The Technical Manager’s Guide to Zero Trust: Network

October 25, 2022

Lead Research Analyst, Cybersecurity

Michael is a world-leading IT industry analyst. He has led North American and global initiatives focused on developing insights and strategies that connect technology solutions with business needs, combining data, knowledge, analysis and advanced content delivery to define options for IT and buy-side businesses.

Submitted by Michael O'Neil on 25, Oct 2022

The Technical Manager’s Guide to Zero Trust: Network

Contributing Subject Matter Experts: Michael Wilcox, Joseph Karpenko, Rob Forbes, Bill McKenzie, Jeff Riggen

This document is the third in the six-part Technical Manager's Guide to Zero Trust series, which articulates critical links between zero trust (ZT) and security strategy within each of the six ZT pillars: identity, devices, network, infrastructure, applications, and data.

Executive Summary

The zero trust (ZT) concept formalizes a change in security strategy that was initially dubbed “de-perimeterization”—a shift from a focus on hardening the corporate network perimeter against leaks and attackers to one that concentrates resources on protecting corporate intellectual property by focusing on identity (who or what is seeking access to resources on the network) and data (what resources are they seeking, and what level of access and authorization should they be granted). Zero trust strategies integrate key “pillars”—identity, devices, network, infrastructure, applications, and data—into the ZT framework, connecting priorities and activities in each area to create a holistic defense of enterprise assets.

Network plays a unique role in this transition. On one hand, the network itself moves from its position as the primary focus of security activity to one of six interrelated areas, and this loss of primacy can be difficult for legacy network-centric security professionals and organizations to absorb. On the other hand, the network is central to the integration referenced above: it is the means by which all other pillars connect. As one expert contributing to this document observed, “an application doesn't live in thin air.” It may run in a corporate data center, in the cloud, or across multiple distributed functions, but in all cases, applications require network access to resources while users require network access to applications and data.

Technical managers responsible for ZT network security need to establish an approach that spans multiple related activities:

- Documenting networking access.
- Understanding device roles.
- Defining interoperability requirements.
- Moving beyond a perimeter-based approach.

- Implementing continuous monitoring and visibility.
- Aligning network capabilities with business requirements.
- Treating each connected environment as an individual, unique entity.

This is not a “project” type challenge; it requires continuous effort and investment focused on building enhanced capabilities over time.

Defining the connections between zero trust and network

The network is central to digital infrastructure—and it is a critical point for actual execution of zero trust.

Corporate networks become more complex every day. With “users” expanding beyond human actors to include software and autonomous devices (as with IoT), and infrastructure extending past physical and VPN connections to cloud-based resources and mobile access, “there’s no edge of the network.” Most security teams can’t keep pace with this sprawl: As one contributor stated, “I have yet to work with a single client who knows all of the ingress, egress, and access points within their environments.” Corporate business activities, such as mergers and acquisitions (M&A), will further complicate the task of establishing a clear, accurate, up-to-date understanding of the enterprise network.

Technical managers responsible for network security in a ZT environment respond to this complexity by focusing “more on the process” than on individual connections. Network ZT supports the overall strategy by providing visibility into key issues, including mapping of workflows and “segmentation, secure access to data, applications, or resources from identities or devices.” As one contributor noted, “you can’t really have ‘trust’ until you have visibility.”

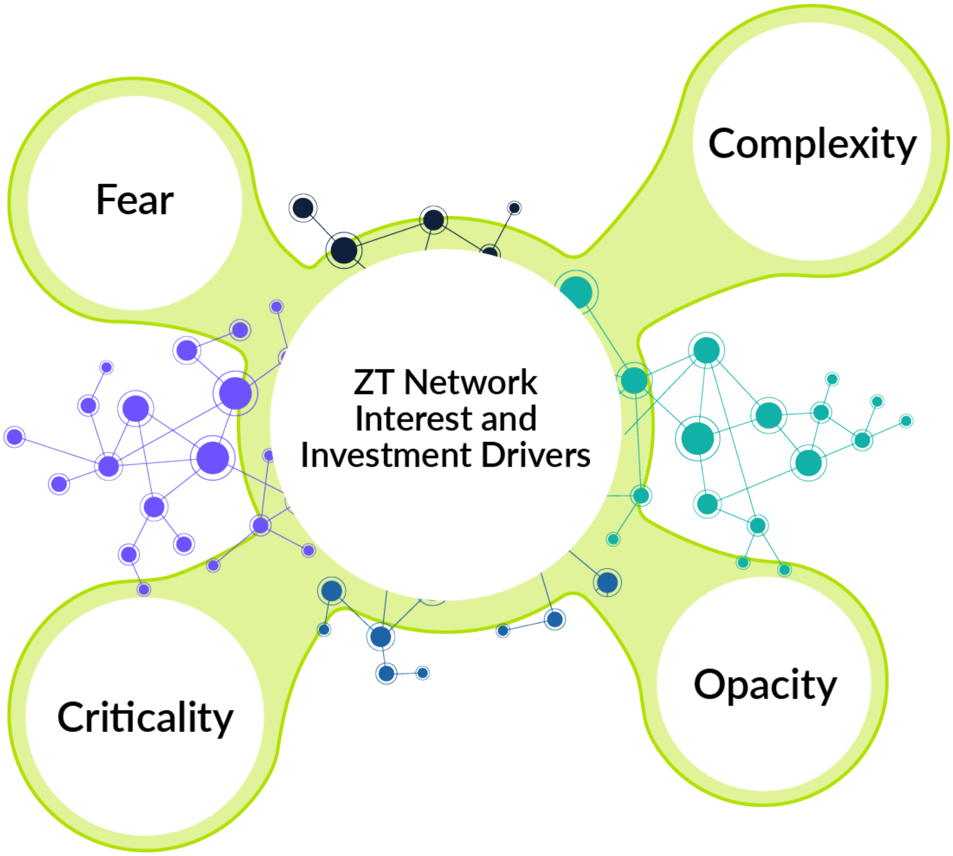
Takeaway : Zero trust has its roots in de-perimeterization, which shifts security focus from hardening the network to focusing security resources on protecting corporate intellectual property. Network still plays a critical role in ZT, however. Network is the nexus for all other ZT pillars and provides essential perspectives on connections and workflows that span the corporate environment. ZT network managers enable cross-pillar visibility that is critical to ZT strategy.

Drivers of ZT interest and investment in network security

To build a cohesive approach to zero trust, security leadership needs to achieve a judicious balance of interests and objectives. These include driving investment and attention to areas of greatest need within the enterprise IT delivery environment and constructing a comprehensive approach to defense of corporate assets. Each pillar has professionals charged with executing on plans within their domain, and each is essential to success of the ZT strategy.

What impels networking security managers to commit to a broader ZT vision, and what factors cause ZT-responsible management to prioritize investment in the network?

Contributors to this document identified four interest and investment drivers that align both perspectives in support of network ZT: criticality, fear, opacity, and complexity. These factors each motivate ZT-focused network security measures and combine to create an environment where ZT network is a compelling business priority.



Criticality

The first factor driving ZT network interest and investment is the understanding that digital infrastructure—including, and especially, the network—*is* business infrastructure in today’s world. “One of the things we learned in the pandemic,” a contributor observed, “is that the line between digital business and business is gone. All business is digital.” Drilling down, this means that “your network includes everybody you do business with—all your suppliers, all your investors, all of your customers, all of your prospects, all of your employees, subcontractors.” Each new constituency needs to provide and access data. “There is going to be a stew of your corporate data, people's personal data, other corporations’ data—data that needs to be somehow walled off from a network perspective.”

The downside to technology infrastructure providing the platform for digital business is that this status makes corporate systems an attractive attack target and makes breaches and failure front-page news. There is a concurrent belief that traditional perimeter-focused security strategies will fail to adequately defend against this mounting pressure: “Traditional security in networking doesn't work.”

Discussion on this topic considered the need to address issues that span multiple functions, including comments to the effect that traditional approaches are “not application aware” or lack the ability to “move up the stack.” These types of constraints arise from an orientation that builds capability silos—or from a ZT perspective, from a lack of connectedness to issues that are handled within other zero trust pillars.

Key point: Digital business makes corporate intellectual property both critical to operational success and a priority for protection against loss or attack. Intense public (including shareholder and regulator) interest in data security brings scrutiny to breaches—and as one contributor put it, “That's why people are investing in [ZT network]. They don't want to be on the front page of the paper tomorrow.”

Complexity

In the digital world, enterprise networks span many kinds of environments and connections:

- Traditional on-premises facilities, servers, and applications.
- Mobile devices that shift locations and access points regularly.
- IoT devices that have limited processing capacity and which may be deployed in report or inaccessible environments.
- Content distribution networks (CDNs).
- Cloud-based systems (both IaaS and SaaS).
- External users—suppliers, customers, and other stakeholders—who need access to corporate resources.

This complexity has been a major challenge for security teams tied to traditional perimeter-based strategies: There is no real perimeter in complex environments. At one time, using VPNs to secure connections to resources housed in corporate data centers helped putty over the authorized incursions from individual external devices and users, but this approach is impractical when the resources are housed in the cloud. The VPN creates a high-overhead bottleneck that increases cost and degrades performance, and the cloud itself expands the perimeter beyond the reach of traditional tools.

Key point: There is a seemingly endless cascade of new network types, new kinds of connected devices and environments, and new security tools and protocols to defend against the new vulnerabilities that these assets create. As a Stratascale SME noted, "existing tools have failed [to protect] the existing components." Reactive and perimeter-oriented strategies can't keep pace with the expanding protect surface. Zero trust provides a basis for a proactive network security strategy.

Fear and Opacity

Fear—of unknown threats, of complexity that masks vulnerabilities and creates attack vectors, of public disclosure of breaches that can have multi-billion dollar impacts on valuations (and deleterious effects on security leadership career trajectories)—can be seen as the awning under which the other ZT network drivers connect.

Fear is not necessarily a negative factor in strategy development: It focuses attention on highest-value, the most-vulnerable, and the most frequently attacked vectors and assets within an enterprise. And fear is fed by opacity—the inability to clearly see and define threats to key assets. As a result, ZT network experts stress the importance of visibility as a network security attribute.

The Stratascale report "Key Zero Trust Technologies and Management Imperatives" positions visibility as a foundational aspect of corporate ZT strategy as well as a critical ZT network issue. Network security managers need to obtain immediate visibility into vulnerabilities and attacks as they arise. They can mitigate fear of the unknown by providing real-time insight into threats and requirements and enable effective remediation of issues before they damage corporate assets.

Key point: Fear is a natural reaction to the business and professional threats that result from breaches. As the saying goes, "sunshine is the best disinfectant." In this context, "sunshine," or clarity, is achieved by addressing complexity and visibility challenges. As one contributor to this report observed, "different [disconnected IT and security] initiatives cause loss of visibility—and now, we don't know how to control access to resources. We lack the visibility needed to know and understand *what's accessing [which resources], and when." In a ZT network context, visibility is both a critical capability and a means of providing a healthy, fact-based response to amorphous fears of cyberattack.*

Three key ZT network security priorities

Priority 1: Catch up to the environment and requirement. Asked what they identify as key priorities for firms looking to align network security with zero trust, one Stratascale SME said bluntly that many firms are "still so far behind the technology they haven't taken step one" towards ZT. Executives, the SME believes, have a grasp on the problems, including the mix of corporate and non-corporate access devices and assets, and the need to prevent unauthorized access to sensitive data. But many "say 'zero trust' like it's a solution that you just open a box and implement," and it is not: It's the beginning of a strategic discussion that requires years' worth of hard work to translate into a robust approach to comprehensive protect surface coverage.

Priority 2. Align your approach with your corporate infrastructure. One of the key foundations of ZT network is microsegmentation—the ability to tightly define where data and access (from users, devices, or between applications) can and cannot connect. Microsegmentation works best when it aligns closely with the corporate infrastructure—with the different facilities (including cloud and hosted as well as on-premises) where data is stored and with the applications that will look for data and resources.

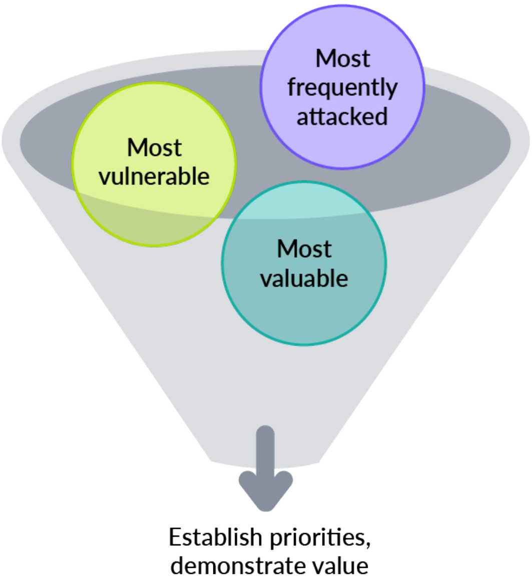
Committing to an approach that wraps in staff responsible for securing other ZT pillars, including infrastructure and applications, as well as identity, devices, and data, pays dividends by ensuring that a key element of your ZT network strategy connects optimally with the systems and information that it is protecting, and establishes a basis for further cross-pillar collaboration in the future.

Priority 3: Commit to a staged approach and to proving value throughout the ZT network journey. This is almost a "bait and switch" priority. Articulating a staged approach—and identifying the "low hanging fruit" objectives that demonstrate value as the journey progresses—requires ZT network managers to develop visibility into where data and applications reside, and how users (and non-human connections, such as IoT devices and application-to-application dependencies) interact with resources. With these inputs, ZT network managers can define a strategy that includes checkpoints which can help colleagues understand benefits as they are delivered.

Because network ZT is so complex, a staged approach is absolutely necessary: No security team can (or should attempt to) deploy all the potential ZT network defenses at once. In this type of extended deployment scenario, it’s “good business” to create opportunities for demonstrating that the steps in the journey have discrete value, and for communicating these benefits to colleagues and other stakeholders. It’s important to note, though, that protect surface priorities can be defined in different ways. Three common approaches include:

- The value of the intellectual property that is being protected.
- The relative weakness of vulnerabilities that could expose data, applications, or other assets.
- The frequency with which a system is probed or attacked.

ZT network managers need to balance these three considerations (potentially assigning highest priority to assets that are subject to frequent exploit attempts) and ensure that both the objective and the reason for prioritizing it is clearly understood within the business. At the same time, ZT network managers need to guard against the temptation, sometimes apparent in engineering-led cultures, to build out entire frameworks before demonstrating any functionality. All corporate stakeholders will expect ZT managers to establish an incremental path to evolving ZT capability.



Source: Stratascale, 2022

Takeaway: ZT network priorities stress the need for a systematic approach to capability building. As the new twist on an old saying holds, "the journey of 1,000 miles doesn't really start with a single step—it starts with a plan." Current ZT network challenges have evolved over a period of years, and will continue to evolve, and the strategies, technologies, and practices designed to proactively address these challenges will also roll out over time. ZT success, in network and across the organization, relies on continuous improvement. In the words of a Stratascale SME, "Nobody will ever be purely secure. But if every day I take on a problem and solve one aspect of it, then I move the needle. You don't have to make huge jumps to move that needle—to have a large [cumulative] impact—and I think a lot of people forget that. Start with the fundamentals, keep building on them. It goes back to a culture [with everyone continuously asking] how do we get better?"

Defining the path to ZT network

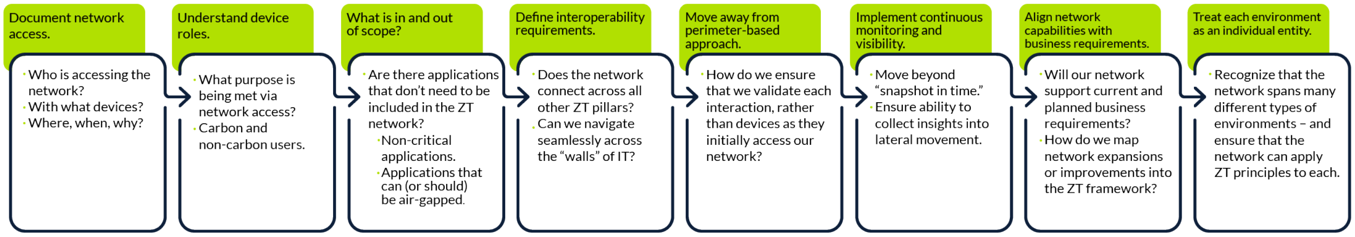
Each document in the *Technical Manager’s Guide to Zero Trust* series incorporates a roadmap providing practical guidance to readers looking to implement ZT within their areas. The advice offered by contributors to this document addresses eight important steps:

1. **Document network access.** ZT network “starts off with the who, what, where, when, why”—with questions like “Who is requesting access to resources via the network?” and, “What devices are attempting to access resources via the network?” Adding context—the location of the identity looking for access (is this user actually based in that country?), the time at which the connection is launched (is this user or device or application often, or supposed to be, active at this time?), and the nature of the request (does this user or device typically ask for this magnitude of data?)—helps to focus attention on potential attacks or intrusions. In the words of a contributor to this research, “You've got to know that on the front end to even start” establishing zero trust network security.
2. **Understand device roles.** The devices accessing the corporate network have attributes that are important to understanding whether they are functioning normally, or whether there is a need for containment and examination. The increasing prevalence of non-human “users”—IoT devices, applications, and other “non-carbon” sources of network access and input/output—complicates the ZT network manager’s role. Contributors stressed that not all devices that appear insecure are hostile. For example, “that Windows Vista computer could be sitting behind the defibrillator that's on the wall. Or it could be the insulin pump that is attached to a patient.” The growing diversity of network-attached devices underscores the need to develop insight into the roles played by different access points.
3. **Determine what is in and out of scope.** Zero trust unites defenses across the environment to protect key intellectual property, but there are cases where this level of protection isn’t needed, or where alternative approaches may satisfy business requirements. Non-critical applications, for example, may not need to be fully incorporated within the ZT strategy. In other cases—potentially, for example, with OT networks—it may be simpler and more effective to air-gap than to extend the ZT protect surface.
4. **Define interoperability requirements.** Traditionally, IT functions have been defined as independent (often, siloed) domains: Networking, infrastructure, devices, and applications have implemented policies autonomously. An important aspect of ZT capability, though, is interoperability across the pillars.

Organizations that lack cross-functional cohesion will take actions—such as investing in point solutions or tools that meet a specific need, but which can't exchange information with systems used to secure other parts of the corporate environment—that may address immediate priorities but don't contribute to overall ZT maturity.

- ○ *NB: This step underscores the importance of maintaining strong connections to managers working in the other ZT pillars. The network provides crucial information to each other function—and they in turn provide insight and content that is necessary for effective ZT network operations.*

ZT Process Roadmap: Network



Document network access.

- Who is accessing the network?
- With what devices?
- Where, when, why?

Understand device roles.

- What purpose is being met via network access?
- Carbon and non-carbon users.

What is in and out of scope?

- Are there applications that don't need to be included in the ZT network?
  - Non-critical applications.
  - Applications that can (or should) be air-gapped.

Define interoperability requirements.

- Does the network connect across all other ZT pillars?
- Can we navigate seamlessly across the "walls" of IT?

Move away from perimeter-based approach.

- How do we ensure that we validate each interaction, rather than devices as they initially access our network?

Implement continuous monitoring and visibility.

- Move beyond "snapshot in time."
- Ensure ability to collect insights into lateral movement.

Align network capabilities with business requirements.

- Will our network support current and planned business requirements?
- How do we map network expansions or improvements into the ZT framework?

Treat each environment as an individual entity.

- Recognize that the network spans many different types of environments – and ensure that the network can apply ZT principles to each.

Source: Stratascale, 2022

5. **Move away from a perimeter-based approach.** De-perimeterization is literally the starting point for ZT. And yet, companies (and network managers particularly) will sometimes revert to perimeter-based approaches, sometimes because they can leverage existing tools to deliver a rapid response to a current problem, and sometimes simply as a result of "entrained

thinking"—perspectives shaped by past experiences. Reliance on perimeter defense, though, is antithetical to ZT strategy: ZT demands "that we validate each interaction, rather than the devices as they initially access our network."

6. **Implement continuous monitoring and management.** In a ZT framework, "a snapshot in time is useless." ZT requires continuous monitoring of access, requests, and interactions: "Everything connects"—on-premises environments and the cloud, legacy applications and SaaS, intracloud and same-cloud processes. Complex environments can mask lateral threats designed to elude scrutiny. It's not possible to keep pace with periodic inspection using tools designed to analyze a single environment, "to try and scan with traditional methods." ZT network managers need to have continuous visibility across the entire network and its attached resources if they are going to protect against threats that may not yet be identified or catalogued.
7. **Align network capabilities with business requirements.** In many cases, ZT network managers are wholly focused on technology issues and interactions with technical peers. In a digital world, though, the business is an important driver of requirements. The most effective ZT network leaders are in contact with business peers to understand how business objectives are progressing and to ensure that all involved know how network security will need to evolve to extend protection to new requirements. This positions the ZT network manager to be a leader in technology-focused strategic conversations as well: They can ask colleagues how the network will evolve to meet new business requirements, and then map in the considerations they need to address to align zero trust with new internal technologies and external connections.
8. **Treat each environment as an individual entity.** It is often the case that "the network" is viewed internally as a highly complex but single organism—that solutions deployed in one area are required everywhere and will adequately manage similar threats arising in different contexts. This can be a perilous assumption. Both the (human and non-human) "user" population and the environments (on-premises, different IaaS and SaaS clouds) that deliver services to these users are becoming more diverse. An approach that creates visibility or highlights anomalies in environments that provide employees with access to core applications may have constraints that limit their utility in IoT environments; they may lack support for processes that span multiple clouds; they may be unable to effectively address devices used by supply chain partners. ZT network managers who develop a granular view of connected

environments can identify both opportunities for use of common tools and situations that demand unique approaches.

Three ZT network roadblocks and challenges

ZT network security offers compelling benefits, and the graphic above defines a workable path for technical managers responsible for its execution. But no strategy is immune to real-world challenges. Where are these most likely to arise on the path to establishing ZT networks? Stratascale SMEs contributing to this document identified three impediments that infrastructure security managers may need to overcome during their ZT journey:

- *Cost, fear, lack of knowledge, and lack of visibility into problems within the environment.* This set of challenges echoes, to a large degree, the drivers of ZT network interest and investment discussed earlier in this report. Cost speaks for itself as a roadblock: Investment in capabilities that by design will never be apparent if they function optimally can be a tough “sell” for network security managers. Lack of knowledge, lack of visibility, and fear are different components of the same problem. Many newly appointed or promoted managers find that their predecessor made it a policy to “not flip over rocks because there are ‘worms’ under them”—to not expose problems that may draw unwanted executive scrutiny, or which can only be fixed with resources that aren’t easily marshalled. This approach can be seen at the top of the security leadership pyramid as well: Experts talk of an “ostrich CISO” persona that attempts to sidestep deeply ingrained problems despite knowing (at some level) that they have some liability for the problem and are responsible for its resolution.
    - *Worth remembering:* Problem avoidance isn’t uncommon, but it is certainly not recommended. ZT network managers should invest in building visibility and use that insight to surface issues that need attention. As one contributor to this report observed, “you've got the same problem regardless of whether you know it's there or not—and if you don't know a problem is there, you're not dealing with it.”
- *Siloed mindsets.* To succeed, ZT network managers need to “work across the business”—yet many lack the language, seniority, or confidence to engage on a peer level with both business leaders and colleagues in other parts of the security and IT organization. But staying within a comfort zone defined by

colleagues sharing common responsibilities is not a preferred approach. It’s much better for the ZT network manager to seek executive support for cross-functional discussions that unlock ZT’s advantages.

  - *Success indicator:* One contributor to this report insisted that “you have to have a center of excellence or a steering committee. The mandate needs to come from the top down, and the collaboration needs to extend across the board.”

- *Network technology.* One contributor to this research advised ZT network managers to be honest about their starting position as they begin to define a zero trust network journey. “What's the state of your network today? Are you running on 10-year-old gear that doesn't have the security capabilities that are standard in new gear? [Aligning with future needs can be] like driving a Ferrari on a road full of potholes. You're not going to get the performance you need. And each pothole provides the opportunity for something bad to happen to the Ferrari.”
  - *Important consideration:* Refresh cycles and new product selection may well be outside the scope of the ZT network manager’s responsibility, but network technology can be a significant obstacle to ZT progress. Be sure that you have input where it is needed, and that you aren’t tied to a plan that relies on products that don’t materialize on or near schedule.

Important ZT network technologies and management imperatives

As part of its *Executive Guide to Zero Trust* research series, Stratascale published the report, Key Zero Trust Technologies and Management Imperatives. The ZT network section of this report highlights the following technologies or practices that managers should understand as they plot their ZT network strategies:

Microsegmentation

Microsegmentation (not exactly as pictured)

microsegmentation (not exactly as pictured)

Microsegmentation is the starting point for most ZT network authorities. In the words of one contributor to this document, “everybody has VLANs and stuff like that. Microsegmentation is [central to] the ZT end goal. You want to have specific rules for a device: ‘These data flows go there, and nothing else shall pass.’”

This distinction matters in a zero trust context. Segmentation is generally deployed in terms of rules that apply to a group of resources, such as a set of databases. Microsegmentation drills down to identity (human and non-human), device, data, and resource-specific data flows.

Contributors to this document noted that the depth of segmentation used by an organization varies with maturity. Some firms have “flat networks” that lack segmentation; others have progressed only as far as VLANs and group-based policies. Organizations with more mature ZT network approaches use microsegmentation that considers identity, device, data, and resources. Firms plotting a ZT journey can position segmentation as a means of improving alignment of defenses with sensitive data and other high-value corporate intellectual property.

Encryption

Encryption seems like it might fit most naturally within the application or data pillar, but many organizations implement encryption within the network. Applications don't apply encryption consistently, and some legacy applications may not encrypt data at all. Network layer encryption ensures that all data is encrypted and can simplify management: The encryption can be performed through different devices on the network (load balancers, firewalls) or via a software proxy. It should be noted that while this approach satisfies the need to encrypt "north side" data—for example, ecommerce communications between a facility and a customer—it may not always encrypt "south side" data: Internal traffic (within a corporate data center, or within the cloud) may still be clear text.

Visibility

Visibility is a complicated topic in zero trust: It applies at both the network level and (as a "foundational requirement") across the entire ZT environment. At a macro level, visibility (and analytics) references the capacity to aggregate, digest, and act on information that spans all pillars and the entire protect surface. This insight relies to a large extent on visibility developed at the network level. It is crucial for ZT network managers to have deep insight into network functions, performance, and potential vulnerabilities and threats. ZT requires success across and within each of the pillars, but the network's unique position as a nexus for access and data makes visibility a key ZT network attribute: A ZT network enables teams to see vulnerabilities and attacks as they arise. This enables network security to take action to prevent attacks from expanding within the corporate environment and issue appropriate intelligence to other pillars as required.

VPN Replacement/Software-Defined Perimeter (SDP)

The pandemic exposed a fundamental flaw in VPN-centric remote access strategies: As the migration of workloads to the cloud kept accelerating, an architecture mandating that a remote user tunnel into a central facility to access cloud-based resources was a poor use of budget, time, and bandwidth. VPNs that only authenticate on entry and then permit access to a vast swath of corporate assets are also a poor fit with zero trust. Moving forward, security leaders will look to establish software-defined perimeters, inspecting traffic and defining rules that govern resource access regardless of where the user or resource is located. Many organizations deploy cloud access service broker (CASB) or secure access service edge (SASE) technologies to address this requirement.

Wait—what about ZTNA?

ZTNA—often referring to “Zero Trust Network Access” and sometimes used as an acronym for "Zero Trust Network Architecture"—is a common term in ZT discussions. It isn't included in this list because products marketed in this category combine several of the core ZT network capabilities described above: “Depending on the vendor, [ZTNA can include] SDP/VPN replacement, microsegmentation for cloud and endpoint devices... CASB and DLP is also included in several vendors' ZTNA products; additionally, you'll see some vendors toss in MFA into their ZTNA.”

This isn't to say that ZTNA may not play an important role in a ZT network strategy. Security managers are often torn between acquiring “best of breed” products that might or might not integrate with other components used in the environment versus “best of group” products that may not be best in a specific area, but which integrate needed capabilities. ZTNA may well be a powerful solution for a specific organization—but it’s incumbent on ZT network management to identify the requirements that a specific ZTNA solution addresses, ascertaining which are truly gaps in the current environment and which may overlap other tools that are already deployed.

ZT Infrastructure recommendations

At the end of the research discussion, contributing SMEs were asked to propose recommendations that will help Stratascale client managers succeed in establishing zero trust infrastructure security. These recommendations include:

- **Define your protect surface.** The ZT starting point for network security managers, one SME insisted, is to understand “What are you trying to protect?”

Enterprises will have different definitions of what intellectual property is critical to the business. Many will lack a clear understanding of where this data resides, and which human and non-human users will access, augment, or change these resources. ZT network managers need to establish a clear understanding of the protect surface—what the organizational priorities are, and why—so that the ZT network roadmap can be positioned as a means of addressing key issues immediately and of building critical capabilities over time.

- **Embrace the brownfield reality, and plan for incremental rollout *and* rationalization.** In discussing this point, one Stratascale SME pointed out that “the easiest way to secure the network is to turn things off.” Unneeded devices require time and material investments but deliver no benefit to the business. Rationalization ensures that security resources are allocated to real requirements, and that each new capability improves the enterprise security posture.
- **Think big, start small, move fast.** This pithy guidance isn’t specific to a ZT network, but it certainly applies in context. ZT network managers need to develop and socialize a network vision that aligns with both evolving business requirements and current and future state network capabilities, one that’s designed to optimize cross-pillar collaboration and whole-environment visibility. But they also need to be agile in their rollout tactics—identifying opportunities for deployments or approaches that deliver rapid, tangible benefits, enabling the ZT network manager to build organizational confidence and support while moving quickly through the rollout plan.

ZT network metrics

As part of its zero trust research program, the Stratascale team has developed the Stratascale Zero Trust Metrics in Context and Action (*Stratascale ZT-MICA*) metrics set, which provides strategic insights to executives, operational perspectives to IT and security management, and tactical data to managers responsible for ZT within each of the six pillars.

ZT network security management metrics within Stratascale ZT-MICA include:

- Total number of devices (corporate/BYOD) utilizing microsegmentation.
- Total number of servers utilizing microsegmentation.
- Percentage of network traffic inspected and logged.

- Number of users with traditional VPN access.
- Percentage of VPN users enrolled in MFA.
- Percentage of network devices enrolled in configuration management.
- Number of network zones for IOT/IOTM/OT devices/systems.
- Number of network zones for on-prem servers.
- Number of network zones for cloud servers/applications.
- Percentage of cloud servers/applications covered by CSPM.
- Number of third-party users with privileged access to network devices (firewalls/routers/switches).

Collectively, these measurements help network security managers assess readiness and progress over time and identify and respond to areas of need before they are exploited.

Readers looking for a downloadable version of *Stratascale ZT-MICA* can follow this link (no cost, but registration required).

ZT network technology suppliers

In its “Zero Trust Vendors to Watch, Know, Understand: ZT Network” series, Stratascale experts reviewed 120 vendors to identify those that could be important to ZT network strategies in the four core areas discussed in the “important ZT network technologies and management imperatives” section of this document—microsegmentation, encryption, visibility, and VPN replacement/SDP.

Caveats to consider in reviewing the lists below:

- In each area, vendors were included only if they were familiar to our team of experts from our work with clients, and considered relevant to both the category and zero trust network strategy.
- Reviewers also drew a distinction between vendors who are broadly applicable to the enterprise environments that Stratascale addresses (generally, Fortune 1000 businesses) and those which are relevant in specific niches but not across all potential enterprise use cases.
- As a default in this document and others in the *Technical Manager’s Guide to Zero Trust* series, firms which have been acquired are listed under their original names, with notes indicating the acquiring company in the profiles included in the linked documents. This gives readers a chance to see how specific

capabilities have been aggregated via acquisition.

Results of these analyses are available in individual reports (linked via the section headers below). Vendors discussed in these reports include:

Microsegmentation

Vendors that buyers should consider when looking to build or enhance enterprise ZT microsegmentation capabilities, listed in alphabetical order:

Alkira	Aviatrix	Carbon Black	Cisco
ColorTokens	Cyolo	Ericom	Fortinet
GuardiCore	iboss	Illumio	Juniper Networks
Netskope	Nile	Palo Alto Networks	Perimeter 81
Pulse Secure	Saviynt	ShieldX Networks	VMware
WiteSand Systems	Zscalar		

Vendors that address specific ZT microsegmentation requirements and may fit specific needs but don't apply to a full spectrum of enterprise ZT microsegmentation use cases:

- Aruba Networks
- Hysolate
- Ordr
- SentinelOne
- Symantec
- Talon Cyber Security
- vArmour

Click here to access the Zero Trust Vendors to Watch, Know, Understand: ZT Network—Microsegmentation report.

Encryption

Vendors that buyers should consider when looking to build or enhance enterprise ZT network encryption capabilities, listed in alphabetical order:

- Baffle
- Check Point
- Gemalto
- Hewlett Packard Enterprise
- Proofpoint
- Thales
- Titaniam

Vendors that address specific ZT network encryption requirements and may fit specific needs but don't apply to a full spectrum of enterprise ZT network encryption use cases:

- Fortanix

Click here to access the Zero Trust Vendors to Watch, Know, Understand: ZT Network—Encryption report.

Visibility

Vendors that buyers should consider when looking to build or enhance enterprise ZT visibility capabilities, listed in alphabetical order:

- A10

Networks Akamai Arbor Networks Arista Aruba Networks

Awake Security Cat Networks Check Point Cisco Cloudflare

Corelight	Darktrace	Extrahop	F5 Networks	Fastly
FireEye	Fortinet	Gigamon	IronNet Cybersecurity	Lastline
McAfee	MixMode	Netscout	Plixer	Vectra AI
Zscalar				

Vendors that address specific ZT network visibility requirements and may fit specific needs but don't apply to a full spectrum of enterprise ZT network visibility use cases:

- Alert Logic
- Imperva
- Neustar
- Radware
- Trend Micro

Click here to access the Zero Trust Vendors to Watch, Know, Understand: ZT Network—Visibility report.

VPN Replacement/Software-Defined (SD) Perimeter

Vendors that buyers should consider when looking to build or enhance enterprise ZT VPN replacement/SD perimeter capabilities, listed in alphabetical order:

- Banyan Security
- Cisco
- Fortinet
- Juniper Networks
- Microsoft
- Palo Alto Networks
- Perimeter 81
- Pulse Secure

- Safe-T
- Tailscale

Click here to access the Zero Trust Vendors to Watch, Know, Understand: ZT Network—VPN Replacement/SD Perimeter report.

Stratascale brings a unique combination of expertise, solution depth and vendor relationships and insight to the cybersecurity market. Readers seeking support in developing zero trust strategies are encouraged to contact their Stratascale Client Advisor or to connect with us at stratascale.com/contact-us/.

This is the third of six documents included in Stratascale's "Technical Manager's Guide to Zero Trust" research series. We have also published an eight-part companion series, "The Executive Guide to Zero Trust", available on the Stratascale website.