stratascale
An SHI Company

The Executive's Guide to Key Zero Trust Technologies and Management Imperatives

Michael O'Neil, Joseph Karpenko, Rob Forbes, Michael Wilcox, and Alex Banghart

Zero trust thought leadership group members: Geeta Kapoor (MSC Direct), Noah Davis (Trane Technologies), Leon Ravenna (KAR Global), Barney Baldwin (ex-MUFG, Columbia), Chase Cunningham (Ericom), Eve Maler (ForgeRock), Sean Frazier (Okta)

Members of the zero trust (ZT) thought leadership group agreed that "ZT is not a product" – it's a strategy, a framework, and/or the journey to implementing that strategy or framework. But the steps on this journey are often defined by technology initiatives. CISOs will aim to instantiate overall zero trust benefits with terrain-level investments and activities. CISOs can make this connection by articulating which technologies and associated management imperatives are important to the ZT path, how these support broader ZT objectives, and why an incremental approach optimizes the value of currently deployed and new technology.

Executive Summary

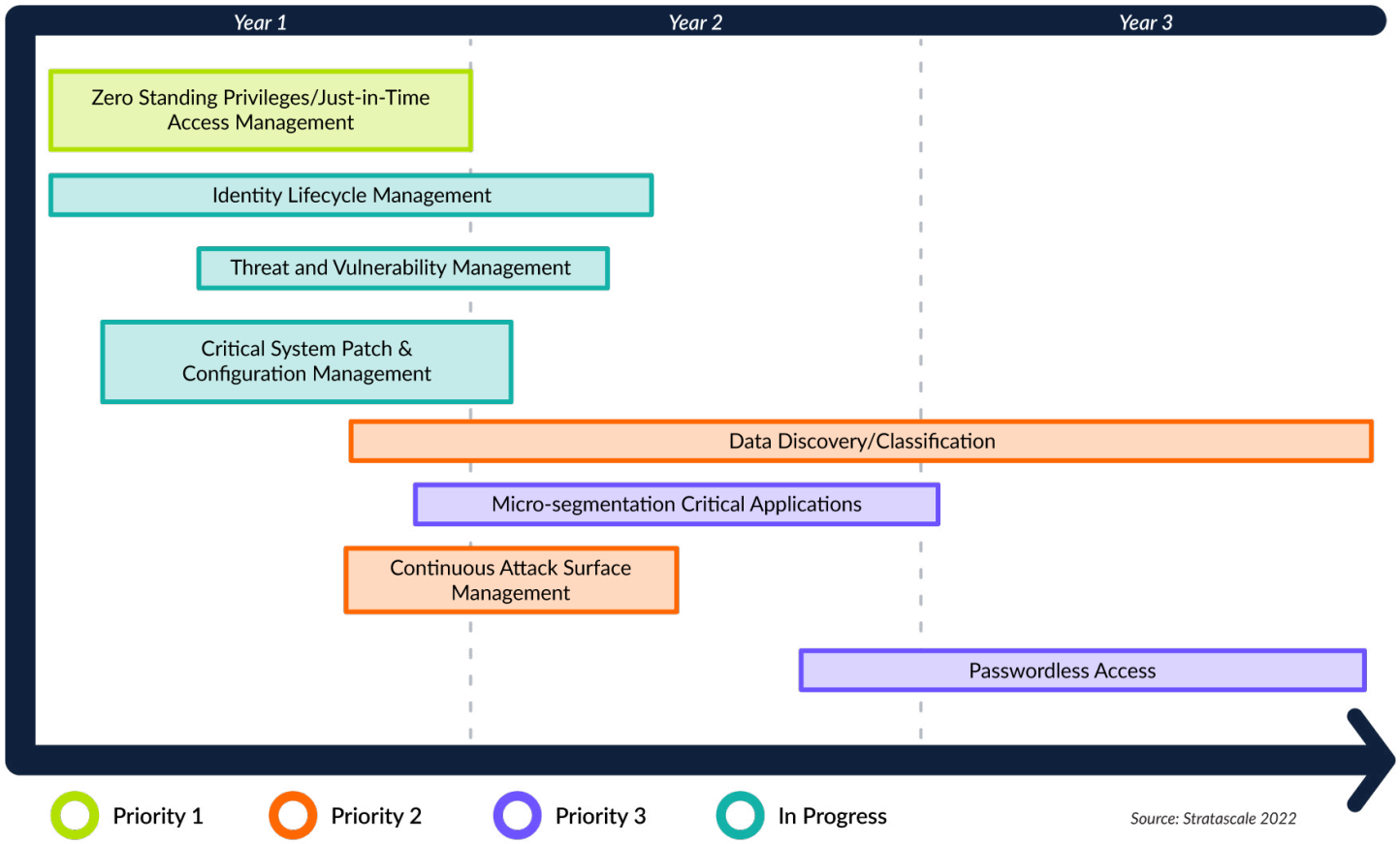
Despite the claims of vendors touting a wide range of security products, zero trust isn't defined by technology; it is best thought of as a strategy that involves a long-term action plan. This plan involves technologies, capabilities, and related practices at the execution level. Each company will build its own unique roadmap, considering its current maturity, environment, timeframes, and budget priorities.

Many executives, however, face pressure to express ZT strategy regarding technology roadmaps. A team of Stratascale SMEs identified the most important technologies, capabilities, and practices in each of the six ZT pillars to address this requirement. Understanding where to focus in each area helps CISOs plot a course that addresses the entire corporate ZT posture. Using this guidance, security leaders can ensure that they have measures in place to respond to requirements across the digital business's protect surface.

Defining a ZT roadmap

This document highlights 33 technologies and management practices across the six zero trust pillars, plus several foundational requirements that support ZT at an organizational level. No business can simultaneously deploy all these technologies, nor should they try. Some required tools are likely deployed today, and others can be positioned across a strategic timeline, allowing the security team to digest and optimize new capabilities. This guide will enable CISOs to allocate investment across pillars, thereby improving cyber hygiene, posture, and resilience.

The diagram below shows how a ZT strategy requires clarity and focus across pillars, technologies, and time. The sample organization is advised to start with identity-related initiatives and layer in needed hygiene (critical system patch and configuration management). Over time, the organization will launch a critical data discovery and classification initiative, address its attack surface, and upgrade its network and application ZT before moving to passwordless authentication to improve and mature its identity program.



Planning for a continuous journey

In our executive discussions, most zero trust thought leadership group members prefaced their guidance with a caveat: zero trust is built on top of existing infrastructure – it is not a "rip and replace" endeavor. In fact, ZT often leads naturally to simplifying approaches in key areas, which can result in solution rationalization and consolidation of products and vendors.[1]

[1]See in particular the "Incrementalism" section in *The Zero Trust Rollout Notebook*.

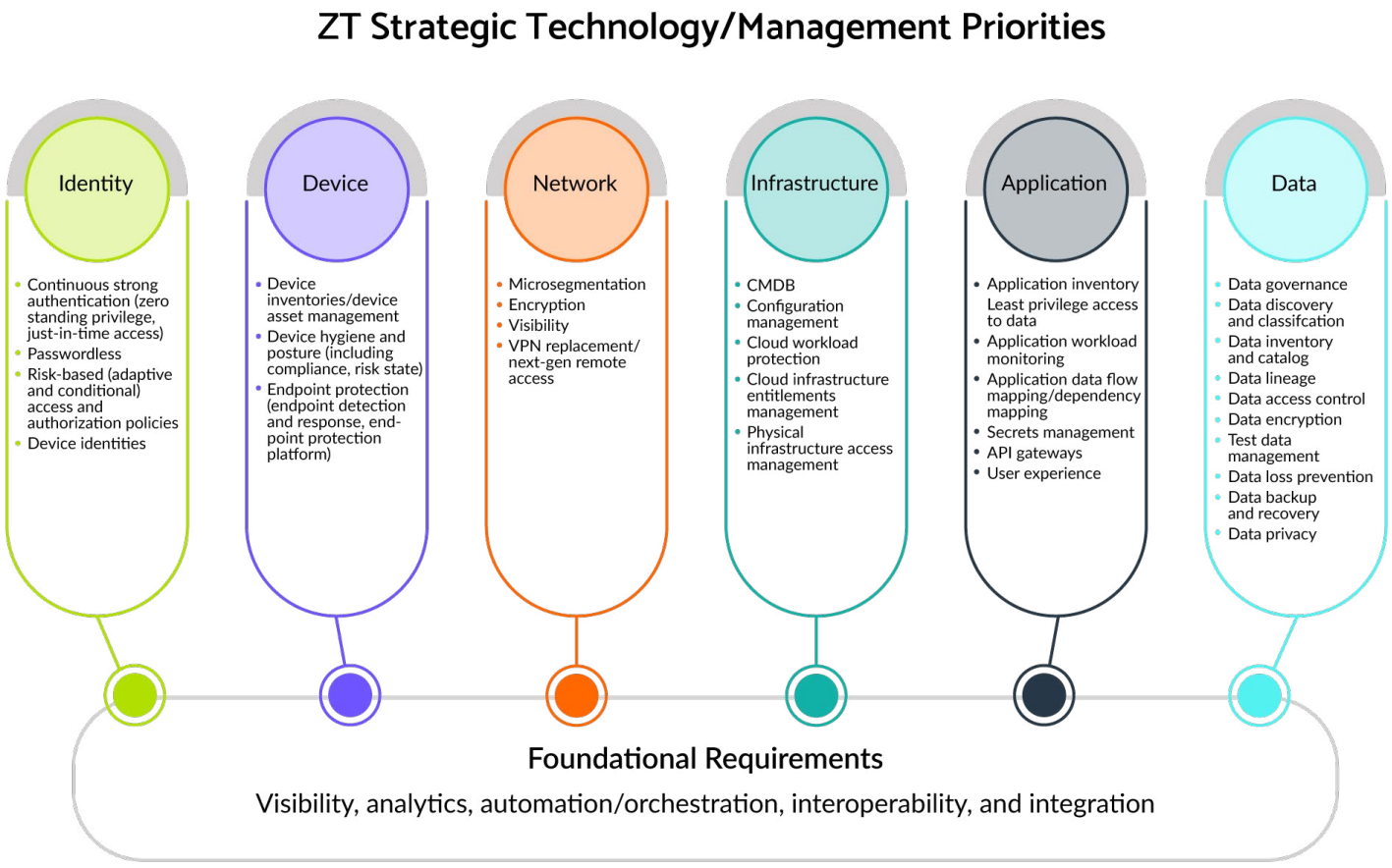
One contributor to this research used the concept of value streams to illustrate how incremental ZT technology plans evolve – why taking a long-term rather than project-based approach to ZT is the only way to capture its benefits. "The worst possible approach is a project mindset, which will fail because projects end. It is much better to adopt a value stream mindset where you recognize that everything that you put in place will require continuous investment."

The CISO went on to emphasize that funding "is always a matter of prioritization" across competing priorities: "You need to make difficult decisions as you [implement zero trust], and you need the right mindset from the whole organization and the right culture to keep things moving forward."

Technologies

The ZT journey doesn't have a defined endpoint. It will require a balanced approach to technology. There is no Zero Trust Off-the-Shelf (ZTOTS?) silver bullet solution that delivers all needed capabilities in an integrated package. Security teams will leverage some currently deployed products as core components of the ZT framework, will phase out others, and will add some new products to address key ZT requirements. Each business will chart its own path across these categories, driven by its current maturity levels, technology environments, key ZT focus areas, timeframes, and available budget.

Some areas of need are common to all businesses. Stratascale's SMEs identified a total of 33 technologies, capabilities, and related management imperatives that combine to create a robust and resilient approach to security within the ZT pillars.



Source: Stratascale 2022

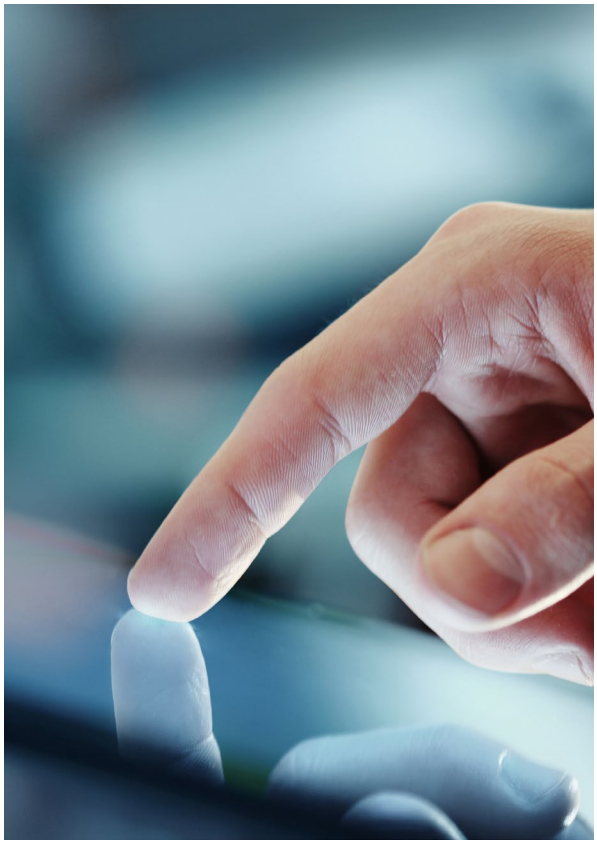
Identity

Much of ZT strategy focuses on the two ends of the pillar diagram above: protecting sensitive data and other intellectual property (IP) – the overriding objective of zero trust – and managing identities to govern access to that IP. One member of the thought leadership group stated that their strategy centered on "three pillars: identity, network, data," adding that they addressed "identity first" to both establish effective access controls and to establish "frictionless" approaches to optimize user experience.

In discussing essential zero trust technologies, Stratascale's SMEs honed-in on four key areas: continuous strong authentication, passwordless authentication, risk-based access and authorization policies, and device identities.

Continuous strong authentication

This category might come with a "start here!" sticker. Zero standing privileges (ZSP)/just-in-time (JIT) access represents a compelling immediate priority for CISOs pressured to show immediate progress. Moving to ZSP/JIT access from more basic privilege access management (PAM) tools aligns identity with ZT objectives by removing "admin user" privileges from the identity equation. Admin users exist only when they are needed and are temporarily created for a specific purpose. Eliminating standing admin users addresses a key source of identity-related risk.



Passwordless

The chart illustrating a sample ZT implementation plan shows passwordless as a second-stage identity technology, with rollout targeted for many months after completion of the ZSP deployment. However, this doesn't mean that passwordless is unimportant to zero trust success. One CISO contributing to this document is focused on passwordless because it is important to "that frictionless access culture," "meeting users where they live," and building identity and security on technologies, such as smartphone biometrics, which users employ in other areas of their lives.[2]

Risk-based access and authorization policies

Adaptive and conditional risk-based access policies address a critical issue in cybersecurity: what do you do to mitigate exposure in the event that a device (or user) is compromised while they are accessing a sensitive resource? Adaptive, conditional access helps to identify scenarios where this may have occurred and restricts access and authorization unless and until it is possible to re-establish trust in the user or device.

[2]For more on passwordless and its advantages in terms of recruitment and retention, see the "Security as a source of differentiation and competitive balance" section in *Zero Trust Interest and Investment Drivers*.

Device identities

Despite the name, device identities fit within the identity pillar rather than the device pillar. Security teams need to establish threat and posture management on devices – particularly as those devices move away from 1:1 connections with human users. Clearly, threat and posture management is important for IoT devices. But implementing device identities extends to firms that have not deployed IoT. Servers, for example, access sensitive resources as a matter of course, and these connections, too, need to be monitored as part of ZT identity.

This is a difficult area to address. One Stratascale SME observed that "everybody is horrible at device identities" and added that "most organizations aren't anywhere near" a point where they can "get their hands around machine identities." Although this is an important objective, if the security team can't identify devices that are accessing resources, they can't make good risk-based decisions on whether any given access request should be allowed or whether it represents an emerging threat within the corporate environment.

Other ZT identity considerations

Additional considerations around identity surfaced during discussions with our thought leadership group, including:

- **"Moving toward a B2C infrastructure for our [multi-factor authentication] MFA platform."**
  - This CISO stated that as the security team opens up the MFA platform to third parties, "[people in] our business get very nervous. We have [supply chain partners] and trying to move them onto a different kind of credential store makes them nervous. But then you walk them through how much easier it is to register" if you apply an intelligent help function that can lead users through the process. This provides a resource-efficient means of safely connecting external users to corporate assets.
    - This discussion speaks to agility gains that can be realized through implementation of better technology. In this case, identity, but the concept could apply to any other ZT pillar. In a broader context, this example argues for a need to layer in capabilities incrementally. A "big splash" might improve capabilities in one area but create issues for current or future systems in another. An important part of ZT is the ability to align new capabilities within a comprehensive framework.
- **Bring your own identity (BYOI)**
  - BYOI can enable "differentiated access to corporate systems…segmentation that differentiates between external users [supply chain partners accessing systems via BYOI – which uses externally managed identities] and internal users [with corporate credentials]."
    - BYOI offers security leaders two primary benefits. One is that it transfers the effort associated with identity maintenance outside the organization, reducing staff commitments. The other, stated in the quote, is that BYOI access provides an inherent basis for segmentation, allowing the security team to identify external users accessing corporate systems and assign them appropriate access and authorization.

- Incremental, non-binary identity signals
  - One thought leadership group member urged security teams to use multiple methods to reaffirm identity on an ongoing basis. By assessing the user's context as it changes, the argument holds that it is possible to use "non-obnoxious methods" to monitor user sessions. The goal is to capitalize on approaches that are "silent or easy to do with biometrics on device [or other options] to refresh." If a session ends because the user logged out or timed out, "you can reauthorize, but you don't have to impose the same [authorization method(s)] – if they're just doing something read-only versus read/write or whatever it is, you could just [apply complementary, potentially unintrusive methods] as much as you want."
    - This sounds amorphous, but there is a great deal of potential in this notion of regular reification of identity via non-obtrusive telemetry or other inputs, as compared with highly intrusive requests for passwords or similar means.

Devices

Devices are a complex category in a ZT framework. Most businesspeople intuitively include corporate-issued PCs, tablets, and smartphones under the "devices" heading, but security professionals also need to consider third-party user devices – both bring your own device (BYOD) and units used by customers or supply chain partners to interact with corporate assets – as well as company-owned and third-party access points, IoT devices, and infrastructure components, such as servers, switches, and even software. In the ZT world, a device is any entity that is looking for access to resources. Each represents a potential point of vulnerability, and each needs to be wrapped into the ZT framework.

Stratascale's SMEs emphasized the need to build sound management capabilities: device inventories/device asset management, device hygiene and posture, and endpoint protection.

Device inventories/device asset management

The first step in ZT devices is to understand what devices need to be protected. "Device inventories, device asset management, unified device management (UDM), enterprise device management (EDM), IT asset management (ITAM), or whatever you want to call it" – there are multiple terms used to describe the ability to track and manage devices. At a foundation level, ZT requires that the security function be able to identify each device that might access corporate resources, answering questions, such as:

- "What user devices do we have in use today – company-owned, BYOD, other human-controlled devices that access our network and resources?
- What IoT or other devices that are not assigned to a human user have access to our network?
- What BYOD devices are we supporting?
- Where is each of these devices?
- Which devices have we retired?
- Do we have proof that they've been destroyed?"

The important thing here is to be as comprehensive as possible, including both corporate and personal devices and maintaining currency over time via proactive additions and deletions from the inventory/register.

Device hygiene and posture

Device hygiene refers to the ability to understand the current status of a device and whether basic security steps have been taken to protect it. The phrase covers a range of factors, including core device attributes (company-owned or personal device? locked down or "jailbroken?"), status (properly patched? accessing the environment via a virtual private network (VPN)?), and the ability to receive and analyze signals and telemetry that support analysis of risk associated with the device. At a higher level, device hygiene can be viewed as referencing the core attributes that comprise device compliance and risk state – ensuring that the device meets defined corporate standards and policies.

Endpoint protection

Endpoint protection goes by several names, including endpoint detection and response (EDR) and endpoint protection platform (EPP). Although some specific differences can be argued across these terms, the general sense of securing the device is common to each –an essential component of a ZT devices strategy. Endpoint protection hardens connected devices against attack by connecting related capabilities: predict, based on threat intelligence and pattern analysis, when an endpoint might be compromised; prevent compromise, if possible; and detect and respond to compromises when they occur. These systems are often delivered via cloud-based platforms that support ubiquitous connections and real-time updates. Effective endpoint protection should connect seamlessly with other ZT pillars – for example, ZT network technologies – to enable anytime/anywhere user access while enforcing ZT access standards consistently across human-controlled and non-human devices.

Network

Network plays a unique role in the shift from traditional perimeter-based security strategies to zero trust. On the one hand, the network itself moves from being the primary focus of security activity to one of six interrelated pillars, and this loss of primacy can be difficult to absorb for legacy network-centric security professionals and organizations. On the other hand, the network is central to critical ZT security functions and to delivering on the foundational requirements highlighted in the "ZT Strategic Technology/Management Priorities" graphic. "De-perimeterization," a concept espoused by the Jericho Forum (which first advanced key ZT principles), may be the basis for zero trust, but ZT network plays an essential role in establishing ZT as a functional strategy.

In a discussion of technologies that are needed for zero trust success, Stratascale security SMEs highlighted four key issues: microsegmentation, encryption, visibility, and VPN replacement/next-generation remote access.

Microsegmentation

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.

Microsegmentation (not exactly as pictured)

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 that have 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 the alignment of defenses with sensitive data and high-value corporate IP.

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, etc.) or via a software proxy. It should be noted that while this approach satisfies the need to encrypt "north side" data – for example, e-commerce communications between a facility and a customer – it may not always encrypt "south side" data – internal traffic (within a corporate data center or the cloud) may still be clear text.

Visibility

"Visibility" is a complicated topic in zero trust. As the graphic above shows, 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 so that they can take action to prevent attacks from expanding within the corporate environment and can issue appropriate intelligence to other pillars as required.

VPN replacement/next-generation remote access

The pandemic exposed a fundamental flaw in VPN-centric remote access strategies. With the already-underway-but-significantly-accelerated migration of workloads to the cloud, 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 (SDP), 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.

Infrastructure

Infrastructure is sometimes overlooked as a necessary component of a zero trust strategy, but it poses an evolving series of challenges for CISOs. Contemporary infrastructure often centers on outside-the-corporate-perimeter cloud resources, which challenges security leaders tasked with establishing a resilient environment delivering confidentiality, integrity, and availability.

While discussing ZT infrastructure technologies and management imperatives, one contributing expert noted that "network and infrastructure are foundational, but those other pieces are what the adversaries are after." Attention may accordingly be drawn to the bookends of identity and data, and their adjacent pillars (devices and applications), but ZT strategies need to also address these core, foundational system elements. To respond to this requirement, Stratascale SMEs urge ZT infrastructure planners to ensure that they have current and accurate CMDBs, configuration management, cloud workload protection platforms (CWPP), cloud infrastructure entitlements management (CIEM), and physical infrastructure access management.

Configuration Management Database (CMDB)

CMDB is seen as a non-negotiable starting point for ZT infrastructure. As one contributor said, "You'd better have a list of all of your servers, all of your domain name system (DNS) services, your domain controllers, directory services, your services in Azure and AWS…You can't function without it."

Configuration management

Stratascale's SMEs emphasized that configuration management, separate from the CMDB, is also a crucial capability to operate within a ZT framework. Configuration management enables security teams and their IT counterparts to establish system hygiene: for example, to ensure that systems have an approved operating system, approved EDR (extended detection and response) protection, and systems that are connected to the correct subnet. Configuration management provides an important ZT infrastructure control.

Cloud Workload Protection Platform (CWPP)

Cloud workload protection touches on both infrastructure and application security, stretching across two ZT pillars. Infrastructure and applications are tightly coupled, and application monitoring is important to each area. CWPP, which protects workloads as they move from one cloud environment to another, is positioned within infrastructure because it provides a critical monitoring capability to organizations that need to ensure that functions or applications based in the cloud can support complex processes – those involving extensive interactions between separate applications or software functions and associated data – without introducing vulnerabilities.

Cloud Infrastructure Entitlements Management (CIEM)

Cloud infrastructure entitlements management – "the other CIEM (SIEM)" – is an important tool in the ZT infrastructure management toolkit. One of the complicating factors with hybrid delivery platforms is that access rights may be defined inconsistently by different suppliers and may not align with internal controls. CIEM gives ZT infrastructure management insight into areas that might not be visible in tools that tie to specific environments.

Applications

Applications are the focus of a great deal of attention within ZT and cybersecurity strategy as a whole. Applications – especially proprietary applications that help an organization build competitive advantage – represent critical IP and need to be protected via the ZT framework.

Applications also represent the point at which security is visible to the business as a whole because all internal users (and in many organizations, external users such as suppliers, customers, and other stakeholders) rely on applications to access and work with needed data. This visibility significantly raises the stakes for the security organization.

Users who find security measures overly restrictive will look for (shadow IT) workarounds, increasing overall organizational IT costs and decreasing visibility into potential vulnerabilities and threats. Measures that imperil critical business processes – for example, a security control that ends up preventing a single quarter-end deal from being processed – will destroy months' worth of goodwill generated by frictionless ZT security approaches.

A second complicating factor with applications is that they tend to enter the organization from two distinctly different sources. Every major business uses a mix of commercial off-the-shelf software (COTS) and internally developed software, which, in today's industry, is the product of a DevOps "software supply chain." Security professionals need to deploy technologies and management practices that are capable of addressing both COTS and internally developed applications.

After considering these factors, Stratascale SMEs identified seven critical ZT application capabilities and technologies:

- Application inventory
- Least privilege access to data
- Application workload monitoring
- Application data flow mapping and dependency mapping
- Secrets management
- API gateways
- User experience

Application inventory

As is the case with devices and infrastructure, step one in a ZT application strategy is discovering and classifying the software present within your internal and extended (external) environments. This is a challenging objective, but "there are tools that will fingerprint your network and inventory the apps that are running."

This inventory provides a basis for implementing ZT applications within a corporate environment, "because if you put new apps up and you don't know what's out there and [the application is] serving data up, how am I going to apply policies and controls to it? How am I going to decide what network zone to put it into? How am I going to know what version it is or what open source software it has within it that needs to be patched?"

Least privilege access to data

This is an extension of a concept raised in the identity pillar, but it applies to ZT applications as well. By their nature, software systems access data in ways that are opaque to users – and to many security professionals. Using technology and policies to establish a principle of least privilege (PoLP) for application data access can avert lateral intrusions that start with a compromised application and burrow into sensitive data sources.

Application workload monitoring

Workload monitoring is "where you are going to catch a lot of anomalies. Wait a minute! Suddenly, this application is downloading two terabytes of data and making 3,000 calls." An unexpected spike in access or connections can be a critical, real-time flag highlighting a compromised application.

Application data flow mapping and dependency mapping

The issue of mapping data flows, or the broader constellation of application dependencies, arises in many ZT-focused conversations. If ZT is intended to allow only applications that require specific data to gain access to it and allow data access only to authorized applications, the security team needs to have a clear idea of the interdependencies between applications and the data that they input or output.

Application data flow and dependency mapping in a major corporation are complex. Large enterprises cannot tackle data flow and dependency mapping manually. They need tools to automate this process, understand (on a current, continuous basis) and inventory which connections must be permitted, and enable automated blocking of non-permitted connections.

Secrets management

The basis of trusted connections between applications is "secrets" – credentials that allow applications to connect securely. Seamless connections between applications are critical to supporting business processes that span multiple software systems or functions – which means that an effective, programmatic approach to secrets management is critical to supporting a digital business environment, across both COTS and internally developed software.

API gateway

API traffic represents an enormous subset of total traffic and potential vulnerability for the businesses that use APIs to connect applications. It is essential that API traffic be managed effectively and consistently. As one contributor to this document noted, "You shouldn't be running APIs out of every single application. You should have an API gateway implemented where you're making calls and every app is using the same API call" – and not coding APIs for common applications like Salesforce into every application that feeds into or takes data from the CRM system. An API gateway provides a single point to control API calls, across both COTS and internally developed software.

User experience

As a category, user experience brings this discussion back to the beginning of the application section, which noted that "users who find security measures overly restrictive will look for (shadow IT) workarounds," adding that "measures that derail critical business processes" will destroy goodwill that takes the security function months to establish.

User experience with ZT applications doesn't rely solely on software itself: burdensome MFA requests disrupt users, and inadequate or unavailable network or infrastructure resources may result in intolerably slow performance. But regardless of the source, users will point fingers at the application that is associated with the poor experience and will seek ways – prominently, unauthorized alternatives to sanctioned applications or platforms – to obtain a better experience. UX may not be a ZT application issue per se, but it creates conditions that lead to security problems that impact the success of the ZT strategy. To ensure success, technology leaders implementing ZT strategies must ensure that user experience is not degraded by their programs.

Data

Data is seen as the "focal point" or objective of zero trust strategies, which makes data protection a primary objective. The notion that data is the objective that drives both attackers and ZT defenses permeated all discussions that fed into this Executive Guide to Zero Trust research series. Many of the technologies and management practices used in ZT data overlap to some extent with measures taken in other pillars (or with each other), but after considering the issue, Stratascale SMEs highlighted 10 ZT data areas that require attention from security leaders.

Data governance

Data governance functions as a capstone consideration for ZT data. Broadly speaking, enterprise data governance policies have been stretched to the point of fraying by the exponential growth in data, data sources, data users, and data use cases: it is increasingly difficult to maintain governance policies that mandate effective data protection practices across all possible scenarios.

ZT data leaders, though, should view data governance as a means of connecting the many ZT data technologies and practices – and related technologies and practices from other pillars – with corporate business objectives and regulatory requirements. This is (or should be) a symbiotic relationship. ZT data initiatives gain credibility from their connection to governance mandates; at the same time, as one CISO contributing to this research observed, a clear and measured implementation of ZT "speaks to the maturity" of the security practice as a whole and helps reduce the time needed for review and audit.

Data discovery and classification

Research contributors saw the data inventory as essential to an effective ZT program. Organizations beginning on their ZT journey must create a data inventory as a foundational step: You "can't do ZT without that." In this pillar, though, building inventories is predicated on multiple capabilities. One is that this process starts with data discovery. With data not fully captured in existing registries, but instead, accumulated within organizational silos, in cloud-based (SaaS) applications, or on individual hard drives, effective and automated discovery tools are essential to creating a data inventory.

The second key capability concerns data classification. Data requires stewardship and governance. Sensitive personal data needs to be managed according to policies that will stand up to regulatory scrutiny and protect the organization from fines or reputational damage. Corporate IP needs to be defended against commercially (or in some cases, politically) motivated intrusions. Other data – including outputs from applications based in various locations, which may be accessing or synthesizing sensitive records – needs to be appropriately classified and monitored on an ongoing basis.

One member of the zero trust thought leadership group positioned the data inventory challenges in the context of inventories in other ZT pillars. User inventories or identity inventories, the contributor stated, can be assembled from existing tools. "Device inventories are a little harder, but still kind of easy," as "enterprises have device management platforms that enable staff to identify devices, their posture, and how they relate to identities." But there isn't an analogous source for insight into where data is and which data is most critical from a confidentiality (and security) perspective. "Data inventories are always the hardest," the contributor believed – and as a result, there is a tendency to "put all these roadblocks and bubbles and firewalls and access control rules around the data."

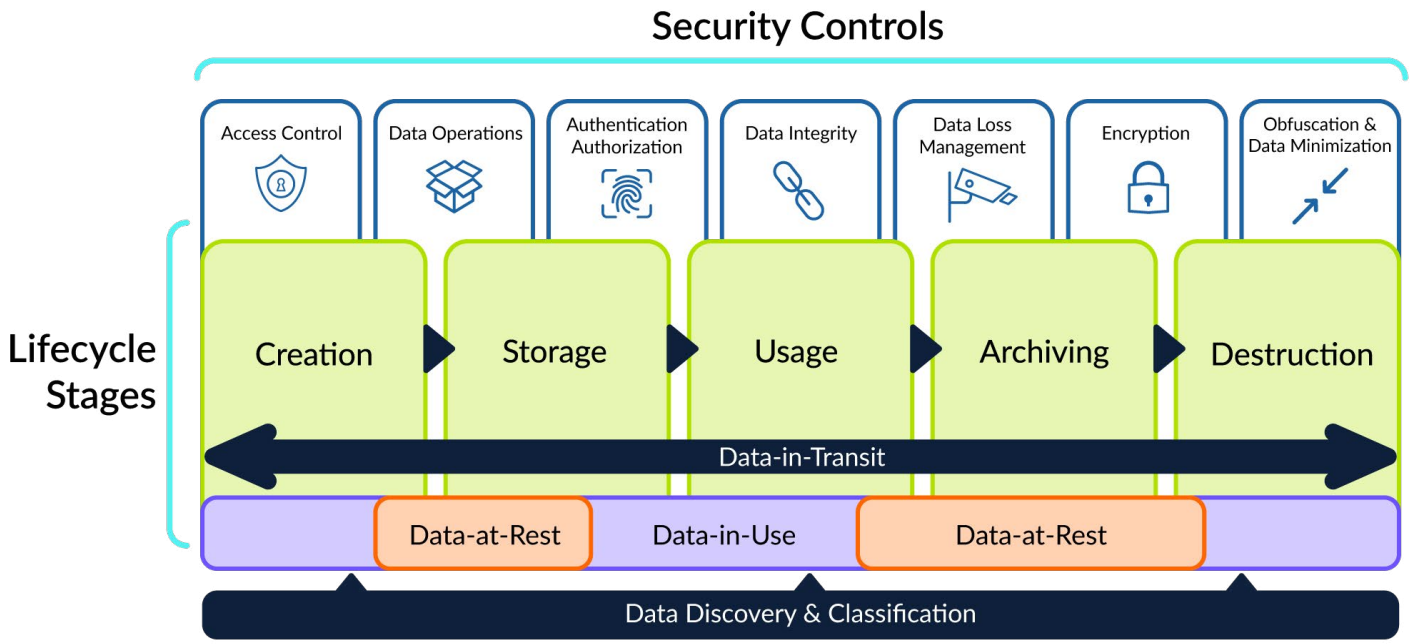
Absent a current and detailed data inventory, security leaders may default to these generalized controls. This approach is the antithesis of the zero trust intention: CISOs need to identify the locations and criticality of corporate IP in order to implement data access control and focus protection on data assets.

Data inventory/catalog

This category is intrinsically linked to discovery and classification: discovery finds data, classification defines its significance, and then inventory and catalog add a centralized organization of the data, enabling it to be understood, consumed, and managed.

Data lineage

Data lineage enables understanding of the data lifecycle, including the point at which data must be archived or destroyed. Organizations tend to be far better at creating and aggregating data than deleting data that should no longer be stored – but data destruction is an important aspect of data security. Data lineage is critical to guiding decisions about data management, including data archiving and destruction.



Source: Stratascale 2022

Data access control

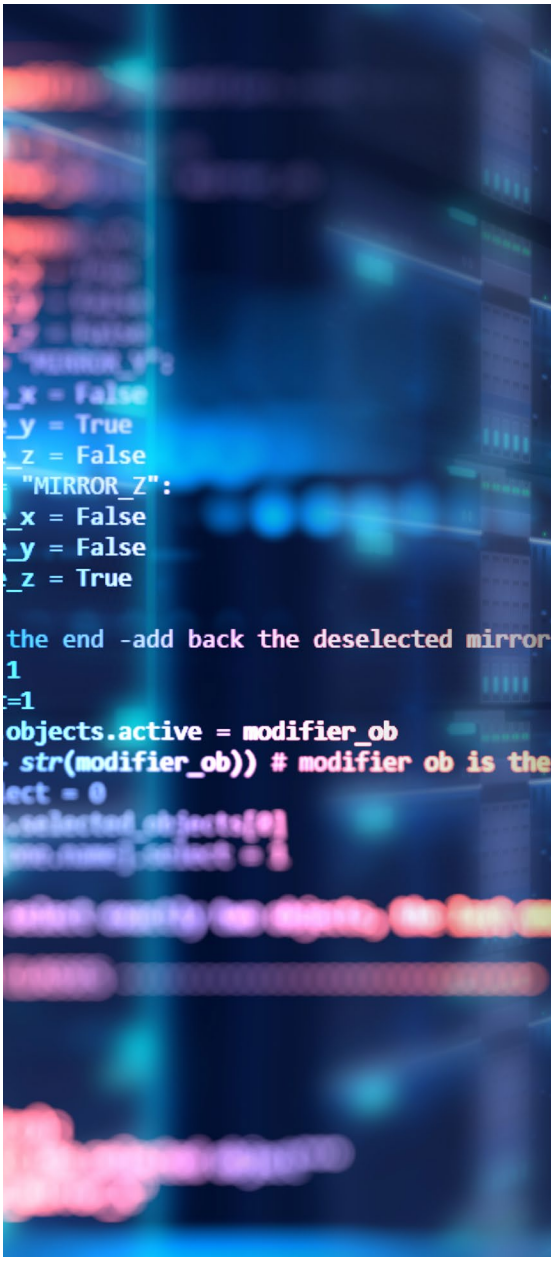
Data access control isn't a technology category per se but is one of several phrases that could be applied to systems and practices that align data access and authorization with policy and governance. The objective is to ensure that access to data is gated based on identity and is informed by the sensitivity and criticality of the data, which assumes a necessary prerequisite focus on data classification.

This seems an appropriate juncture to emphasize that access requests may come from human or non-human (e.g., IoT) users. The ability to classify these identities and devices, which relies on success in the identity and access pillars, is important to successfully managing access to data. Within the data pillar, information on identities and devices is mapped to the data inventory and used to limit data access, reducing the potential for a compromised device to harvest data that isn't logically connected to the user or device function.

Data encryption

Data encryption is (or ought to be) standard practice for security teams. It is fundamental to ZT data – protecting data that resides in storage or is "in flight" from one device, application, or user to another is a hygiene-level step in the ZT process.

Surprisingly, there are environments where security professionals eschew encryption of data in motion. Such practitioners believe that VLANs, segmentation, and other measures provide adequate protection for unencrypted data, rendering encryption in motion superfluous. SMEs contributing to this report vehemently disagree. There are many attacks (including router compromise, spam forwards, attacks on load balancers or application servers, etc.) that can open a window into traffic – and if that traffic is unencrypted, it provides a clear view of the data itself. Data encryption, including encryption in transit, is critical to ZT data success.



Test data management

"Test data management" doesn't generally leap to mind when data security is raised as an issue. But as one CISO contributing to this document noted, "test data is a critical, thorny issue. You need data isolation. You can have a good [test] strategy and good tools with an ecosystem comprised of knowledgeable people that can manage the process – DBAs and business professionals. But who can manage the data obfuscation?"

Again, "data obfuscation" is rarely priority #1 for security leaders. But in some contexts – notably, when the ultimate system will deal with PCI or other regulated data – it is very important. "You're not going live with the system that's never been production tested, right?"

In many corporations, there will be multiple systems under development that will process sensitive, confidential, and/or regulated data when they are in production – which means that there is a need to support multiple test environments. The CISO concluded by saying that this is "a very solvable problem on paper, but it's challenging to build up to that level of maturity."

Data loss prevention

Data loss prevention (DLP) is a mature technology – meaning that it is likely deployed in most organizations that are pursuing a zero trust strategy – but there is a need to ensure that DLP products and policies are consistent and integrated with ZT data and organizational ZT framework priorities. Key attributes of DLP, including visibility into the data and the ability to deploy consistent policies that map data access to device posture, are important to overall ZT data capabilities. Other ZT functions and technologies may ingest DLP outputs, such as warnings about potential exposure of sensitive data. By providing visibility into how data is used and moves and enforcing security policies that respond to content and context, DLP supports the overall ZT data strategy.

Data backup and recovery

With the huge increase in the use of cloud-based resources adding to the strains imposed by business unit data stores and files resident on local hard drives, IT organizations have needed to revamp backup and recovery approaches and tooling. The security team plays a critical role in shaping this strategy, since security issues – ransomware protection, support for audit, and compliance – feed into the backup and recovery strategy. Security leaders may also be accountable (to some degree) for Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO), which further connect data backup and recovery to the ZT framework.

Data privacy

Data privacy is more an imperative than a defined toolkit, but it is "becoming a nightmare" for security leaders and can't be overlooked. Data privacy builds off discovery and classification and the data catalog, referencing the need to govern how sensitive data is collected, tracked, used, and shared. Data privacy ensures the confidentiality of sensitive data (such as personally identifiable information (PII) or protected health information (PHI)) – objectives that are intrinsic to data governance mandates.

Foundational requirements

The 33 technologies and activity areas identified above are intended to help CISOs plot an incremental path that enables continuous progress within each pillar. There is a separate class of capabilities, shown in the diagram as "foundational requirements" that are essential to ZT success across pillars. These include:

- Visibility and analytics: Visibility is highlighted in the network section of this report as both a network-specific focus area and as a foundational requirement. Network visibility is a critical aspect of a ZT network, providing organization-wide input that supports understanding of the current state of enterprise security. At a foundational level, security teams need visibility into vulnerabilities and attack sources, and this insight enables teams to prioritize and respond to threats to identities, devices, the network, applications, and data. CISOs rely on the network both for proactive and reactive management actions within the ZT framework. The sheer volume of this data is overwhelming – which means that CISOs will position analytics as a core component of ZT visibility, using AI or other intelligent systems to prioritize issues that require attention or highlight areas that degrade the readiness of the overall corporate security posture.
- Automation and orchestration: Stratascale believes that a key strength of the ZT pillar approach is its ability to connect diverse capabilities to focus protection on a business's most critical assets. But to combine capabilities and escalate issues to the appropriate resource, security organizations must establish effective procedures for integrating defenses within each pillar and connecting insights and capabilities across pillars. Security teams cannot rely on manual processes given the complexity associated with each task and with the broader systems. To be successful, organizations need to automate each discrete area as fully as is feasible and then orchestrate the exchange of information and notifications across areas.
- Interoperability and integration: The idea that zero trust is an incremental, organization-wide approach to securing critical assets is predicated on the belief that ZT components must function seamlessly together. This has a meaningful implication for vendor and product selection: a best-of-breed product will not improve the overall ZT framework if it can't integrate and interoperate with other products within its pillar or requires orchestration across pillars.

By establishing organizational competencies in these areas – through effective management frameworks and use of technologies, such as extended detection and response (XDR), which enables organizations to automate orchestration – CISOs will have the operational tools and practices needed to meld ZT capabilities into a whole-organization protection approach greater than the sum of its parts.

Working with this content

CISOs looking to integrate this perspective on key zero trust technologies to inform their ZT strategies are encouraged to consider the following takeaways:

- Progress in ZT can't be defined in terms of progress in a single pillar or across two of the six ZT focus areas. CISOs need to balance investments across pillars to ensure that progress isn't over-concentrated in one area while another lacks effective defense options.
- Similarly, progress isn't always best attained by addressing the most evident source of vulnerability. CISOs need to weigh the practical daily and worst-case scenarios before allocating funds to a particular investment area. Vulnerability, the value of the asset being protected, and the frequency with which that vulnerability is being probed or attacked, all factor into the prioritization of ZT attention. One contributor to this document cited research showing that "if there is a very sensitive asset that has a vulnerability, but there's no exploitation of it – and there are other, medium-sensitivity assets that are being exploited – the best approach is to remediate those medium-level sensitivity assets because there's active exploitation of a vulnerability." CISOs who have deployed the technologies and practices described in this document will have a great deal of intelligence about risks and threats and will be able to make informed prioritization decisions that combine ZT strategy with solid intelligence and response capabilities.
- Stratascale's ZT research has identified "incrementalism" – the process of viewing ZT as "an incremental journey rooted in existing technologies and processes" – as a key consideration in defining a ZT roadmap. As another document in this series[3] observes, "ZT doesn't demand that CISOs unplug their current infrastructure in favor of new and different technology. It is a concept holding that a long-term strategy for reorienting security focus from the perimeter to identity/access and data can be articulated in a framework of capabilities needed across six core pillars and realized through a 'continuous journey' that emphasizes or reinforces relevant current technologies and processes, adds new resources where needed, and allows for the removal of unneeded tools." This document provides ZT strategy leaders with a view of key technologies, capabilities, and management imperatives that define the ZT framework, enabling CISOs to evaluate the depth of current capabilities in all relevant areas and to prioritize investments across the ZT journey.

[3] "Incrementalism" in *The Zero Trust Rollout Notebook*.

This is the fifth of eight source documents included in Stratascale's "An Executive Guide to Zero Trust" research series. We will also publish a capstone report connecting these eight pieces, plus a six-part companion series ("The Technical Manager's Guide to Zero Trust") and several compilations and ancillary documents and tools.

Readers interested in specific executive-level perspectives on zero trust may wish to explore the other reports in this series:

- *Defining Zero Trust*
- *Zero Trust Sponsorship and Commitment*
- *Zero Trust Interest and Investment Drivers*
- *Zero Trust Business Objectives*
- *The Zero Trust Rollout Notebook*
- *The Path to Zero Trust*
- *Zero Trust Metrics*
- *The Executive Guide to Zero Trust: Drivers, Objectives, and Strategic Considerations (capstone report)*
- *The Executive Guide to Zero Trust: Drivers, Objectives, and Strategic Considerations (eook consolidating all nine reports)*
- *Stratascale Zero Trust Metrics in Context and Action tool (Stratascale ZT-MICA) (downloadable tool – no cost, registration required)*

Zero Trust Thought Leadership Members

Geeta Kapoor

VP Information Security, MSC Industrial Supply Co.

Geeta is vice president of Information Security for MSC Industrial Supply, North America's leading distributor of metalworking and maintenance, repair, and operations (MRO) products and services. Prior to joining MSC in 2022, Geeta was responsible for developing and executing the security strategy to reduce overall cyber risks for Beaumont Health, Michigan's largest healthcare system.

Previously, she served in a variety of roles covering network management, cybersecurity engineering and architecture, identity and access management, and monitoring and incident response, as well as governance, risk, and compliance. Geeta can be found on LinkedIn here.

Noah Davis

Director, Cybersecurity Operations & Incident Response, Tran Technologies

Noah is an internationally experienced, results-driven technologist for IT compliance, cybersecurity, and operations within Fortune 500 diversified manufacturing. Noah has established himself by successfully partnering IT with business, streamlining operations, and reducing cost. He brings over 20 years of experience across multiple IT disciplines.

As the director of Cybersecurity Operations at Trane Technologies, Noah is responsible for all global detection and response activities to protect the organization from the continually expanding cybersecurity threat landscape. Noah can be found on LinkedIn here.

Leon Ravenna

Chief Information Security Officer & Chief Information Officers, KAR Global

Leon is a passionate information technology and security executive focusing on system availability, data protection, and privacy of information assets, as well as on technology innovation, mentoring, and personnel development. He has more than 30 years of experience in healthcare, financial services, and technology companies.

Leon is the chief security and information officer at KAR Global, a leading operator of digital marketplaces for wholesale used vehicles and a financial services company. He leads global security strategy, privacy, and compliance for over 5,000 employees. Leon is one of only a few experts worldwide to hold six major global privacy certifications. Leon can be found on LinkedIn here.

Barney Baldwin

Lecturer, Columbia University

Barney has directed risk technologies for many of the world's leading financial institutions. Over his career, he's served as executive director for UBS, CTO for KBC Financial Products, and global head of Risk Technology for RBC Capital Markets. His most recent corporate role was as a managing director for Risk and Security Technology at MUFG (Mitsubishi UFJ Financial Group).

Upon retiring from MUFG, Barney started a new role as a lecturer at Columbia University, where he developed a course on Risk Technology. Barney can be found on LinkedIn here.

Chase Cunningham

Chief Strategy Officer, Ericom; host of the DrZeroTrust podcast

Chase is a retired U.S. Navy chief cryptologist with more than 20 years of experience in cyber forensic and analytic operations. He gained his experience from real-world operations supporting offensive and defensive cyber operations in work centers for the NSA, CIA, FBI, and other government agencies.

Currently, Chase is the chief strategy officer for Ericom Software, a leading provider of zero trust secure access solutions that protect organizations from advanced cybersecurity threats. He is also a published author and host of the popular DrZeroTrust podcast. Chase can be found on LinkedIn here.

Eve Maler

Chief Technology Officer at ForgeRock

CTO of ForgeRock, Eve is a globally recognized strategist, innovator, and communicator on digital identity, security, privacy, and consent, with a passion for fostering successful ecosystems and individual empowerment. Eve has over 20 years of experience innovating and leading standards, such as SAML and User-Managed Access (UMA), and has served as a Forrester Research security and risk analyst. Eve leads the ForgeRock Labs team, investigating and prototyping innovative approaches to customers' identity challenges. She also heads ForgeRock's industry standards leadership. Eve can be found on LinkedIn here.

Sean Frazier

Federal CSO, Okta Inc.

Currently the federal CSO at Okta, Sean spent over 25 years working in technology and public-sector security for companies such as Duo Security, Netscape, LoudCloud/Opsware, Proofpoint, Cisco, and MobileIron.

He has helped lead numerous projects used by the Department of Defense and the intelligence community, including the Fortezza Crypto Card and the Defense Messaging System (DMS). He also has extensive experience in identity and public key infrastructure (PKI), network, applications, mobile, and IoT. Sean advises public/private partnership working groups, including ACT-IAC, ATARC, and many others. Sean can be found on LinkedIn here.

Contributors

Michael O'Neil

Lead Research Analyst – Cybersecurity

A frequent keynote speaker, author of several books, and hundreds of reports, Michael is one of the world's most accomplished IT industry analysts. He brings to Stratascale's cybersecurity business a multi-faceted understanding of how IT functions in a business context, as well as the ubiquitous requirement for effective security practices. Follow Michael on LinkedIn.

Joseph Karpenko

Lead Technical Advisor – Cybersecurity

Joe leads Stratascale's technical client security and risk strategy conversations. Using practical experience and insights, he provides guidance from market analysis and assessments focused on business, technical, and use case intelligence. Follow Joseph on LinkedIn.

Rob Forbes

Director of Zero Trust and Identity Services

Rob has over 30 years of information technology experience working with Fortune 500, Global 1000, and government organizations focusing on information/cyber security to establish and run successful security programs. His broad background allows him to excel in a variety of roles, including individual contributor, SME, manager, and director. Rob possesses practical experience in cloud environments, containerization, DevSecOps, networking, Windows/Linux-UNIX/Mainframe system administration, database administration, business continuity planning, managing support and operations groups, as well as strategic and tactical planning. His extensive, hands-on experience in various IT specializations provides a superior foundation for his security expertise.

Alex Banghart

Researcher - Cybersecurity

Alex is a cyber security researcher at Stratascale. A background in both research and practical security experience allows Alex to provide a unique perspective on security with a risk-based approach. He uses his experience to focus on emerging technologies, data-driven IT strategy, and tactical solutions to large security problems.

Michael Wilcox

VP – Office of the CISO

Michael Wilcox has more than 20 years of experience providing IT Security Leadership across a comprehensive portfolio of security environments. He has developed programs and centers of excellence for IT Security services, including forensics, incident response, education and awareness programs, vulnerability assessments, penetration testing, data loss prevention, enterprise information security architecture, compliance, encryption, identity and access management, and disaster recovery. Michael has held CISO roles for a global Fortune 300 manufacturing company and the largest non-profit organization for cancer research. He holds a Bachelor of Science in Information Technology/ Information Systems Security and maintains various IT certifications including CISSP, CISM, Security+, Project+, and ITILv3f. Michael is a peer and advisor to Stratascale's executive-level cyber leaders.