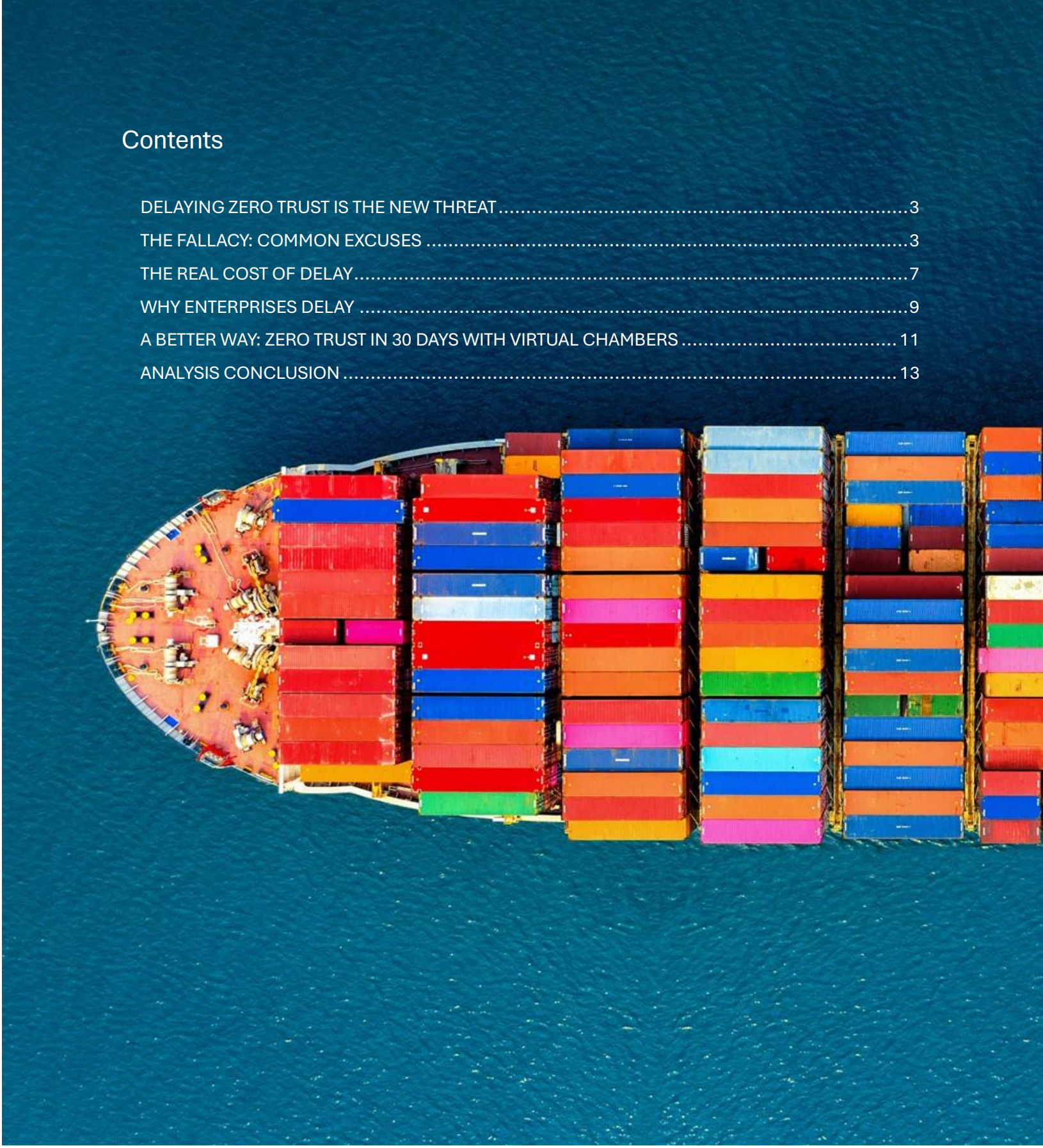
The Cost of Delaying Zero Trust

How Risk Compounds Faster Than Traditional Defenses Can Contain It

Contents



DELAYING ZERO TRUST IS THE NEW THREAT

The era of delaying Zero Trust cybersecurity is over. In 2025, delay isn't caution - it's negligence dressed up as strategy. With attack paths compounding faster than traditional defenses can contain them, businesses cannot afford to put off implementing this critical security infrastructure. Infrastructure operators increasingly face escalating regulatory pressure, tightening insurance requirements, growing reliance on remote access and vendor connections, AI-powered threats eroding time advantage, and growing board-level expectations for segmentation. Every quarter postponed worsens risk exposure and inflates the eventual cost of remediation. The silent culprit is no longer technology – it is delay! Businesses can no longer afford to continue to delay Zero Trust.

This report explains:

- The fallacy of delay excuses
- Technology hurdles causing delay
- The real cost of delay
- Why traditional segmentation cannot keep up
- A better way: Zero Trust in 30 days with Zentera Virtual Chambers

The bottom line is for you to learn the compounding costs of delay and know how to implement Zero Trust to fend off growing threats.

THE FALLACY: COMMON EXCUSES

Executives rarely delay Zero Trust because they disagree with its principles. They delay because they misjudge the true risk curve. This misjudgment creates an accepted narrative to justify years of inaction. Statements like "We're not a target", "We have segmentation", "We'll prioritize Zero Trust next quarter", and "Budgets are tight this year" have created an acceptance of status quo. The uncomfortable truth: the status quo is degradation against threats. Let's look deeper at each of these excuses.

Recent breaches help illustrate the level at which all businesses are at risk. Each of these businesses may have felt that their risk was lessened using one of the major excuses. Each suffered significant costs and impacts that would have been dramatically reduced with Zero Trust controls in place.

Recent Cases & Impacts

Case (Breach Date)	Impact Details	Cost	Security Failure

UNFI (2025)	• Weeks-long food supply chain disruption
	• Nationwide grocery shortages
	• Perishable goods spoilage
		$400 Million	• **VLANs Failed**
			  ○ Broad VLAN scopes (100s of servers per VLAN)
			  ○ Flat L2 connectivity
			  ○ No dynamic policy enforcements
			• **Firewalls Failed**
			  ○ Perimeter-only focused firewalls
			  ○ No east-west filtering
			  ○ Stateful rules bypassed via trusted flows
			• **Traditional microsegmentation Failed**
			  ○ Static ACLs didn't adapt
			  ○ Manual rule management
			  ○ No application-layer visibility

MGM (2023)	• Operational breakdown
	• Casino systems offline 10+ days
	• Slot machines disabled
	• Hotel systems down
		$100 Million	• **Microsoft Exchange Failed**
			  ○ Legacy on-prem exchange
			  ○ Missing modern authentication
			  ○ Weak Multi-factor authentication bypass
			• **Firewall Failed**
			  ○ Allowing internal trust
			  ○ No identity-aware filtering
			  ○ Service account exceptions
			• **VLANs Failed**
			  ○ Shared VLANs across business units
			  ○ No workload isolation

Change Healthcare (2024)	• National healthcare payment chaos
	• 15 billion+ transactions disrupted
	• Pharmacy payment failures
		$872 Million	• **Compromised Microsoft Exchange account**
			  ○ Remote PowerShell access
			  ○ No session timeout enforcement
			• **Traditional microsegmentation failed**
			  ○ Coarse-grained policies
			  ○ Service-to-Service trust
			  ○ No continuous validation
			• **Firewalls failed**
			  ○ Allowed RDP/WinRM internally
			  ○ No application context
			  ○ Encrypted traffic blind spots

Table 1: Example of Recent Cyber Attacks

We're not a target

Nearly 3 decades ago, a technology colleague uttered the words, "I use security through obscurity." Although later he was hacked, his belief holds true to human nature. As people, we commonly undervalue our own risk while elevating others' risk. Simply put: The other person's risk is greater than mine, or they are a greater target than I. The problem with this mindset is that it is simply untrue. All businesses are targets.

The limited examples above demonstrate similarities across completely different industries. Industries ranging from food suppliers to healthcare. In addition to these, multiple U.S. water utilities, such as Oldsmar, Florida, Water Treatment Plant, manufacturing plants, hospitals, and regional grids, have all faced breach incidents in recent years. The simple truth is that everyone is a target.

We have segmentation

Segmentation often creates an illusion of safety. Most environments claiming segmentation rely on VLANs, broad firewall zones, legacy microsegmentation, and ad-hoc exceptions that accumulate over time. These controls look like segmentation on paper, but in practice ,they leave large lateral-movement gaps.

VLANs failed in all three cases.
UNFI, MGM, and Change Healthcare each operated with hundreds of hosts per VLAN due to the difficulty of managing granular network segmentation. This flat Layer 2 design allowed attackers to pivot freely, broadcast internally, and expand the breach before detection. VLANs did not contain anything - they amplified the blast radius.

Firewalls failed for similar reasons.
Once attackers passed the perimeter, firewalls offered little to no east-west protection. Identity-blind rules, trusted internal flows, slow manual updates, and inevitable policy drift all left gaps that attackers exploited. Firewalls were never built for granular, dynamic Zero Trust and cannot keep pace with environmental growth.

Legacy microsegmentation also broke down.
Tools like NSX rely on static ACLs and manual operations. As environments evolve, rulesets fall out of sync, exceptions pile up, and coarse service-trust relationships remain in place. At UNFI and Change Healthcare, these gaps contributed directly to large outages.

Across all three examples, organizations believed their VLANs, firewalls, and legacy microsegmentation kept them safe. In reality, they provided only the **illusion** of protection - and the breach revealed the cost of that misconception.

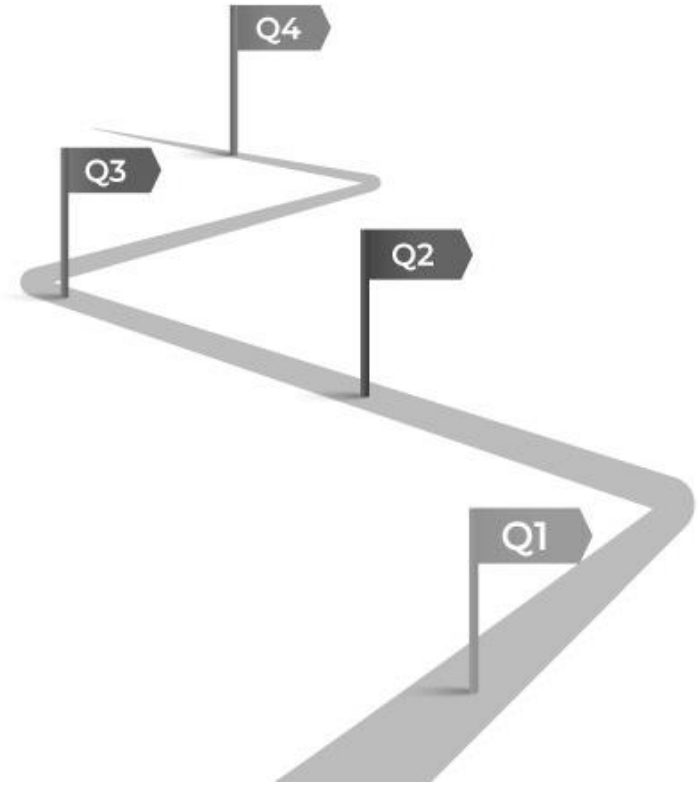
We'll prioritize Zero Trust next quarter or budgets are tight this year

This is classic *status quo* thinking: the belief that delaying Zero Trust keeps risk steady until the organization is "ready." In reality, the environment continues evolving, and risk compounds beneath that assumption.

Several forces make delays increasingly costly:

- **More assets:** New applications, servers, and devices expand the attack surface.
- **More integrations:** Additional workflows and data flows create new implicit trust paths.
- **More third-party access:** Vendor and OT support channels increase external entry points.
- **More unmanaged endpoints:** Exceptions accumulate and widen lateral movement opportunities.
- **Higher regulatory pressure:** Compliance requirements tighten, raising penalties and remediation exposure.

Each quarter an organization waits, the environment becomes larger, more interconnected, and harder to secure - making the eventual shift away from the *status quo* far more expensive.



THE REAL COST OF DELAY

People typically assess risk as being static or maintaining the status quo. However, modern networks are not static. They are evolving continuously and often without security oversight. A traditional cybersecurity approach can take up to 18 months to implement. Far slower than the rate at which exposure is growing. Every quarter of delay puts the organization further behind. Real environment quarterly growth averages may grow by:

- 3% - 7% Assets and Endpoints
- 5% - 12% Identities (Users, service accounts)
- 8% - 15% Unmanaged Devices
- 10% - 20% Vendor/Contractor Connectivity

This growth often comes with little or no security oversight, creating a growing set of technical debts. Even worse if the organization has Shadow IT. The ever-changing network steadily erodes defenses, making the status quo a false belief.

Organizations typically estimate only the cost of action (budgets, tools, staffing, etc.) while the cost of inaction is much greater. Disruption to operations due to security can have direct and indirect costs. Direct costs are lost revenue or transaction losses, overtime and emergency response labor, penalties or refunds, and recovery or remediation expenses. Less tangible costs include productivity losses, brand damage, customer churn, and loss of opportunity in the market. These costs can vary in industry and business. Below are a few examples of hourly downtime costs:

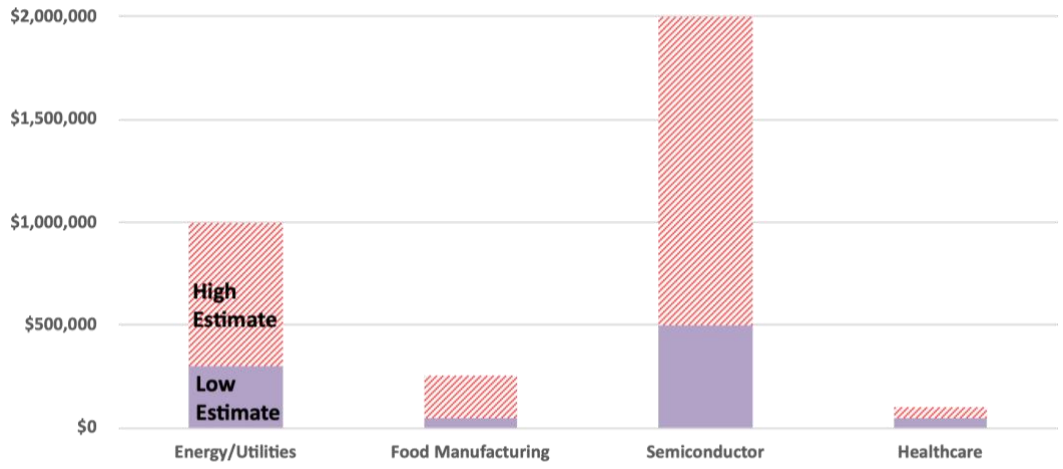


Chart 1: Hourly Cost of Downtime by Industry Averages

Measuring the growth of the environment, along with advances in threats, needs to be analyzed objectively. Not every year will an organization incur downtime due to hackers within its network. To provide a meaningful true cost of risk, it is important to use a Monte Carlo approach. A Monte Carlo method estimates the annual probability of loss due to cyberattack by establishing the potential

lower and upper costs of a breach. The analysis simulates a single random year 10,000 times to create a statistical picture of risk.

For analysis purposes, we use annual measurements based on the 2024 FAIR Institute Cybersecurity Risk Report[1]. Below are the risk valuations used:

Attack Theme	Annual Probability of Loss
Insider Misuse	9.4%
Basic Web Application Attacks	4.5%
System Intrusion	3.6%
Insider Error	11.2%
Social Engineering	2.0%
Ransomware	1.9%
Denial of Service	1.8%

Table 2: Annual Probability of Loss Percentages

To determine the true cost of delay, we have broken down these annual probabilities into monthly exponential risk percentages. For example, Insider Misuse represents 0.01%, 0.88%, 4.27%, and 9.4% after quarter 1, 2, 3, and 4; respectively. In effect, reversing the annual risk into its cumulative exponential monthly risks. For each month, we conducted independent Monte Carlo analyses, averaging 10,000 representative years a general business with ~$503M revenue.

To reflect the degradation impact on risk due to growth within the environment, we used a 20% CAGR rate against revenues. The CAGR was reversed into its annual cumulative exponential monthly risk using the same method as probability of loss risk. A separate set of Monte Carlo analyses was conducted against the growth alone to understand the impact of organization expansion.

Chart 2 shows the objective true cost of risk. Waiting only two quarters results in over $2.2M in increased cost of risk. This climbs to over $12M and $33M in the next two quarters. Delay in implementing Zero Trust increases risk quickly beyond acceptable rates.

[1] 2024 Annual Cybersecurity Risk Report

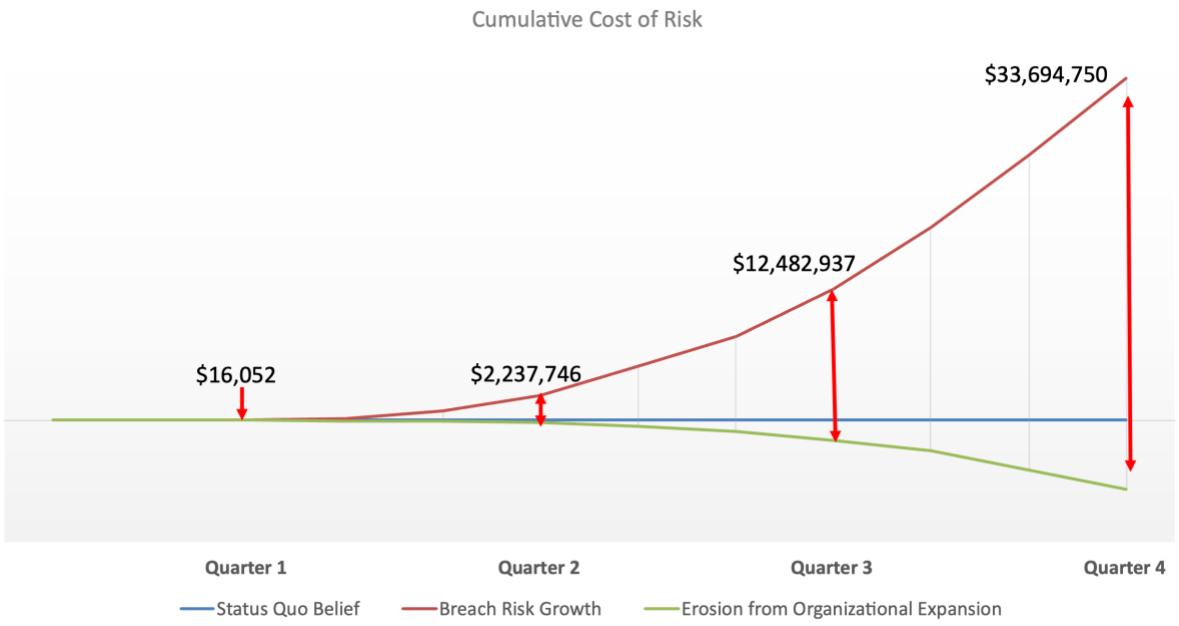


Chart 2: Quarterly Cumulative Cost of Risk

WHY ENTERPRISES DELAY

Enterprises do not delay Zero Trust because they are comfortable with risk. Enterprises delay out of fear of self-inflicted disruption to ongoing operations. Consider a business smoothly servicing customers, creating strong revenue, and good profitability, and implementing a major network change. A future prospect of breach risk seems abstract and unmanageable, while irreversible operational disruption feels weighty. Management downplays the future risk while amplifying current fear. These feelings are often reality-based and not easily dismissed.

Technology environments are ever-changing, too often with little or no maintained documentation. Administrators struggle to just keep up with the additional users, devices, or workloads and documenting changes is deprioritized. Without proper documentation, the environment deteriorates into reliance on individual knowledge of internal experts, causing an overreliance. These experts are a key resource needed to make any change within the environment, and far too often are highly limited or unavailable.

Introducing complex traditional network segmentation into the environment results in great uncertainty. Deploying change into a brittle framework leads to extensive planning and reevaluation cycles, requiring more time from the experts. This is time that the experts do not typically have, leading to delayed project timelines.

Let's briefly review some of the complexities of the traditional network segmentation which require so much expertise.

Firewalls and security zones, long considered a cornerstone of network defense, are difficult to implement to meet a granular Zero Trust need. Firewalls rely on manual configuration of rulesets requiring definition, extensive testing, and highly coordinated deployment to avoid disruption. In addition, firewalls are unable to distinguish between users, devices, or workload roles. Errors can result in network packet loss, interrupted traffic flows, or isolation of critical application communications. Many enterprises will opt to deploy firewalls using broad segmentation as a one-size-fits-all approach, negating firewalls ability to achieve Zero Trust.

More difficulty is found with VLANs. VLANs rely on Layer 2 network mechanisms to separate networks into abstracted segments. Using Layer 2 to segment creates many complexities that administrators need to navigate. For example, limitations in segment or VLAN ID (typically 4,094 usable IDs) make this technology notoriously hard to maintain at scale. Secondly, communication is limited to packet routing and flow. No information is known about which applications or services are communicating, workload identity, or whether the traffic should be allowed. The difficulties with VLANs result in organizations lagging behind growth due to constant slow and error prone manual reconfiguration needed. Many organizations are moving away from VLANs as an effective technology to achieve segmentation, seeing VLANs now obsolete.

Even advanced legacy approaches like VMware NSX migrations come with severe drawbacks. These projects rarely finish on time and typically take more than 6-12 months, making the project effectively unachievable. Organizations do not have internal expertise in NSX incurring high consultant costs and significant operational risk due to external consultants lacking internal expertise. And, deployments not matching organization's norms, such as naming methods and deployment standards, create challenges for internal organizations that need to maintain NSX post deployment.

Modern microsegmentation tools, while marketed as the solution, often create new problems. They suffer from agent bloat that impacts performance, struggle with accurate identity data integration, lead to unmanageable policy sprawl, and have limited or no applicability in operational technology (OT) and industrial environments.

Chart 3 shows typical deployment timelines needed by technology solution.

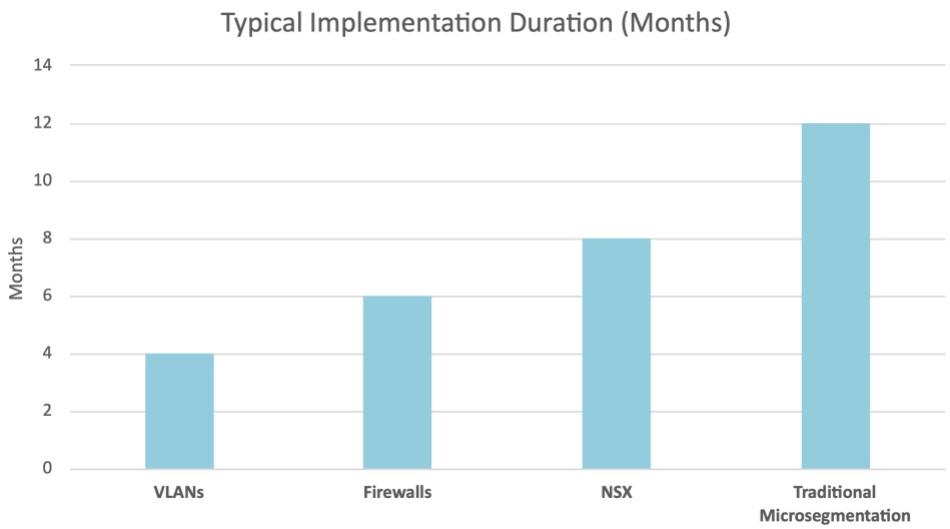


Chart 3: Typical Deployment Times by Solution

A clear pattern emerges when trying to move fast with complex legacy security solutions: Months to Years to implement. A delay that organizations cannot afford.

A BETTER WAY: ZERO TRUST IN 30 DAYS WITH VIRTUAL CHAMBERS

Zentera Systems delivers software-based Virtual Chambers that achieve the desired Zero Trust cybersecurity goals in 30 days. Virtual Chambers is the only viable defense that can match the speed of change between risk growth and expanding erosion.

Virtual Chambers represent a core innovation in zero trust security, enabling organizations to create dynamic, software-defined microsegmentation environments that isolate workloads and resources without relying on traditional hardware boundaries. By leveraging Zentera's Zero Trust Fabric, Virtual Chambers enforce granular access controls based on identity, context, and least privilege principles, preventing lateral movement of threats in hybrid and multi-cloud infrastructures. This approach simplifies compliance, reduces attack surfaces, and supports seamless connectivity for distributed teams, all while maintaining visibility and policy enforcement at scale.

> *"CoIP gives you the security that you need, and at the same time it gives you a level of agility that you just don't have today in a traditional infrastructure... we can turn things around, create projects, and complete those projects very fast."*
>
> Senior IT Manager, Siemens

Virtual Chambers in 30 days means you gain the security outcomes of:

- Elimination of lateral movement paths
- Immediate risk reduction
- Segmentation of critical assets
- Enforcement of least privilege
- Secure contractor/vendor access
- Visibility across OT/IT boundaries

With:

- No network redesign
- No downtime
- No forklift upgrades
- No disruption to OT systems
- Identity-based, packet-level control
- Virtual isolation of critical assets
- Hybrid support (cloud + on-prem + OT)

All within 30 days - making Virtual Chambers the natural solution for delivering Zero Trust without delay.

ANALYSIS CONCLUSION

The era of treating Zero Trust as a future-year initiative has ended. Every month of delay compounds risk, inflates remediation costs, erodes insurance eligibility, and exposes organizations to AI-accelerated attacks that traditional defenses can no longer contain. The excuses have been debunked, the technology barriers removed, and the financial, regulatory, and reputational penalties of inaction are now measured in real time.

With Zentera Virtual Chambers, true Zero Trust microsegmentation is no longer a multi-year project; it is achievable in as little as 30 days without ripping and replacing existing infrastructure. The silent threat is no longer the attacker; it is continued procrastination.

The choice is clear: deploy Zero Trust now with Zentera and neutralize tomorrow's threats today, or keep delaying, and further guarantee those threats will find you first. The time for Zero Trust is not coming; it is long overdue. Start today.

About Zentera

Zentera Systems is the leader in Zero Trust Security solutions for the digitally-transformed enterprise. Founded by experts in networking, security, and remote access, we offer award-winning Zero Trust networking, security, and multi-cloud connectivity that overlays any fragmented infrastructure and deploys rapidly on premises or as a service.

Our global enterprise customers and network of partners use our products to secure employee and third-party access, protect against data leaks, and instantly defend applications in complex hybrid and IT/OT environments. Based in Silicon Valley, we have received numerous recognitions, including Cool Vendor for Cloud Security by Gartner.

www.zentera.net

sales@zentera.net

+1 (408) 436-4811

About 2BSalt Financial Engineering

At 2BSalt Financial Engineering, we aim to be the premier business and finance consulting service for our clients. Our mission is to help both sellers and buyers gain a clear understanding of the business impacts of their technology decisions. By providing this clarity, we empower them to make informed choices and achieve better outcomes. We are committed to going beyond traditional financial consulting, striving to leave our clients better equipped, more confident in their solutions, and inspired with fresh ideas and insights after every interaction.

2bsalt.com