MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

ACHIEVING MISSION ASSURANCE FOR ENTERPRISES TODAY AND TOMORROW

ZERO TRUST, THE CLOUD, AND OTHER TOOLS

by Samuel S. Visner

Executive Summary

This MITRE white paper covers current cybersecurity challenges and how new cybersecurity technologies can help us meet them. The recent SolarWinds exploit against network management systems and the enterprises they serve highlight vulnerabilities in current enterprise infrastructures.

We learned that the cybersecurity approaches being employed to protect them are simply insufficient. This incident reminds us how sophisticated and determined our adversaries are. They are constantly innovating their tools and techniques—and no organization is invulnerable. Traditional cybersecurity defenses that rely on signatures of known malware are not likely to detect network intrusions, either through product supply chains or through new, non-signature threats.

TRADITIONAL CYBERSECURITY DEFENSES ARE NOT LIKELY TO DETECT NETWORK INTRUSIONS.

The paper gives particular attention to Zero Trust Architecture (ZTA) models, as well as other tools, including cloud-based analytics and rules to mediate access by users to specific resources. Overall, this paper describes a world in which entry to a network is no longer sufficient to gain access to specific resources. Rather, we consider a world in which every user's access to specific resources is mediated individually, possibly using artificial intelligence (AI).

Contents

Introduction

The recent SolarWinds exploit against network management systems and the enterprises they serve highlights enduring vulnerabilities in enterprise infrastructures upon which we depend. It is clear the cybersecurity approaches currently employed to protect them are simply insufficient. This incident reminds us how sophisticated and determined our adversaries are. They are constantly innovating their tools and techniques—and no organization is invulnerable.

For too long we relied on a technology approach that allows security to be a distant second to the development of new information technologies. We allowed ourselves to follow the purported approach of the famed automobile designer, Ettore Bugatti. He replied to a customer about obsolete brakes in an otherwise high-performing car: *"I make my cars to go, not to stop."*[1] We cannot afford an approach in which security is an afterthought. We must accelerate the development of effective cybersecurity solutions, synchronizing them with the development of the advanced infrastructures we need to secure.

Like Bugatti's car, our high-performance enterprise infrastructures are increasingly complex and dynamic. Endpoints are multiplying and will only do so more swiftly as 5G and Internet Protocol version 6 (IPv6) continue to be implemented. Hybrid architectures that conjoin on-premises systems, public and private clouds, and cloud orchestration are reducing the control of chief information officers (CIOs) of the information technology estate for which they are responsible—and chief information security officers (CISOs) of the ability to protect them. The rise of cloud service providers calls for shared security responsibility between those providers and the CISOs of the enterprises they support.

Our vulnerabilities are evident. Traditional, signature-based cybersecurity tools do not detect new, non-signature-based threats. Our supply chains are not sufficiently robust. As the SolarWinds incident shows, software updates are an effective avenue for cyber intruders. Finally, users granted entry to networks may have unfettered access to sensitive resources. Insider threats are a growing menace; well over half of organizations surveyed in 2019 believe that privileged IT users are the most significant insider security challenge.[2] Allowing these users ungoverned access to network resources amplifies this challenge.

We are also seeing that recent advances introduce new risks. For instance, cloud-mobile enterprises use cloud computing to "deliver applications to mobile devices,"[3] and are pursuing an approach called Network Functions Virtualization (NFV) that promises to make application development easier and speed their use and refinement. NFV virtualizes network node functions into common building blocks and offers additional incentives to migrate to cloud (and cloud-mobile) architectures. The promise of NFV is also to increase resource efficiency. Indeed, industry observers hope to see reduced operational and capital expense result from this approach. The problem is that these approaches and others increase both the complexity of the networks and the management of their security.

FOR TOO LONG WE RELIED ON A TECHNOLOGY APPROACH THAT ALLOWS SECURITY TO BE A DISTANT SECOND TO THE DEVELOPMENT OF NEW INFORMATION TECHNOLOGIES.

Lastly, the topology of our enterprises has changed and will continue to do so. The COVID-19 pandemic led to an acceleration toward remote work environments; we're not likely to see a wholesale reversal in how and from where people work. As the future unfolds, the network of today will diminish. "Peripheries" will shift from the networks themselves to defense of individual resources, some of which will be located outside traditional network perimeters. In the future, we may find that individual pieces of data will be safeguarded by their own defenses, mediated by ZTA-based or other data security access rules, though we have yet to develop the technology needed to achieve this goal.

What's Gone Wrong

Currently, the SolarWinds incident is ongoing and not fully resolved, but supply chain risks endure. As Figure 1 shows, the incident also reveals that signature-based and perimeter defenses, and even the concept of "defense in depth," while still helpful, are no longer sufficient approaches to defend our networks and infrastructures. Indeed, the concept of "defense in depth" implies a "fortress" protected by layers of defense. In today's complex, dynamic, cloud mobile, and hybrid world, few such fortresses exist around which defenses can be layered.

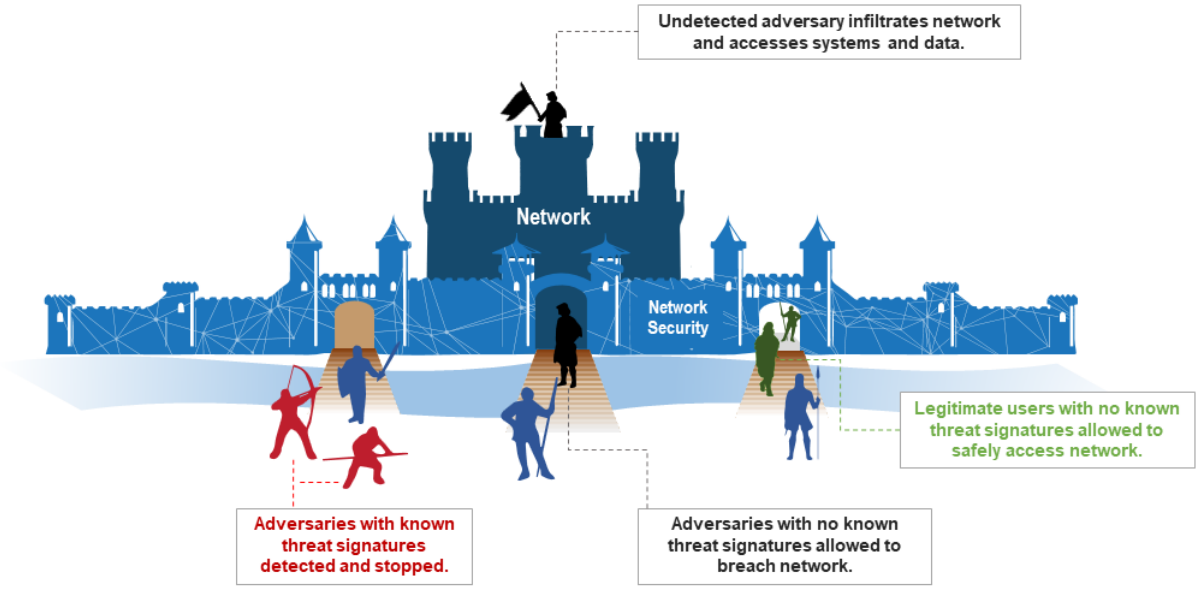

FIGURE 1. SIGNATURE-BASED DEFENSES LET US DOWN.

What Can We Do?

First—and apart from supply chain issues—security approaches must migrate from the perimeter to every aspect of an enterprise. ZTA shifts our thinking by compelling us to "prove" the authenticity and integrity of each link in the chains that comprise our enterprise networks. As described by the National Institute of Standards and Technology (NIST):

> *"Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established. Zero trust is a response to enterprise network trends that include remote users, bring your own device, and cloud-based assets that are not located within an enterprise-owned network boundary. Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource."*[4]

Zero trust helps move us beyond perimeter-based defenses in a world that has fewer and fewer perimeters. In other words, ZTA focuses less on the structure of a network, which may always be permeable, and more on individual resources or assets—access to each must be authenticated. ZTA-based asset authentication allows control asset access "vertically" (between varying levels of an enterprise) and "horizontally" (between varying assets and asset groups).

Adopting ZTA can offer profound benefits throughout the enterprise. These benefits include improved user, partner, and customer experience. ZTA significantly reduces an enterprise's attack surface, even as it simplifies compliance, and enables new and more flexible business models. User experience improvements are particularly noteworthy. Many enterprises control user access through virtual private networks (VPNs). Such access, however, can leave users open to "explore" network resources freely. ZTA, however, controls user access to each resource directly, without the need for a complex (and sometimes slow) VPN. "Losing" a VPN can allow users faster access to the internet through the nearest gateway. Access can be mediated through the nearest cloud gateway, rather than by on-premises gateway appliances.

Partnering is also made easier and more secure. Current models require sophisticated protections and leave enterprise resources exposed to the internet. These models often require a specific security infrastructure for each enterprise system or environment. ZTA, however, provides for scalable, software-defined "precision access" by authorized users to specific internal resources and platform and partner/customer environments, using a cloud-based security infrastructure that mediates zero trust-based, specific access. New business models that engage partners are also easier to implement, given the replacement of cumbersome security appliances with software- and policy-driven access to specific resources.

Security improves accordingly. Users and endpoints constitute a larger—and growing—attack surface. Any user and any endpoint with access to an enterprise network may have access to the entirety of a network's resources. Using ZTA, however, endpoints are never

connected to an enterprise network. In contrast, endpoints are connected only to applications specified for that endpoint user. The policy governing such access is managed in the cloud. The cloud, once feared as a gigantic security vulnerability, can become an important security feature in this new approach to enterprise architecture, depending on a specific cloud provider's architecture and security approach.

The architecture itself can become easier to manage, even as it becomes more secure. Current security architectures feature broad network zoning, the use of expensive firewalls, and complex firewall policies. These policies must be configured and managed, which can be difficult to scale. A more contemporary approach, such as ZTA, lets enterprises manage compliance through software-defined policies governing endpoint access to applications and environments only when they conform to specific internal controls, making the management of policies easier and more scalable.

The path to ZTA can be evolutionary, allowing an enterprise to stage its investment. Initial investment can be focused on policy-based access by users and endpoints to protected resources; subsequent investments can extend ZTA to policy-based connectivity between back-end resources such as servers. This provides an even greater level of security without many of today's expensive security appliances, some of which have proven fallible in the face of advanced threats such as the one gaining prominence because of the SolarWinds breach. Overall, ZTA can move us, as shown in Figure 2, from a world where users are provided access to systems and networks to one in which users are provided access to applications and data—regardless of where they are deployed. Even VPN access goes away, given that it can represent a significant attack surface should a compromised endpoint connect to a network. For ZTA, the endpoint can only connect to applications or resources for which they are authorized, using software-defined micro-segmentation. We can remove, finally, the concept of "network access."

ZTA CAN MOVE US FROM A WORLD WHERE USERS ARE PROVIDED ACCESS TO SYSTEMS AND NETWORKS TO ONE IN WHICH USERS ARE PROVIDED ACCESS TO APPLICATIONS AND DATA.

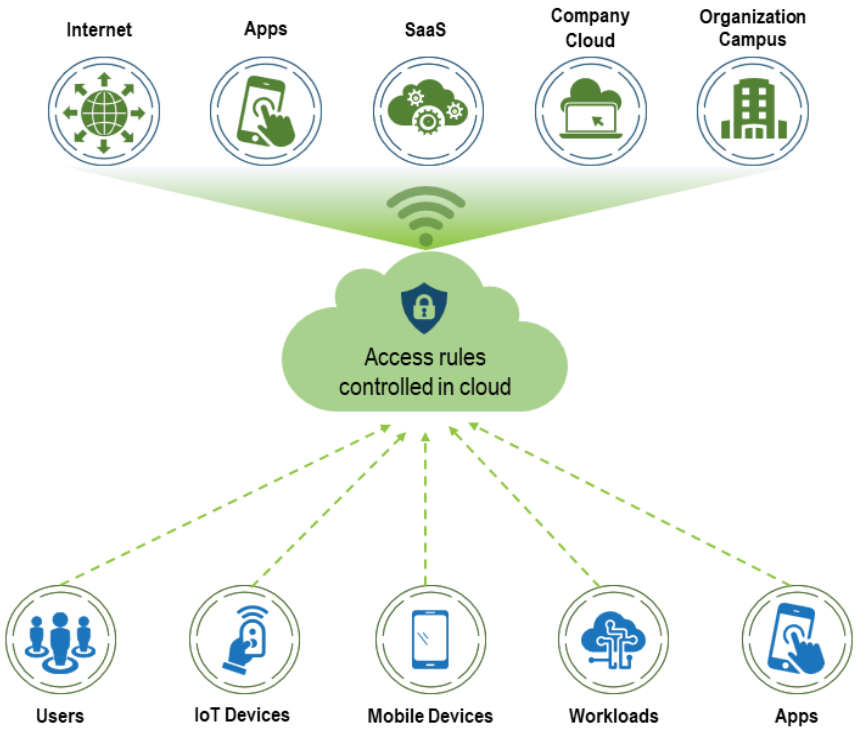

FIGURE 2. ZERO TRUST ARCHITECTURE ECOSYSTEM.

The federal government recognizes the value of ZTA. NIST released a Special Publication (SP 800-207—Zero Trust Architecture[5, 6]) that provides useful guidance on the adoption of ZTA. The Defense Information Systems Agency (DISA), the National Security Agency (NSA), and the Department of Defense (DoD) overall are moving to ZTA models; DISA inaugurated a new testing lab[7] to facilitate adoption, while NSA issued guidance urging that ZTA be considered for all critical national security systems, DoD critical networks, and systems within the defense industrial base.[8]

The cloud itself can become a powerful security appliance. The use of security "connectors" between endpoints and cloud security services allows for cloud-based access mediation. Newer tools, such as Cloud Infrastructure Entitlements Management and Security-as-a-Service Security Posture Management allow for access management in multi-cloud and hybrid environments, and monitor cloud security risk and the posture of cloud security controls, respectively.[9] Again, newer architectures offer the promise of stronger security.

To be clear, ZTA used by the enterprises infected by the SolarWinds exploit would not necessarily have prevented their compromise, but the use of ZTA by companies in the software supply chain could have prevented their exploitation and the use of their software update channels to introduce an exploit into their customers, which would have prevented unauthorized access to sensitive product development resources.

And that brings us to our next point: the SolarWinds attacks made clear that our supply chain is vulnerable. Advanced persistent threats represent both advanced technology and sophisticated tradecraft. Such tradecraft is the hallmark of well-sourced, disciplined, and patient nation-state actors. These actors may decide to exploit a target directly, or they may decide—as in the case of SolarWinds—to create an exploit in their targets' supply chains. In other words, they worked patiently to determine which of their targets used a common network management tool; they compromised that tool, and let that compromise penetrate their target networks.

This kind of sophisticated approach, while dangerous, is not new. In 2011, a nation-state actor attacked RSA's network, allowing access to the dual-factor authentication tokens in use worldwide. In this case, the perpetrator elected to compromise a tool in common use, and then used it to exploit numerous lucrative targets. The RSA example is ironic, given that the supply component comprised was itself a security appliance. Just as telling, despite the *National Strategy for Global Supply Chain,*[10] which the Department of Homeland Security published in 2012, supply chain risks continue to accrue. Supply chain attacks—leveraging information technology common to many enterprises—are likely to become more common as off-premised tools for access management and other enterprise services come into ever-broader use.

Finally, we must not ignore the basics, including employee vetting and training, and intentional and unintentional insider threats. Good insider threat tools, coupled with rigorous programs, can detect intentional actions, as well as risky, albeit unintentional user behavior. Such insider threat programs can also detect the abuse of endpoints that result in anomalous behavior that warrants further investigation. Other steps, including the use of exercises that test employees' susceptibility to phishing, are also useful, basic tools.

SUPPLY CHAIN ATTACKS—LEVERAGING INFORMATION TECHNOLOGY COMMON TO MANY ENTERPRISES—ARE LIKELY TO BECOME MORE COMMON AS OFF-PREMISED TOOLS FOR ACCESS MANAGEMENT AND OTHER ENTERPRISE SERVICES COME INTO EVER-BROADER USE.

The "Right Stuff"

As we confront evolving cyber threats, we can and must do better.

First, understanding adversary tactics, techniques, and procedures can help us prepare for the exploits and attacks we will inevitably face. The MITRE-developed ATT&CK® model allows us access, in concert with partners and information-sharing organizations, to an increasingly rich understanding of our adversaries' capabilities and means of operation. This understanding can help us strengthen and adjust our defenses, both at the perimeter and within our enterprises.

We can also monitor for anomalous behaviors that can reveal an exploit within our enterprises and complex, hybrid networks (including cloud-mobile). Machine learning can be used to understand network behavior patterns. Artificial intelligence can be used to characterize anomalous behavior, deduce the presence of malware, and array defenses swiftly and dynamically to prevent data theft or alteration. End-to-end encryption[11] can make it more difficult for adversaries to exploit exfiltrated data.

CIOs and CISOs must understand their networks completely—including their interconnected and dynamic natures. Cloud service providers and their partners must agree to share security responsibility, ensuring authorized access to both on-premises and cloud resources is managed by the appropriate party. CISOs should convene virtual security teams consisting of representatives of their partners and themselves, charged with the collective responsibility of the networks they share. No one can face this problem alone and succeed.

We need, too, a relentless focus on protecting information itself, even as we secure our enterprises with new architectures, such as zero trust. Encryption at rest recognizes that integrated computer networks comprise large, referential databases of great interest to adversaries. Even "at rest" these repositories may be accessible to these adversaries. End-to-end encryption can ensure that valuable information that exits an enterprise and is shared among inter-enterprise users can be protected. Both encryption approaches, for which tools are widely available, are sine qua non for any organization that takes security seriously, including those that comprise our nation's critical and business infrastructures.

The Federal Government Can Lead the Way

Federal government information systems are among the most sensitive, serving our civilian government, and our defense and intelligence communities. A concerted move toward ZTA, particularly in the wake of the SolarWinds exploit breaches, would signal serious intent to Congress and the public regarding the commitment of the Executive Branch to the best cybersecurity it can attain. Such an effort would also add to the toolset employed to create "deterrence by denial," depriving our nation's adversaries, extremists, and criminals access to information about our citizens and sensitive government operations.

Several paths are available to encourage such an initiative. The Office of Management and Budget (OMB) could undertake a study regarding feasible government-wide paths toward ZTA. Such a study could be informed by both the Federal CIO Council and the Cybersecurity Community of Interest of the American Council for Technology and Industry Advisory Council, a public-private partnership focused on improving federal government IT. An OMB study regarding ZTA could result, importantly, in the outlines of guidance federal departments and agencies could use in preparing their annual budget submissions.

Other federal government tools are also available. NIST Special Publication 800-207[12] describes principles and architectural features of various aspects of ZTA. Additionally, soon ZTA can be made a baseline component of an update of requirements to comply with the Federal Information Security Modernization Act (FISMA). An update to NIST Special Publication 800-53[13] (SP 800-53 Security and Privacy Controls for Information Systems and Organizations) could complement that. Such a revision could provide control specific to ZTA, making such controls a FISMA requirement.

The federal government can build on other, ongoing NIST efforts. NIST's National Cybersecurity Center of Excellence (NCCoE) released a Federal Register Notice[14] "for the development of an example solution for implementing a zero trust architecture." Typically, the NCCoE's work results in "reference architectures" comprised of existing technologies and products, representing practical examples that can be used by industry and government. NIST should move expeditiously to pursue this important effort to create a practical zero trust reference architecture.

The OMB study, an update to SP 800-53, and the NCCoE effort likely can be informed by work underway now at the DoD. The DoD Digital Modernization Strategy (FY19-23) notes that U.S. Cyber Command, DISA, and NSA are already exploring the use of ZTA and intend to rapidly deploy it once key technologies are selected. The Air Force is also exploring ZTA, coupling its efforts with a unified approach to identify, credential, and access management.[15] The work of the agencies could surely inform other parts of the federal government. In addition, DISA's progress toward the use of ZTA might well be used to update Impact Level 2 standards (non-controlled, unclassified information) and those used for FedRAMP Cloud use authorization.

In addition, at the national level, cybersecurity research and development that couples public and private sectors has become more important and urgent than ever. As we move to a world in which our infrastructures reside within complex networks, the nation must accelerate cybersecurity research and development (R&D)—and synchronize it fully with information technology R&D.

If and when a National Cyber Director is appointed—as required by the National Defense Authorization Act of 2021—these initiatives could have a strong champion at the federal level, one who could help establish priorities for the use of ZTA and other advanced cybersecurity technologies, empower a national cybersecurity R&D community, and work with federal CIOs to create new information technology architectures that are more secure intrinsically.

More Can be Done

Given the stakes made evident by SolarWinds, industry and government cybersecurity organizations face a difficult challenge. Managed security service providers (MSSPs) and security-as-a-service (SECaaS) providers should look carefully at the toolsets they employ, many of which are rooted in outdated firewall and perimeter-based defenses. The MSSP/SECaaS community should work with IT infrastructure architects and providers to develop a set of interoperable ZTA tools that allow for the mediation of user-to-resource management. Such interoperability is vital, given that modern enterprises may employ several cloud infrastructures and orchestration services. One might consider how access to common commercial environments (e.g., Office365 and Google Docs) could be made more secure through a common ZTA approach, while also enhancing the security of the enterprises using these environments.

Building blocks already exist, such as identity and access management approaches that use self-service identification to enable network access for users. Adaptive access control techniques include user and device context information in access control decisions, an approach already demonstrated in the financial sector where users may be allowed access only when using a known device with a verifiable configuration. Adaptive techniques can also incorporate user behavior profiles that assess whether an authentication of access request is consistent with expected behavior. Such adaptive techniques make real-time risk estimates and use those estimates in access decisions. We can build on prior work done in this regard, known as risk-adaptive access control to strengthen and make "smarter" our approach toward identity and access management. Such an approach represents a building block toward the adoption of ZTA.

What might come next? Access policy orchestration by ZTA, combined with risk-adaptive identity and access systems can provide a new and powerful view of user activity and behavior, one that generates threat analytics specific to each user, as well as each resource. Such analytics might even be combined with deception technologies that create decoys and seemingly valid files to which adversaries might be redirected, an approach explored as early as 2015. Some of these technologies are already available; newer versions promise the use of artificial intelligence to ensure that decoy material is updated dynamically, providing ever-changing false targets for adversaries. ZTA-based analytics could vector adversaries automatically to artifacts created by these deception technologies. In addition, endpoint detection and response tools that search for anomalous behavior could contribute to this more complete approach to cybersecurity, particularly if they make effective use of AI to identify real adversary activity. Finally, the use of manufacturer user descriptions (MUD) for Internet of Things (IoT) devices mediates the access of IoT devices[16] to other network resources. This could serve as a useful adjunct to the rules-based approach used by ZTA, which controls user access to resources. Future MUD implementation may even use AI to manage device access. Figure 3 provides a notional architectural view combining these techniques.

FIGURE 3. AI CAN GUIDE CYBER DEFENSE.

To be clear, ZTA itself is not a panacea. ZTA can be difficult to implement in enterprises that already allow peer-to-peer communication, common in Windows networks to allow for more efficient bandwidth use during operating system updates, for example. Legacy applications and IT resources, what some call "technical debt," may be incompatible with ZTA. The constant mediation of user-to-resource access may impose system overhead costs, and the capital expense cost of ZTA adoption will have to be considered and budgeted carefully. However, Palo Alto's John Kindervag observes that the simplified security model that can result from ZTA can lower recurring, operational expenses.[17]

ZTA itself also requires enterprises to define their security policies, something not every enterprise has done. ZTA relies fundamentally on security policies that are expressed in the rules governing user-to-resource access.

A couple of other observations: it is important that rigorous controls, such as code scanning, be put in place by companies to ensure their ZTA products do not introduce supply chain risks to the companies that adopt ZTA. Finally, observers agree that ZTA would likely not have stopped adversary access to the SolarWinds software, but note, too, that ZTA would have impeded subsequent adversary activities throughout target networks.[18]

One final issue confronts us: who is responsible for security and resilience in this new, cloud-enabled world? Vague mentions of "best practices" are not sufficient. Clear obligations for security and resilience must be accepted by information technology infrastructure managers and the cloud providers to whom they turn for specific services. Both IT managers and their providers must be held to account for security lapses and failures to communicate clearly to users and customers regarding what has happened, what damage has occurred, and what is being done to mitigate and recover from these lapses.

We're Moving Out

MITRE itself is moving aggressively to adopt ZTA. Our approach will offer both better security and an improved customer experience. It moves existing endpoint perimeter protections to a cloud gateway as we move our users away from our current VPN. MITRE users will be able to gain access to external resources through the security mediation offered by a cloud gateway, rather than on-premises perimeter security appliances. MITRE's approach allows for precise, software-defined precision access only by authorized users to specific resources. Our use of security infrastructure in the cloud will allow for significant scalability as users change, needs evolve, and new environments become necessary. External users will be connected to specific resources through proper mediation, but never to the general MITRE network environment itself. Finally, MITRE expects to realize considerable savings as compliance moves from a myriad of zones and firewalls products and rules to precise, software-defined policies. MITRE intends to make this migration swiftly; work is already underway.

As the nation's critical and business infrastructure confronts these challenges, MITRE stands ready to support and help guide these important efforts.

We urge decision makers and stakeholders to look carefully at our cybersecurity and architecture recommendations. The application of advanced cybersecurity approaches and technologies to our government, critical, and business infrastructures requires strong coordination between policy and technical experts, as well as those experienced in the development and implementation of programs that can be implemented gradually, but surely. MITRE's systems engineering expertise and track record represent powerful resources to bring together the deployment of advanced information technology infrastructures and new cybersecurity technologies. As the nation's premier systems engineering organization, we stand ready to help our government, our critical infrastructure, and our nation's businesses meet this challenge.

MITRE'S APPROACH ALLOWS FOR PRECISE, SOFTWARE-DEFINED PRECISION ACCESS ONLY BY AUTHORIZED USERS TO SPECIFIC RESOURCES.

Endnotes

1. Grand Prix History, "Bugatti 35," [Online]. http://grandprixhistory.org/bug35.htm. [Accessed March 18, 2021].
2. Cybersecurity Insiders, "2020 Insider Threat Report," 2019. [Online]. https://www.cybersecurity-insiders.com/wp-content/uploads/2019/11/2020-Insider-Threat-Report-Gurucul.pdf. [Accessed March 18, 2021].
3. IBM, "What is mobile cloud computing?" [Online]. https://www.ibm.com/cloud/learn/what-is-mobile-cloud-computing. [Accessed March 18, 2021].
4. National Institute of Standards and Technology (NIST), SP 800-207, "Zero Trust Architecture," August 2020. [Online]. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf. [Accessed March 18, 2021].
5. ibid
6. For an illustrative view of how Zero Trust Architecture changes and simplifies enterprise security, see: A. Kerman, National Institute of Standards and Technology (NIST), "Zero Trust Cybersecurity: 'Never Trust, Always Verify,'" October 28, 2020. [Online]. https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify. [Accessed March 18, 2021].
7. K. Atherton, Breaking Defense, "DISA Puts Trust in Zero Trust With New Strategy, Testing Lab," December 2, 2020. [Online]. https://breakingdefense.com/2020/12/disa-puts-trust-in-zero-trust-with-new-strategy-lab/. [Accessed March 18, 2021].
8. National Security Agency Central Security Service (NSA/CSS), "NSA Issues Guidance on Zero Trust Security Model," February 25, 2021. [Online]. https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2515176/nsa-issues-guidance-on-zero-trust-security-model/. [Accessed March 18, 2021].
9. For a discussion of newer, cloud-based approaches to security, see: L. Columbus, Forbes, "What's New in Gartner's Hype Cycle for Cloud Security, 2020," October 25, 2020. [Online]. https://www.forbes.com/sites/louiscolumbus/2020/10/25/whats-new-in-gartners-hype-cycle-for-cloud-security-2020/?sh=1aebcbf7bd92. [Accessed March 18, 2021].
10. U.S. Department of Homeland Security, "National Strategy for Global Supply Chain Security," July 13, 2017. [Online]. https://www.dhs.gov/national-strategy-global-supply-chain-security. [Access March 18, 2021].
11. Too often honored in the breach (pun intended).
12. National Institute of Standards and Technology (NIST), SP 800-207, "Zero Trust Architecture," August 2020. [Online]. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf. [Accessed March 18, 2021].
13. National Institute of Standards and Technology (NIST), SP 800-53 Revision 5, "Security and Privacy Controls for Information Systems and Organizations," September 2020. [Online]. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. [Accessed March 18, 2021].
14. National Archives, Federal Register, "National Cybersecurity Center of Excellence (NCCoE) Zero Trust Cybersecurity: Implementing a Zero Trust Architecture," October 21, 2020. [Online]. https://www.federalregister.gov/documents/2020/10/21/2020-23292/national-cybersecurity-center-of-excellence-nccoe-zero-trust-cybersecurity-implementing-a-zero-trust. [Accessed March 18, 2021].
15. M. Jasper, Nextgov, "Air Force Working on Foundational Zero Trust Activities, CIO Says," March 26, 2021. [Online]. https://www.nextgov.com/cybersecurity/2021/03/air-force-working-foundational-zero-trust-activities-cio-says/172955/. [Accessed March 29, 2021].
16. National Institute of Standards and Technology (NIST), National Cybersecurity Center of Excellence (NCCoE), SP 1800-15, "Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)," September 2020. [Online]. https://www.nccoe.nist.gov/publication/1800-15/VolA/index.html. [Accessed March 18, 2021].
17. J. Kindervag, Sirius Edge, "4 Major Myths of Zero Trust Architecture," January 18, 2018. [Online]. https://edge.siriuscom.com/security/4-major-myths-of-zero-trust-architecture. [Accessed March 18, 2021].
18. D. Nyczepir, Fed Scoop, "Industry urges agencies to accelerate zero trust adoption after SolarWinds hack," January 9, 2021. [Online]. https://www.fedscoop.com/agencies-zero-trust-solarwinds/. [Accessed March 18, 2021].

Authors and Contributors

Samuel S. Visner (principal author) with contributions from John Wilson, Anne Townsend (NCF), and Don Faatz (NCF).

MITRE's Mission

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™