DOI:10.1145/3573127

Article development led by acmqueue
queue.acm.org

BY MATTHEW BUSH AND ATEFEH MASHATAN

From Zero to 100

Demystifying zero trust and its implications on enterprise people, process, and technology.

CHANGING NETWORK LANDSCAPES and rising security threats have imparted a sense of urgency for new approaches to security. Zero trust has been proposed as a solution to these problems, but some regard it as a marketing tool to sell existing best practices while others praise it as a new cybersecurity standard. This article discusses the history and development of zero trust and why the changing threat landscape has led to a new discourse in cybersecurity. Drivers, barriers, and business implications of zero trust provide a backdrop for a brief overview of key logical components of a zero trust architecture and implementation challenges.

In recent years, attackers have sown the seeds to feed a growing awareness of the flaws in common cybersecurity practices. Firewalls were applied to create a strong perimeter around enterprise networks; however, once inside the perimeter, an attacker can easily move through a company's intranet. With the increasing adoption of mobile and cloud technologies, a singular perimeter is becoming more difficult to enforce. With new attack vectors and technological changes, perimeter-based security models are moving toward obsolescence.

Despite the prevailing attitude that most threats are external, the source of attacks is approximately even between external attackers and insiders.[1] Insiders and supposedly trusted devices have become a serious cause for concern. Network access is being spread out among mobile devices, cloud users, employees working from home, and Internet of Things (IoT) devices. According to Cisco's 2018 Annual Cybersecurity Report, the scope of attacks is also increasing. Organizations reported a growing trend of security breaches that affected more than 50% of systems.[4] Larger breaches means larger sums of money are required to handle the aftermath. Security directly affects the bottom line, and high-level decision-makers need to take notice.

The approach wherein security teams have little input regarding high-level business decisions is outdated. The 2017 Equifax disaster, for example, forced the CEO, CIO, and CISO to resign. Capital One, a massive player in the U.S. financial industry, experienced a similar situation in 2019 with more than 100 million accounts compromised, followed by a huge class-action lawsuit.[5] The scale of cyberattacks, breaches, and privacy violations is getting larger and becoming increasingly visible to the public. Many organizations desperately need to improve their approach to cybersecurity, or this problem will only get worse.

Amid this changing cybersecurity landscape, zero trust has been lauded as a potential solution to many of these problems. With all the hype, though, many are unsure about what

IMAGE BY ALICIA KUBISTA/ANDRIJ BORYS ASSOCIATES


ZERO
TRUST
bersecur
irewalls

the term exactly means and how to implement it. Where did the concept of zero trust come from, and what does it mean for businesses today? Is zero trust a new standard or just cybersecurity done properly?

De-Perimeterization and Zero Trust

The core ideas behind zero trust were first given major consideration in 2004. The Jericho Forum recognized that traditional security practices were quickly becoming inadequate because of increasing numbers of endpoints and device mobility requirements.[3] Firewalls, antivirus, and intrusion detection system (IDS) did not consider the threat from within the network. The initial term used was *de-perimeterization*, which focused on strengthening internal defenses and placing less emphasis on the external boundary. In 2007, the Jericho Forum published "commandments" that outlined principles and practices necessary for de-perimeterization.[10] The same year, DISA (Defense Information Systems Agency) and Department of Defense identified some key principles. The security strategy called "black core" was a security model that focused on moving away from perimeter security and focusing on individual transactions.[18] While the Jericho Forum and DISA laid a lot of the groundwork for de-perimeterization and shifting security focuses, they were not nearly as well-recognized as zero trust is today. It was not until John Kindervag from Forrester Research, Inc. introduced the concept of zero trust and zero trust architecture (ZTA) in 2010 that these ideas truly caught on.[11,12] The accompanying table illustrates a timeline of significant events in the history of zero trust conceptualization.

Zero trust is a broad concept that can apply to technologies, network architectures, and security policies. It has been described as a technology-agnostic mindset that puts security first. It requires that all actors within a network be treated as if they could pose a threat, because they really do. Enterprise resources should be protected individually and subjects accessing these resources should be constantly evaluated to ensure they are not a threat.

According to one of Forrester's seminal reports, three core concepts enable zero trust: All resources must be accessed securely; strict access control based on least privilege must be enforced; and all traffic must be inspected and logged.[12]

The problem with this conception of zero trust is that none of these ideas is particularly novel. In fact, they would strike most IT professionals as good security hygiene we should have been practicing all along. Many security professionals would agree that security should be a design goal of any enterprise system and that insider threats are just as dangerous as any others. This skepticism is warranted as many early explanations of zero trust fail to capture its unique value. A more recent definition from Jason Garbis and Jerry W. Chapman does a better job of explaining the core concepts enabling zero trust:

"A zero trust system is an integrated security platform that uses contextual information from identity, security and IT Infrastructure, and risk and analytics tools to inform and enable the dynamic enforcement of security policies uniformly across the enterprise. Zero trust shifts security from an ineffective perimeter-centric model to a resource and identity-centric model. As a result, organizations can continuously adapt access controls to a changing environment, obtaining improved security, reduced risk, simplified and resilient operations, and increased business agility."[9]

This definition draws attention to the difference between a zero trust *system* and the more abstract zero trust *mindset*. This mindset should not be confused with ZTA, which is any security architecture that enables zero trust. A zero trust mindset emphasizes that enterprise security should be extensible so any future additions support the goal of zero trust. Zero trust recognizes that no two security environments are the same. For example, data centers have unique security requirements when compared with cloud deployments or IoT networks. The National Institute of Standards and Technology (NIST) Special Publication 800-207 goes into further detail about potential implementations. It outlines multiple architecture models and technological implementations of the core logical components.[18]

In 2018, Forrester updated its original ideas for zero trust with the ZTX (zero trust eXtended) platform, which is intended to assist an organization's efforts in acquiring technology and implementing ideas for adding zero trust to legacy systems.[6] It is based on seven capabilities for mapping solutions to zero trust implementations: data; networks; people; workloads; devices; visibility and analytics; and automation and orchestration. This work ensures zero trust does not stagnate and that new ideas can be implemented within a zero trust environment.

Significant events in the history of zero trust.

1	2004	The Jericho Forum introduces the concept of "de-perimeterization"
2	2007	DISA and the Department of Defense identify "black core" security strategy The Jericho Forum publishes its Commandments for de-perimeterization
3	2010	John Kindervag introduces zero trust
4	2014	Google publishes the first BeyondCorp article about its efforts to implement zero trust
5	2018	Forrester Releases the ZTX platform
6	2020	NIST publishes SP 800-207 providing guidance on zero trust

Why *Trust* Zero Trust?

The intersection of people, process, and technology (PPT) has long been a critical focal point for organizations evaluating their business practices. The PPT framework was introduced in the 1960s by Harold Leavitt in *Applied Organizational Change in Industry*.[14] The original model, which consisted of tasks, structure, people, and technology, combined tasks and structure into the process category, resulting in PPT. Bruce Schneier brought PPT to the forefront of the information security field in the late 1990s.[19] Even though it has been suggested that technology has become the most crucial aspect in today's threat responses, a strong relationship remains among all aspects of PPT. The organizational change that accompanies the transition to zero trust can be mapped onto this framework for a more structured approach to the topic.

Zero trust is a new mindset that

requires sweeping changes to be implemented effectively. There are obviously numerous drivers and barriers influencing an enterprise's choice to adopt zero trust, and so the question remains: Why *trust* zero trust?

People. The zero trust mindset brings several benefits that are motivating enterprises to consider adopting it. Zero trust requires that all employees take an active role in the security of an organization. With the increased prevalence of remote work, it is more important than ever that these workers be made aware of good security hygiene. An organization that commits to zero trust will likely try to increase organizational awareness of security and drive acceptance of zero trust.[17] This will have the knock-on benefit of forcing organizations to educate their employees about security. A more security-aware workforce will be a natural by-product of zero trust adoption.

From a cultural perspective, zero trust fosters interdepartmental cooperation and the adoption of IT. Since the network's systems will be geared toward secure networking, cooperation is critical to achieve a working zero trust security architecture. The successful integration of teams can improve network and security extensibility and prevent finger-pointing when problems arise.[5] Resources can be distributed equitably because these security and infrastructure teams will be cooperating and no longer competing to achieve different goals.

Not only might it improve the cooperation among existing teams, but zero trust also enables more flexible hiring. When it comes to hiring skilled workers, the ability of zero trust to create a superior remote work environment relieves security fears surrounding new hires. During a time where remote work is becoming increasingly prevalent, security and efficacy considerations may prevent an enterprise from hiring otherwise excellent employees.[20] Zero trust can help alleviate some of these fears and makes security onboarding much easier for remote work.

The final major people-centric driver of zero trust is management support. Senior decision-makers can be more easily convinced to take on zero trust initiatives because they can lead to long-term cost savings. Legacy networks often require a multitude of vendors, technologies, and solutions to ensure they remain secure. More time, money, and staffing are necessary to support these complex networks. Consolidating these controls into a more uniform and extensible zero trust solution means that vendor, management, and upkeep costs can be reduced more easily.[6] The increasing awareness that security is not just a cost sink, and that proper implementation can save time, money, and effort will make it much easier to garner support from upper management for zero trust projects. A successful zero trust endeavor will aid in digital transformation.[5]

Process. A unique opportunity to improve security posture has been presented to all enterprises affected by the pandemic. Zero trust drives enterprises not only to patch the holes created by transitioning existing processes, but also to improve the security of business processes. The reimagining of business processes will allow for better flexibility with remote work and a security-first mindset.

The open-ended nature of zero trust will enable greater extensibility to ensure organizations can freely adapt their security to the threat landscape. Extensibility by design is further aided by zero trust's emphasis on data collection and auditing. This allows enterprises to view information required to make informed decisions about secure process adjustments.[6] Collectively, this serves to reduce future costs and increase an organization's agility.

Security processes will likely be improved in the short term as well. Many zero trust deployments can take advantage of continuous authentication to reduce the friction that employees experience without compromising security. Google's BeyondCorp deployment effectively eliminated the need for a virtual private network (VPN) when remotely connecting to the network.[2] This saved both time and frustration related to configuring and connecting to a VPN. Research has found that 87% of security professionals who have adopted a zero trust approach have found that it improved productivity.[20]

Additionally, persistent data collection on the state and behavior of an entity allows for modeling normal entity behavior on the network. Continuous authentication allows security checks to identify unusual behavior and quickly respond.[7] This streamlines both everyday security processes and threat response processes.

One of the key tenets of zero trust is to protect data by collecting data. A working zero trust deployment requires an extensive audit of organizational resources. Knowing where different data is stored and what it is used for improves data organization and promotes informed security decision-making. Data can be identified and protected with varying degrees of security, depending on its sensitivity.[5] Better data management also aids privacy initiatives, such as ensuring General Data Protection Regulation (GDPR) compliance because the organization will know where its relevant data is stored and how to protect it.

Technology. Zero trust also has the potential to have a significant impact on the way enterprises use technology. Networks can be greatly simplified and split into modular segments, reducing maintenance and upgrade costs. Rather than continue managing the patchwork of devices and protocols across the whole network, individual segments can be implemented one at a time. This way the entire network need not be changed every time an upgrade is required.[11]

Segmentation also allows flexibility in different parts of the network. An IoT network may require a different security configuration than a network supporting cloud applications. Segmentation provides flexibility in implementing individual segments without compromising the overall needs of a zero trust network.[6] Industry regulations, such as Payment Card Industry Data Security Standard (PCI DSS) require only that the relevant segmented area meets all the specific regulations. A properly segmented network means that the focus on compliance can be limited to the segments that require it.[5] This again helps to reduce overall network complexity, saves money on compliance initiatives, and enables extensibility.

The technology that enables zero trust enables better security as well. NGFWs (next-generation firewalls) allow for inspection of application-layer traffic. Therefore, attack signatures that are otherwise invisible to traditional firewalls can be identified and quickly dealt with.[9] The damage from

attacks that do get through is limited because of network segmentation.[5] Overall, technology enables zero trust to enhance threat response and mitigate successful attacks.

Zero trust aims to combat threats by providing superior data protection. By protecting individual resources, granular data-protection rules can be implemented. As a result, large-scale data breaches will become less common because data access will be predicated on a risk-based approach. The location, value, sensitivity, and common usages of data will clearly define how it can be accessed. Network segmentation can further reduce the risk of individual breaches by keeping sensitive data in separate parts of the network.[7]

Trust through entity verification is not a new concept for cybersecurity professionals. Zero trust simply advances the idea by requiring that trust to be earned constantly rather than only once. BYOD (bring your own device) schemes bring inherently untrustworthy devices into the network. A universal set of trust requirements that apply to all devices makes managing security a much easier task.[7]

A zero trust mindset will have numerous benefits for any organization with significant digital assets. Properly implemented, ZTA will provide greater visibility into networks while simultaneously improving vulnerability management and breach detection.

Zero trust requires the inspection of all network traffic. NGFWs can inspect application-layer traffic, making it easier than ever before to get a clear picture of an organization's network. The added visibility helps to mitigate or even prevent data breaches. If unusual traffic can be inspected for signs of a breach, then it can be dealt with much faster. The FireEye M-Trends 2019 report states that the median time to discover a breach is 78 days.[8] Better network visibility means identifying vulnerabilities faster and allowing security professionals to react before anything has a chance to occur.[5]

A Word of Caution

Given the number of factors driving adoption and the numerous benefits of zero trust, it would seem as if every organization should be rushing to implement a ZTA. Despite vendors complaining that zero trust is a game changer, it should not be implemented without caution. A variety of barriers and potential downsides means that zero trust adoption must be considered carefully.

Organizational readiness. Before an organization commits to zero trust, it must consider cultural compatibility. Zero trust security and network professionals are better-versed and more likely to see the value in the systems they already work with. If the teams responsible for implementation and operation are not convinced or run into too many difficulties during the transition, it will not be successful. Similarly, during implementation, user issues can diminish support for zero trust and lead to the perception that it decreases productivity and increases frustration.

It will be challenging for any organization to reap the benefits of zero trust if its users do not understand its value. For example, WestJet found it necessary to establish CoEs (centers of excellence) to promote learning and cultural acceptance of zero trust.[13] An enterprise that cannot provide similar resources may struggle to get networking and security professionals on board.

Since Kindervag's original work in 2010, a few organizations have begun implementing ZTA. A telling feature of this transition is that only recently have complete or near-complete zero trust initiatives been evaluated. Google's BeyondCorp is an example of a complete organizational shift that took multiple years from start to finish.

ZTA means a substantial pivot that requires forward-thinking, executive support, contingency plans, and commitment. Shifting to zero trust without a plan can result in half-complete measures and more complexity for security professionals to manage. Culture, technical bias, and emotional stake in current security practices can be a major barrier to success with zero trust. There may also be a misconception that zero trust is simply a marketing buzzword.[9] Therefore, organizations hoping to adopt a zero trust approach must be prepared for a long process with both political and technical issues that need to be resolved.

Zero trust is rarely being implemented by organizations that can start from scratch, but in its beta version of ZTA design principles, the U.K.'s National Cyber Security Centre (NCSC) acknowledges that even a greenfield environment requires patience and careful planning.[21] This means many organizations with established security practices and infrastructure may lack the agility and flexibility to simply start operating with zero trust. During the transition an enterprise may require changes to systems that cannot afford significant downtime, or a process component may not be readily replaceable with a zero trust counterpart.

Any organization that lacks flexibility to deal with such issues may find itself in a difficult position. The organizational inertia that current processes have and lack of one-to-one replacements for various process components can make transitioning to zero trust a difficult endeavor.

Technological challenges. Zero trust depends on excellent data management and information literacy. To segment a network and implement necessary controls properly, an organization must have excellent knowledge of its own data environment. Where does traffic need to go? Which resources are required for what roles? Where is high-priority data located? These are just some of the questions that need to be answered for a successful zero trust deployment.

NIST SP 800-207 suggests a complete audit of network components, data sources, actors, and enterprise assets such as managed devices.[18] An organization that lacks visibility into these areas is much more likely to implement an ineffective security system at great cost. At worst, it will reduce the effectiveness of workers. Setting up systems with the requisite visibility and analytical capability can require a large amount of money and effort, causing a significant barrier to adoption.[6]

IAM (identity and access management) is a necessity in any proper zero trust system. Poor management of user groups and disparate identity providers can lead to significant difficulties while implementing zero trust. Zero trust policies leverage identity attributes and user groups to grant access to resources safely and reliably. Zero trust could be the catalyst for improving IAM practices, but this still means that an enterprise needs to address these problems if it is to proceed with zero trust.[9]

Assets and technology used in ZTA

implementation may not be easy to migrate from or replace without excessive cost. Service providers could be highly specialized, meaning that if they experience issues, enterprise resources and business functions could be disrupted. Many core components of zero trust can be challenging to implement with current commercially available solutions.[21]

Artificial intelligence (AI) and software-based agents might be used for security purposes on an organization's networks. These agents, in turn, need to interact with various ZTA components. How these agents authenticate themselves is a largely unsolved problem for ZTAs. A non-person entity (NPE) may have a lower bar to entry, so attackers trying to gain access to a network may impersonate an NPE. In addition, the NPE may be an attack vector itself that could be manipulated into performing malicious actions.[3]

Data stored as a part of network monitoring could also become a target for attackers. This information would be useful for reconnaissance and planning future attacks. The management tools used to encode access policies are also potential points of attacks because they contain information about user and policy data.[18]

Policy engine (PE) and policy administrator (PA) are single points of failure for ZTA. Should the PE become compromised by a malicious or incompetent administrator, its rules could be changed to the point where they disrupt operations or create vulnerabilities in the system. A compromised PA could allow access to resources that would otherwise be off limits. To mitigate this threat, a policy could be housed in a secure cloud environment or exist in several locations. The blockchain may be a viable solution to managing PE policy.[18]

Much of the traffic on the network may be opaque to layer 3 network-analysis tools. Traffic may be coming from non-enterprise assets or simply be resistant to monitoring. As a result, different methods must be used on encrypted traffic, such as collecting metadata and machine-learning techniques.[18]

Recommendations for a High-Risk, High-Reward Journey

Adopting a zero trust approach to cybersecurity is a high-risk, high-reward option for an enterprise. Correctly envisioned, zero trust offers a myriad of security improvements, an improved cultural mindset toward security, cost savings, and a highly extensible starting point for adding further enhancements. While the benefits are significant, it should be noted that zero trust needs to be an ongoing effort and transitioning to a zero trust approach can be a long and arduous process. Recommendations for an enterprise looking to adopt zero trust should follow the PPT template.

Zero trust depends on excellent data management and information literacy. To segment a network and implement necessary controls properly, an organization must have excellent knowledge of its own data environment.

People. Given that zero trust adoption is a long process, it is important that it has proper managerial and cultural support. A newer or more agile company may have an easier time aligning business objectives with the zero trust approach. An established enterprise, however, requires more effort to refocus managerial and cultural attitudes. Google ensured it had an effective technical support strategy to reduce user frustration during rollout. It also engaged with any impacted teams very early on in deployment.[21] WestJet created CoEs to enable its network and security teams to familiarize themselves with and learn the new technology.[13] These were also places where people could address concerns and suggest solutions during deployment.

Such strategies to gain the support of stakeholders are key for adopting any new technology or process. Lobbying important managerial positions by reinforcing the benefits of zero trust is one way to obtain the necessary support. Naturally, management will not be convinced unless there is a well-constructed plan.

Getting over political barriers can be eased by clearly enumerating the benefits of zero trust, finding an active executive champion, starting with minor projects that will show clear benefits, or actively seeking to work with networking or cybersecurity counterparts. Avoiding the misconception that zero trust will destroy or replace the infrastructure and architecture that others have worked hard to develop is a good way to ease interdepartmental and political tensions.[9]

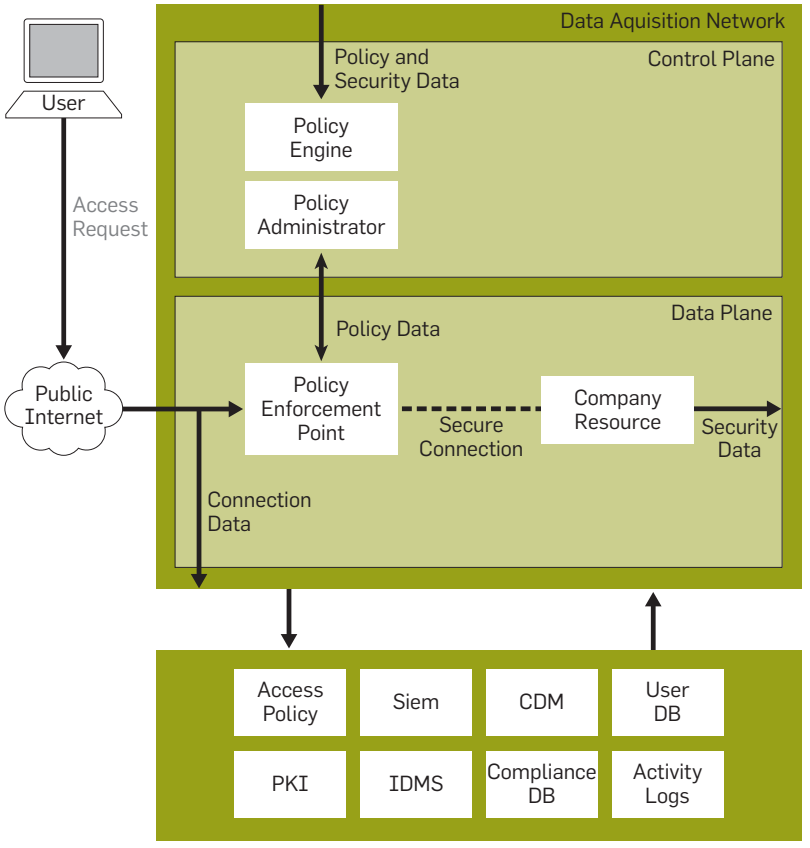
Process. The implementation process for zero trust is imperative for a successful transition. NIST SP 800-207 provides an effective way to transition from a perimeter-based network. The key steps are:

- Identifying actors who will use the system

What Does Zero Trust Architecture Look Like?

Although ZTA can be implemented in numerous ways, there are a few core logical components. The accompanying figure shows an example of a basic ZTA. A policy engine (PE) is located before the protected resources and makes the final decision regarding a subject's access to a given resource. A PE is paired with a policy administrator (PA), which is responsible for carrying out access decisions. It will signal to the policy enforcement point (PEP) that a session be created or destroyed.

Significant events in the history of zero trust.



The PEP acts as the gateway and manages the actual sessions between an entity and a resource. As these are logical components, the specific implementation details can vary, sometimes having a single device play multiple roles.[18] Many of these components also feed data into a data-acquisition network, which interacts with a variety of security policies, tools, and databases such as:

- **Access policy**
- **SIEM (security information and event management)**
- **CDM (continuous diagnostics and mitigation) programs**
- **User databases**
- **PKI (public-key infrastructure)**
- **IDMS (integrated database management system)**
- **Compliance databases**
- **Activity logs**

By interfacing with these and other data sources/sinks, the data-acquisition network allows for constant evaluation of the network's status. Apart from these core components, ZTAs can be implemented in various ways that have distinct advantages and disadvantages. For example, the UK's NCSC (National Cybersecurity Centre) suggests SSO (single sign-on) and token generation at the PEP, which is broadly applicable to many architecture models despite this not being a requirement for an effective ZTA.[15] Effective architecture is a moving target and ideas will change over time to support the core tenets of zero trust.

- Identifying enterprise assets
- Identifying key processes and evaluating risks associated with executing process
- Formulating policies for the ZTA candidate
- Identifying candidate solutions
- Planning for initial deployment and monitoring
- Expanding ZTA

The requirement to perform extensive audits to gather information is a key takeaway. Successful zero trust enterprises need to know the impacted stakeholders, relevant assets, and the processes that must be reimagined during the transition. Otherwise, the organization is likely to have gaps in its implementation that can lead to even more significant security flaws in the future. ISACA has also identified visibility as a vital component of a successful ZTA.[17]

System analysis and auditing can be extremely difficult for complex systems. Zero trust deployments such as BeyondCorp and PagerDuty deployed zero trust broadly, spanning multiple business areas with fine-grained access control. They performed extensive network analysis to ensure these efforts would not interrupt productivity. This approach took much more time and effort than an incremental approach would. It can also be just as effective to onboard groups of users slowly and start with more coarse-grained access control. As the zero trust initiative progresses, it will become easier to tighten up these controls.[9]

Formulating policies, identifying potential solutions, and initial deployment should make use of all the collected information. Logical architecture and technological components should fit the enterprise's specific needs. The initial deployment and monitoring further collect information about how the implementation works and provide areas for improvement.

The final step is the most significant part of any implementation approach. Zero trust is meant to be extensible and provide the flexibility to adapt to changes in the security landscape. As ZTA is expanded, these steps should be repeated to maintain a continuously informed and improving security system. Given its novelty, zero trust networking will likely have evolving best practices, so a flexible approach is advised.[15]

A significant barrier to zero trust

initiatives is "analysis paralysis." Zero trust is a significant undertaking that contains many unknowns. An enterprise may also lack complete visibility into numerous internal factors. These problems balloon when approval from many stakeholders requires that a zero trust system immediately meet the same standards of existing enterprise systems. Consequently, zero trust initiatives can move extremely slowly and provide little to show for all of the effort. Effective milestones, close cooperation with stakeholders, and iterative deployment are some of the measures that can help reduce analysis paralysis.[9]

Technology. The final set of recommendations considers technology and implementation details. Zero trust is applicable in a variety of settings, including IoT, big data, and the cloud. The specific architecture should consider the environment for which it is being deployed. A company that is transitioning to zero trust may want to treat its IoT assets differently from internal applications. Network segmentation provides the flexibility to mix and match technologies and methods for different portions of the network. An enterprise should not attempt a one-size-fits-all architecture but instead, build out its zero trust network according to the requirements of different segments.

Many organizations are also subject to regulatory and compliance restraints. To avoid a situation where an enterprise zero trust system fails to meet compliance, it is essential to engage with external auditors and third-party compliance specialists early on.[9]

Additionally, ZTA should not be implemented with a singular focus on endpoints. An attacker able to subvert endpoints can move freely throughout a network again. Zero trust should be implemented in a layered approach that does not neglect network security policies. ISACA recommends implementing network security policies and adding endpoint capabilities to ensure the effects are complimentary.[14]

Future Directions

As zero trust is deployed in increasingly complicated environments, security becomes more imperative. *Fog computing* occurs in a network where both users and devices are heterogeneous. There is an added caveat that server capacity in fog computing is far lower than in cloud computing, and as a result, zero trust would require a lighter-weight implementation.[22]

Next-generation network technologies will provide numerous benefits but will also cause more heterogeneity. Managing different types of access devices through the centralized architecture of zero trust poses a problem that is only beginning to be explored. Software-defined networking (SDN) is one solution that may fit well with zero trust networks.[22] Organizations such as Ericsson are aware that zero trust is technology-agnostic and have begun outlining how 5G networks impact ZTA.[16]

Zero trust requires that networks efficiently authorize traffic and data, but this becomes difficult as data volume and complexity increase. AI is one potential solution. By extracting features and classifying data, an efficient AI system could greatly increase the efficiency of a zero trust network.[22]

NIST is the only standards organization to provide a systematic exploration of zero trust. Literature about holistic schemes is rather thin outside of private organizations. As different architectures are developed for situations involving cloud networks, IoT, and big data, it will be necessary to classify general schemes that can achieve zero trust in different circumstances.

Zero trust brings few new security principles to bear, but more importantly provides an approach to get the most out of what cybersecurity professionals already consider good practice. Least privilege, strong authentication and access control, segmentation, defense in depth, and extensive logging and auditing are all existing practices that zero trust puts together with a cohesive goal in mind. The goal is security by design and a security-first mindset. Naturally, such a broad goal leaves much room for further research and development of new technologies that fit into ZTA. As new ways to enable zero trust emerge, security practices will only improve. As threats increase in number and severity, you should trust zero trust, because it includes all the things you should be doing anyway. C

References

1. Bendovschi, A. Cyber-Attacks—Trends, patterns and security countermeasures. *Procedia Economics and Finance 28* (2015), 24–31; https://doi.org/10.1016/S2212-5671(15)01077-1.
2. Beske, C. M., Peck, J., Saltonstall, M. Migrating to BeyondCorp: Maintaining productivity while improving security. *Login 42*, 2 (2017). Google Research; https://research.google/pubs/pub46134/.
3. Bleech, N. What is Jericho Forum? Visioning White Paper, Jericho Forum, 2005; https://collaboration.opengroup.org/jericho/vision_wp.pdf.
4. Cisco. *Annual Cybersecurity Report 8*, (2018), 19; https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf.
5. Cunningham, C., Pollard, J., Holmes, D. The eight business and security benefits of zero trust. Forrester, 2019; https://bit.ly/3M9v2Cq.
6. Cunningham, C. *The Zero Trust eXtended (ZTX) ecosystem*. Forrester, 2019.
7. Embrey, B. The top three factors driving zero trust adoption. *Computer Fraud & Security 2020*, 9, 13–15; https://doi.org/10.1016/S1361-3723(20)30097-X.
8. FireEye. M-Trends 2019; https://content.fireeye.com/m-trends/rpt-m-trends-2019.
9. Garbis, J., Chapman, J.W. *Zero Trust Security*, 1st ed. Apress, 2021
10. Jericho Forum. *Jericho Forum Commandments*, 2007; https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf.
11. Kindervag, J., Balaouras, S., Coit, L. *Build security into your network's DNA: the zero trust network architecture*, 2010, 1–26. Forrester; https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf.
12. Kindervag, J., Balaouras, S., Coit, L. No more chewy centers: introducing the zero trust model of information security. Forrester, 2010; https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf.
13. Kindervag, J., Mak, K. Case study: WestJet redefines its security with Forrester's zero trust model. Forrester, 2015; https://bit.ly/3fJgs8w.
14. Leavitt, H.J., March, J.G. *Applied Organizational Change in Industry: Structural, Technological and Humanistic Approaches*. Carnegie Institute of Technology, Graduate School of Industrial Administration, 1962; https://books.google.ca/books?id=P_KZNQAACAAJ.
15. National Cybersecurity Centre. *Mobile device guidance: network architectures* (2020); https://bit.ly/3rs6vin
16. Olsson, J., Shorov, A., Abdelrazek, L., Whitefield, J. Zero trust and 5G—realizing zero trust in networks. *Ericsson Technology Review* #05 (2021); https://bit.ly/3rrzFhA.
17. Pironti, J.P. Five key considerations when adopting a zero trust security architecture. @ISACA 7, 2020; https://bit.ly/3ygzAB8.
18. Rose, S., Borchert, O., Mitchell, S., Connelly, S. Zero trust architecture. NIST SP 800-207, 2020; https://csrc.nist.gov/publications/detail/sp/800-207/final.
19. Schneier, B. People, process, and technology. Schneier on Security, 2013; https://www.schneier.com/blog/archives/2013/01/people_process.html.
20. Sheridan, O. The state of zero trust in the age of fluid working. *Network Security 2021 2*, 15–17; https://doi.org/10.1016/S1353-4858(21)00019-2.
21. U.K. National Cyber Security Centre. Zero-trust-architecture. Github; https://github.com/ukncsc/zero-trust-architecture.
22. Yan, X., Wang, H. Survey on zero trust network security. *Artificial Intelligence and Security. Communications in Computer and Information Science* 1252 (2020). X. Sun, J. Wang, E. Bertino, Eds. Springer Singapore; https://doi.org/10.1007/978-981-15-8083-3_5.

Matthew Bush is a research assistant at Toronto Metropolitan University's Cybersecurity Research Lab. His research interests include managing privacy, security, and ethical concerns stemming from Internet of Things, big data, and machine learning.

Atefeh Mashatan is a Canada Research chair and an associate professor at the Ted Rogers School of Information Technology Management and the founder and director of the Cybersecurity Research Lab at Toronto Metropolitan University (formerly Ryerson University). She investigates challenges and opportunities brought forward by these new technologies and how they change the threat landscape of cybersecurity. In 2019, Mashatan was recognized by *SC Magazine* as one of the top five Women of Influence in Security globally.