Harnessing Zero Trust Security

Cybersecurity is awash with acronyms, jargon and marketing slogans. There is no dearth of so-called "silver bullets." Yet, history and headlines demonstrate the ongoing success of adversaries and tell us a different story. Zero trust security offers promise, but it is largely misunderstood and perceived by some as yet another overly hyped buzzword. To properly understand zero trust, it is important to dissect the emergence of this concept, identify what it is (and is not), and determine if it can help advance cybersecurity and how.

Why Zero Trust Is Needed

Zero trust should be examined in the context of some of the biggest breaches in the 21st century (**figure 1**).[1]

The much-publicized Target breach of 2013, in which 110 million customers had their personal data stolen, including credit and debit card details, does not even make the list of the top 15 breaches of the century. The growing scale of cyberattacks suggests that efforts often fall short against hackers' tactics. Lack of budget and skilled staff are often cited as some of the persistent problems in securing organizations. Arguably, the security budgets at each one of the enterprises listed in **figure 1** exceeds the annual revenues at scores of others, and many were decently equipped (if not well-equipped) with skilled cybersecurity staff and contractors.

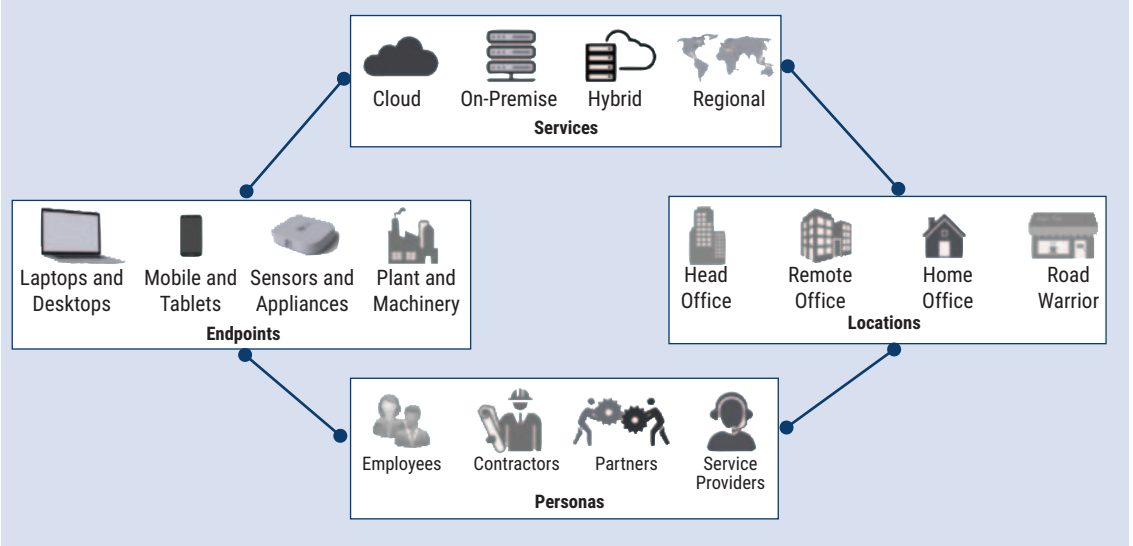
But there are more than just numbers to consider when assessing cyberthreats. The growth in interconnectivity and ensuing complexity leaves even the best of enterprises on the defensive, especially when defending against an ever-evolving threat landscape. Some of the factors driving complexity (**figure 2**) include growing numbers and types of devices connected to the network, increasing demand for application availability and resiliency, consistent quality of service for the work-from-anywhere model, accessibility for strategic business partners and service providers, adaptability for business landscape evolutions and end-user requirements, and audit and regulatory compliance requirements. Security starts when these requirements are satisfied and, historically, has been bolted onto this framework.

As the scale of connections rises and threats evolve, the need for sophistication by attackers goes down (e.g., malware as a service can be purchased for as little as US$150[2]). As business dependency on IT rises and regulatory requirements ramp up, organizations are constantly trying to catch up with attackers and get ahead of breaches. This is akin to having no walls at your home and trying to safeguard your assets by scanning everyone who walks in to ensure that they are doing

Rajiv Raghunarayan
Is the senior vice president of products and marketing at Cyberinc, where he leads the product management, marketing and strategic alliance functions. Raghunarayan has spent more than 25 years in the technology industry, having held technology and marketing leadership positions at FireEye, Cisco and SentinelOne. His areas of expertise include network security, email security, endpoint security, network management, infrastructure security and wide area network (WAN) optimization.

Figure 1—Top-15 Breaches of the 21st Century			
Organization	**When**	**Impact**	**Notes**
Adobe	October 2013	153M user records	Exposed customer names, IDs, passwords, and debit and credit card information
Adult Friend Finder	October 2016	412.2M accounts	Names, email addresses and passwords
Canva	May 2019	137M user accounts	Email addresses, usernames, names, cities of residence, and salted and hashed passwords; OAuth login tokens for Google sign-ins
Dubsmash	December 2018	162M user accounts	Email addresses, usernames, password hashes and other data such as dates of birth
eBay	May 2014	145M users	Names, addresses, dates of birth and encrypted passwords. 3 compromised employee credentials allowed complete access for 229 days.
Equifax	July 2017	147.9M consumers	Social Security numbers, birth dates, addresses, and in some cases driver's license number and credit card numbers Application vulnerability and inadequate segmentation
Heartland Payment Systems	March 2008 (discovered Jan 2009)	134M credit cards	Standard Query Language (SQL) injection
LinkedIn	2012 (and 2016)	165M user accounts	Email addresses and passwords; put up for sale for just five bitcoins
Marriott International	2014-2018	500M customers	Contact information, passport number, Starwood Preferred Guest numbers, travel information, and in some cases credit card numbers and expiration dates Started with Starwood and propagated to Marriott after acquisition; attributed to Chinese intelligence group
MyFitnessPal	February 2018	150M user accounts	Usernames, email addresses, IP addresses and password hashes Part of total of 617M customer accounts offered for sale on Dream Market
MySpace	2013	360M user accounts	Email addresses, passwords and usernames; put up for sale for six bitcoins
NetEase	October 2015	235M user accounts	Email addresses, passwords and usernames; put up for sale for six bitcoins
Sina Weibo	March 2020	538M accounts	Email addresses and plaintext passwords; denied by NetEaxe
Yahoo	2013-2014	3B user accounts	Real names, email addresses, dates of birth and telephone numbers A second breach compromised 1B names, dates of birth, email addresses and passwords, and security questions and answers.
Zynga	September 2019	218M user accounts	Email addresses, hashed passwords, phone numbers, and user IDs for Facebook and Zynga

Figure 2—Multifaceted Enterprise Networks Add to Security Woes



nothing wrong. The general open connectivity philosophy is not far from this scenario, which drives up the cost of security and imposes a constant need for more skilled resources[3,4] while also driving up stress levels for security practitioners. And, unfortunately, as shown in **figure 3**, there is a tremendous skills shortage in cybersecurity. Therefore, it is necessary to rethink the best approach to this problem.

Figure 3—Skills Shortage and Challenges

66 percent

Increased workload on existing staff

47 percent

Inability to learn or utilize security technologies to their fullest

41 percent

Recruit or train junior employees since they do not have experienced professionals

40 percent

Limited time to work with business units to align security with business practices

What Is Zero Trust?

Although the term may be relatively new, the concept of zero trust has been around for several decades. Critical infrastructures such as military installations, power plants, nuclear facilities, medical facilities and financial institutions have, historically, operated using the concept of air-gapped networks.[5] The idea of air-gapping is to separate the network into high (classified) and low (unclassified) segments, with physical separation between the two to minimize the exposed attack surface. Assets on the high network are highly valuable and the low network is not trusted with access to those assets. Although this model is not user friendly, it delivers stronger security than traditional networks.

The term "zero trust" was coined by Forrester analyst John Kindervag in 2010.[6] It has been an evolving definition, but at the core, zero trust is a philosophy or framework for thinking about cybersecurity in today's hostile environments.

As Forrester defines it, the traditional "trust, but verify" cybersecurity model offers attackers a broad attack surface that leaves security teams flat-footed and always in crisis management mode.[7] Zero trust implements methods to localize and isolate threats (i.e., "never trust, always verify") through micro-core, micro-segmentation, and deep visibility to identify threats and limit the impact of any breach.

> ALTHOUGH ZERO TRUST IS A FRAMEWORK, IT IS SUPPORTED BY SEVERAL DIFFERENT UNDERLYING TECHNOLOGIES THAT OFFER PROTECTION ON VARIOUS FRONTS.

Although the world is still in the early stages of the zero trust revolution, this thinking has some key benefits including:

- Reduction of exposed attack surface
- Proactive security
- Damage containment
- Relief of pressure on security teams by moving away from alert-driven architectures

Implementing Zero Trust

Although zero trust is a framework, it is supported by several different underlying technologies that offer protection on various fronts.

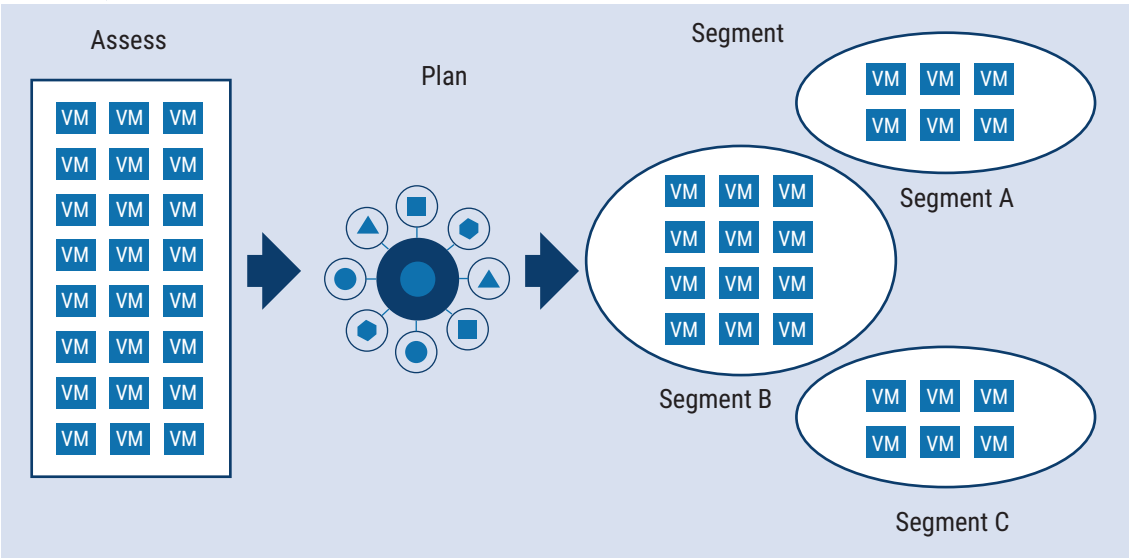
Microsegmentation

One of the earliest concepts to be positioned under the zero trust umbrella, microsegmentation was primarily designed to protect against lateral movement to minimize the impact of a breach. Lateral movement to capture information from key assets in the data center is a key component of several attacks. Microsegmentation aims to limit unsanctioned communication between workloads if they have no operative reason to do so, thereby minimizing breach impact (**figure 4**). Unlike typical north-south protection offered by firewalls, microsegmentation looks at east-west security for workloads.

Several vendors in the market offer products for microsegmentation, including Cisco, VMWare, Illumio and ShieldX. Different microsegmentation solutions tend to have differing models of implementations including agent-based, hypervisor-based, network-based and hybrid deployments.[8] Agent-based solutions have the advantage of residing on the host and can, therefore, look more easily at protocols and encrypted traffic. Network-based deployments extend a segmentation model that many network administrators are familiar with and minimizes the learning curve. Solutions are usually capable of both on-premise or cloud deployments, but hypervisor-only models may be limited in their capability to look into containers or bare metal while offering benefits in a virtual machine (VM)-heavy environment.

It is also worth highlighting that very basic levels of isolation among different cloud workloads can be implemented using native cloud controls such as security groups, L2/L3 firewalls and subnet level filtering capabilities.

Figure 4—Microsegmenting to Minimize Lateral Spread



The questions to ask when considering micro-segmentation include:

- Is the organization's applications communication model understood? Modeling network communications is crucial to ensure that segmentation does not break applications.
- Can the solution offer visibility, administration and migration? Policy management can be time-consuming, but it is an important step to ensure true success of the project.
- Does the infrastructure include nontraditional endpoints such as supervisory control and data acquisition (SCADA) systems, Internet of Things (IoT) and mainframes? Many solutions do not cover these nontraditional endpoints.
- Are there compatibility considerations between microsegmentation and other security technologies (e.g., endpoint agents, network intrusion prevention systems [IPSs], next-generation firewalls [NGFWs])?
- Is the organization looking at cloud deployments or primarily on-premise deployments? What level of segmentation is needed for the cloud? Would native controls suffice?

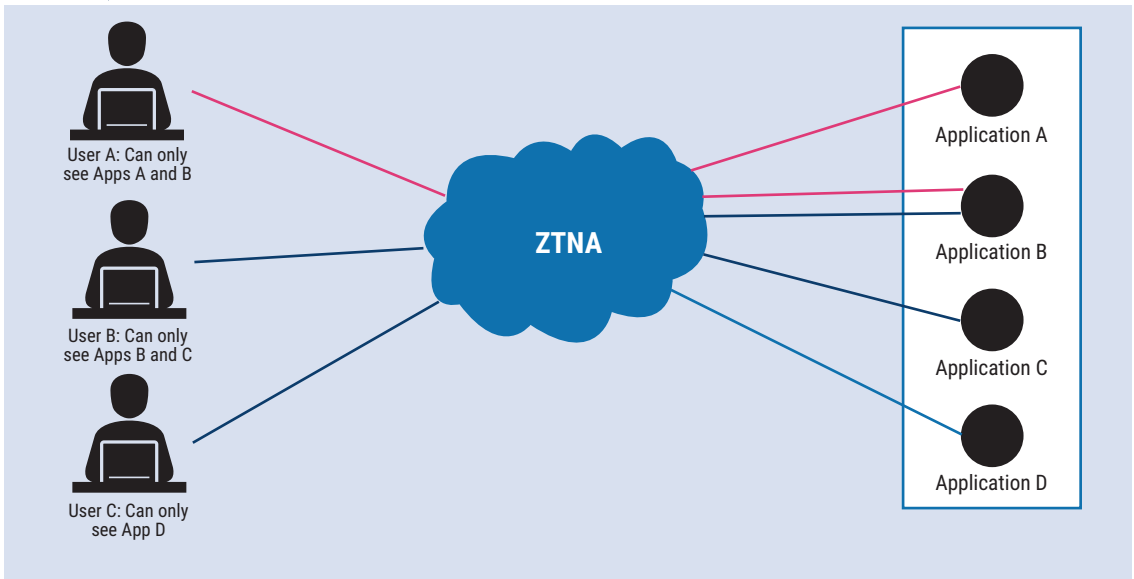
Zero Trust Network Access

Zero trust network access (ZTNA) creates a context-based logical boundary for application access. The goal is to minimize access and abuse by user- and device-context-driven application access. ZTNA challenges the assumption that the location of an entity (e.g., inside a network) should grant trust automatically to a user or device. ZTNA hides all applications on the network and allows access based on attributes such as user identity, device, geolocation and security posture.[9] In other words, users get access to applications they need, but they see nothing else on the network (**figure 5**). A ZTNA broker assesses the user's profile before granting access. The user may be an enterprise employee, a partner or a contractor. ZTNA has its roots in the BeyondCorp[10] architecture and concepts of software-defined perimeters. Sample vendors include Akamai, Netskope, Perimeter81, Pulse Secure and Zscaler.

Although ZTNA has been touted as a virtual private network (VPN) replacement, not all solutions truly replace VPNs. Also, it is important to note that not all applications lend themselves to ZTNA (e.g., consumer-facing applications).

There are two approaches to implementing ZTNA: endpoint-based or network-based. In the former case, ZTNA initiates at the endpoint, and successful end-user authentication exposes the appropriate

Figure 5—Zero Trust Network Access Minimizes Access and Abuse



applications. This typically requires an agent to be installed on the endpoint. In the latter case, a connector initiates registration with the ZTNA broker on behalf of the application provider. A user is given access to the service once they pass the appropriate context and identity checks. This model traditionally works well with Hypertext Transfer Protocol (HTTP)/Hypertext Transfer Protocol Secure (HTTPS)-based applications.

The questions to ask when considering ZTNA include:

- Is the organization able to ensure appropriate user-to-application mapping and application-usage modeling? The key to ZTNA success is knowing who needs what access under what circumstances.
- Are there unmanaged devices that need access to applications, and how would endpoint models work in this case? Is it also necessary to consider programmatic access?
- Do partners, contractors or others need third-party authentication services? Does the ZTNA provider offer this capability?
- How scalable and resilient is the ZTNA broker? It could be a single point of failure.
- Where are the points of presence, and what is the expected latency for a cloud provider?

Remote Browser Isolation

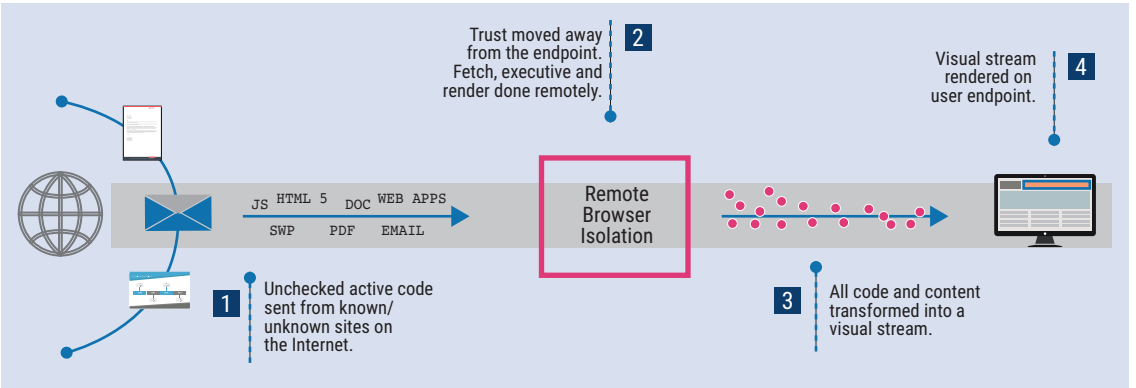
Remote browser isolation (RBI) operates on the principle that end users represent the weakest links in any organization and Internet access is one of the largest attack surfaces responsible for breach origination. Therefore, one of the most effective ways to shrink the endpoint/end user compromise in a cloud-first world is to isolate web access to eliminate browser exploits and threats such as ransomware, malvertising and phishing.

> "THE KEY TO ZTNA SUCCESS IS KNOWING WHO NEEDS WHAT ACCESS UNDER WHAT CIRCUMSTANCES."

Building on the concept of air-gapped networks, RBI creates a virtual airgap to ensure security while also addressing the user experience. Instead of trying to detect all potential dangers and training people to avert them, the RBI model isolates the risk.[11] When an employee clicks on a link, RBI remotely renders the page to ensure that the malware does not even reach the endpoint (**figure 6**).

Enterprises offering browser isolation include Cyberinc, Ericom, Menlo Security and Symantec (Broadcom). Browser isolation can be delivered at the endpoint or in the network. The former necessitates an agent installation with appropriate virtualization support on the endpoint but is deployed closer to the point of breach. The network-based RBI deployments are more popular, can be on-premise or in the cloud and usually require minimal changes at the endpoint.

Figure 6—Remote Browser Isolation Shrinks the Attack Surface to Eliminate Threats



The questions to ask when considering RBI include:

- Does the user experience remain relatively intact with RBI? Some solutions require more user training, which is counterproductive.
- Does the solution cover different security risk scenarios such as web threats, file-based threats, email-based threats and credential theft attacks? Some solutions do not remotely render, which may open the endpoint to risk from media- or CSS-based attacks.
- Do the deployment models align with the enterprise vision and goals? If using the cloud, does the solution have the right points of presence to minimize latency? What edge deployment options does the provider support?
- What level of administrative visibility and control does the solution offer? Do more components need to be purchased to gain visibility and necessary security?
- Does the solution interoperate with security tools such as secure web gateway (SWG), firewalls, and security information and event management (SIEM)?

Conclusion

Zero trust is not a panacea and no vendor should give that impression. The goal of zero trust is to minimize the risk by assuming that breaches are a constant and adapting deployment strategies to localize, isolate and limit a breach's impact.

Revisiting the Target breach through the lens of zero trust shows that there are several points where it could have played a role (and perhaps has in other instances). It is well-documented that the breach started with a phishing attack on a third-party heating, ventilation and air conditioning (HVAC) contractor. This led to a compromise of credentials, which, in turn, allowed access to internal systems, eventually allowing the jump to the point-of-sale (POS) systems across stores. Although some security solutions did generate an alert, they were lost among several thousand other alerts security teams already had to address. A zero trust model would have stopped the initial compromise using technologies such as RBI; credential abuse would likely have been blocked by ZTNA and the jump to the POS segment could have been prevented by microsegmentation.

Most zero trust technologies coexist, complement and interoperate with traditional technologies. However, it is important to understand and evaluate them to suit each organization.

The best return on investment (ROI) usually comes from assessing risk and then understanding feasibility. For instance, if controlled access to cloud services is the biggest risk, ZTNA might be a good place to start, but if end users are a weakness, RBI would be a smart investment. The best place to start the zero trust journey is to assess where risk is the highest.

Endnotes

1 Swinhoe, D.; "The 15 Biggest Data Breaches of the 21st Century," *CSO*, 17 April 2020, *https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html*
2 Bennett, D.; "The Time I Sabotaged My Editor With Ransomware From the Dark Web," Bloomberg Businessweek, 6 February 2020, *https://www.bloomberg.com/features/2020-dark-web-ransomware/*
3 Olstik, J.; "Five Ways to Cope With Cybersecurity Skills Shortage (That Don't Involve Hiring)," *CSO*, 27 January 2020, *https://www.csoonline.com/article/3516113/5-ways-cisos-are-addressing-the-skills-shortage.html*
4 Olstik, J.; "Is the Cybersecurity Skills Shortage Getting Worse?," *CSO*, 10 May 2019, *https://www.csoonline.com/article/3394876/is-the-cybersecurity-skills-shortage-getting-worse.html*
5 "Air gap," Techopedia, *https://www.techopedia.com/definition/17037/air-gap*
6 Higgins, K. J.; "Forrester Pushes 'Zero Trust' Model For Security," *DarkReading*, 17 September 2010, *https://www.darkreading.com/attacks-breaches/forrester-pushes-zero-trust-model-for-security/d/d-id/1134373*

7 Forrester, "Zero Trust," *https://go.forrester.com/government-solutions/zero-trust/*
8 Edwards, J.; "Microsegmentation Architecture Choices and How They Differ," ARN, 27 April 2020, *https://www.arnnet.com.au/article/678528/microsegmentation-architecture-choices-how-they-differ/*
9 Craven, C.; "What Is Zero Trust Network Access (ZTNA)?" sdxcentral, 14 August 2020, *https://www.sdxcentral.com/security/definitions/what-is-zero-trust-network-access-ztna/*
10 BeyondCorp, *https://beyondcorp.com/*
11 Hechler, D.; "Browser Isolation: An Island of Relief from Attack," Cyberinc, 20 May 2020, *https://blogs.cyberinc.com/browser-isolation-an-island-of-relief-from-attack/*