover, this is not always supported by legacy applications, or cumbersome architecture schemes.

Something we should never underestimate is people's tendency to reject change, especially a change deriving from security. **This tenet, being tied up with a "shift-left" approach, introduces change into the way applications are built."**

ADVICE FOR IMPLEMENTATION

"First of all, the teams responsible for such implementations need to have a good idea of the value behind this; **developers' security training is a key to success.**

Confirmation of proper implementation should also be considered, along with regular and proper checkpoints, especially for transactions referring to critical assets.

Last, consider the fact that this does not solely bring our IT environment to a zero trust ready state. It should be part of a bigger change or **accompanied with a holistic approach towards zero trust transformation.**"

TENET 4

Dynamic Policy-Led Access

Access to resources is determined by dynamic policy

WHY IS THIS TENET IMPORTANT?

"Dynamic policies are a way of defining and enforcing authorisation rules that can change over time. This is important because it allows us to constantly adapt our security posture to the ever-evolving threat landscape. These policies are a vital part of the zero trust security model because they aim to grant access to resources based on the continual verification of identities, devices, and access to services. The ultimate goal of zero trust is better security by not trusting any user implicitly and reducing the risk of breaches. By tying access to resources with dynamic policies, we can ensure that only authorized users have access to the data and systems they need."

» **Christina Morillo**
Principle Security Consultant

REAL-WORLD CHALLENGES

"A few key challenges include:

Complexity: With the size and complexity of the environment, it can be challenging to establish all of the necessary policies.

Lack of Visibility: It can be difficult to properly enforce policies without proper visibility into who is accessing what resources.

False Positives: If policies are not well designed, they can result in false positives, leading to service disruptions.

As with any security solution, there may be a trade-off between security and convenience. Therefore, it is important to strike a balance between security and convenience when designing the authorisation process.

ADVICE FOR IMPLEMENTATION

"When implementing dynamic policy-based access control, I advise starting with the understanding that zero trust is not a single solution or application. While there may be solutions enabling these principles, there is no one solution that provides zero trust.

Once you've figured out what matters most to the business, you'll better understand the appropriate use cases and granular access requirements, which will inform your tools and implementation approach."

TENET 5

Integrity Controls

The enterprise monitors & measures the integrity & security posture of all owned & associated assets

WHY IS THIS TENET IMPORTANT?

"The concept of security and integrity being a known state for all assets is important in a world where a security breach can start anywhere. If zero trust isn't implemented, a compromised laptop connecting to the corporate VPN, an old printer running insecure firmware, or a cloud-hosted server not spotted by traditional discovery tools all have the potential to be the point of weakness that an attacker can exploit before moving across the organisation. **Failure to identify the "who" and the "what" to monitor is a common failure** of the traditional security model. That is why the zero trust approach to assuming you are at risk until you can confirm otherwise makes discovery and monitoring a key aspect to ensure your systems' integrity."

» **Chris Hudson**
Professional Services Technical Architect

REAL-WORLD CHALLENGES

"The reality of monitoring and securing all assets is a long journey that requires continuous nudges to keep your strategy on track. Discovery and monitoring presents challenges around gap analysis (how do you know what you're missing when your discovery tool fails to find something), whilst monitoring requires careful consideration about what is "useful" information versus "noisy data."

A move away from traditional security alerts and responses, as well as providing continuous monitoring can also present new complexities for security teams' responses and can result in some **significant changes to day-to-day security operations that need to be carefully planned out."**

ADVICE FOR IMPLEMENTATION

"I highly recommend approaching this with a 'discovery stage' that you can regularly revisit during your zero trust project. Successful strategies to address this tenet require that you assess your successes and weaknesses as new information is discovered about your network and your approach.

From a practical perspective, **identify how you want to classify your monitoring and security information from the outset so that you may gradually ratchet up your trust levels over time** based upon well-established and understood schemas for your security information. This information must include data around ownership and risk, which can significantly reduce the burden to provide categorisation later on."

TENET 6

Authentication & Authorisation

All resource authentications and authorisations are dynamic & strictly enforced before access is allowed

WHY IS THIS TENET IMPORTANT?

"The concept of "securing the perimeter" has morphed into "securing the resource." Man-in-the-middle (MitM), or on-path attacks can be all too easy to accomplish. Multi-factor authentication (MFA), with all its virtues, can potentially be bypassed by tactics such as capturing a token or using real-time phishing. Similarly, auth tokens can be captured. This is all compounded because people can work from anywhere, presenting more opportunities for impersonation. **For zero trust to remain true to its model, nothing is trusted, and everything is verified."**

» **Ross Moore**
Cybersecurity Analyst & Writer

REAL-WORLD CHALLENGES

"The big challenge is the allocation of resources. Resources include people, training, the right technologies and devices, and time to implement and maintain—it's not all about finances. Even if each of these was obtained, having a coherent and cohesive approach to company-wide deployed and managed authentication mechanisms is a major obstacle.

If all stakeholders don't take the time to **align their plans and projects with each other,** then there's a motley assortment of solutions, leading to interoperability issues, and ending up with bad security, which is further away from a zero trust architecture than if advancements had not been made at all."

ADVICE FOR IMPLEMENTATION

"Security needs to be positioned as a cost preventer. All the authentication/authorisation controls need to be reasonable, but they're also there to prevent breaches, as well as regulatory, and legal sanctions. **This can be accomplished with a short-, mid-, and long-term roadmap.**

Think of what needs to happen first and second, then build on that when it happens, and keep track of your progress so you can look back in a few years and see how much progress you really made."

TENET 7

State of Assets

The enterprise collects as much information as possible about the current state of assets

WHY IS THIS TENET IMPORTANT?

"This tenet is important because **cyberattacks are becoming more sophisticated, networks are increasing in size and complexity, and businesses are continually looking to be 'agile' and responsive to customer requests.** By implementing a zero trust architecture, we start from a foundation where everything must be questioned and verified. This requires organisations to think more thoroughly about why they need to do what they do. The tenet isn't an inhibitor to business, but it is an inquisitor to the business. For far too long organisations have developed platforms and infrastructures without any in depth analysis of the security required. Zero trust forces this conversation."

» **Gary Hibberd**
Professor of Communicating Cyber

REAL-WORLD CHALLENGES

"As with most things, **the challenge is always resistance to change.** This is why it's so important to articulate clearly the benefits of zero trust. This needs to be discussed in ways the business understands and benefits from.

Additionally, of course, the challenge will be more considerable based on the size and complexity of the infrastructure in place. But again, understanding why you are doing something will help set the scope for the change."

ADVICE FOR IMPLEMENTATION

"Showing the small wins and bringing people along on the journey will ensure the adoption of this tenet. We would do well to remember that businesses move at the speed of trust, and therefore zero trust seems counter-intuitive. Its very name conjures up thoughts that we are not trusted.

It is important to consider the current approach to architecture development and design, be clear about what zero trust means, and explain it to the business. Everything must start with a clear understanding of the objectives and benefits of zero trust, or you run the risk of alienating the very people you seek to protect."

NEXT STEPS

What is the Current State of Your Organisation's Zero Trust Program?

One of the most important elements to understanding your progress along the zero trust journey is to assess your current standing, and then make forward steps to further strengthen zero trust.

To help you get started, take our self-assessment quiz. You will then automatically get a personalised report about your current bearing, with tailored advice on next steps.

Zero trust is not only necessary for better security, it is also attainable with the right partner to help you along the way.

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-tw-gd-1222-r1-hm