Beyond Zero Trust: Trust Is a Vulnerability

Mark Campbell, EVOTEK

Trust is a vulnerability and, like all vulnerabilities, should be eliminated. Zero trust is a systemic approach to information security that trusts no user, transaction, or network traffic unless verified.

At the very dawn of digital computing, security was of paramount importance. As quirky mathematicians and Allied code breakers pored over the latest Enigma decryptions in World War II, armed guards patrolled the Bletchley Park perimeter with orders to shoot first and ask questions later. Within the verdant grounds, their secret work was compartmentalized between teams in dozens of physically separated concrete block houses and wooden huts. Workers were restricted as to which huts they could enter, what they could access, and identity papers were checked frequently—no one was trusted.[1]

PERIMETERS

After its embryonic beginnings in World War II, digital computing grew to dominate all aspects of business, government, academic, and personal worlds, and it exposed the need for information security. Physical security was soon buttressed with network, system, database, and application security layers to form a solid fortress around computing systems and the information they housed. Security technologies, like firewalls and virtual private networks (VPNs), emerged to create a network security perimeter that allowed trusted users in and kept untrusted users out.

Going a step beyond mere network access, many security thought leaders declared "identity is the new perimeter,"[2] requiring users to show their metaphoric identity papers at the entry checkpoint, determine if they should be trusted, and then grant them entry into the intranet. More advanced layers have been created to shore up the perimeter and report if breaches occur. Intrusion detection systems, intrusion prevention systems, Web application firewalls, network access control, identity governance, and identity access management products and services have filled the security market to help enterprises fortify their digital frontiers.

We have, indeed, come a long way—except, fundamentally, this approach is flawed. The idea of a solid defensible perimeter is an illusion in today's global, mobile, remote, and cloud-based IT landscape where the attack surface is never static, never localized, and never impregnable.

Digital Object Identifier 10.1109/MC.2020.3011081
Date of current version: 5 October 2020

0018-9162/20©2020IEEE

EDITOR **MARK CAMPBELL**
EVOTEK; mark@evotek.com

The inevitable breaches of the hard-crunchy perimeter leave a "chewy center" virtually unprotected.[3] Somewhere along the intervening years we had forgotten what our forbearers learned at Bletchley Park—trust no one.

ENTER ZERO TRUST

The school of perimeter-based security is built on the implicit requirement that there is some way to filter users, network traffic, and transactions into trusted and untrusted buckets. Unfortunately, this assumption has proved intractable. The meteoric rise in breaches from insider threats, hijacked credentials, compromised devices, and phishing attacks give lie to the fallacy of a defensible perimeter. A criminal, competitive adversary, or simply a curious user inside the perimeter can, and does, wreak havoc as suggested by estimates that cybercrime damages are expected to double from US$3 trillion in 2015 to US$6 trillion in 2021.[4]

The solutions mentioned above are themselves not the root of the current crisis. The rotten core, today, as in 1942, is the concept of trust. In a recent interview for this article, John Kindervag stated: "trust is a vulnerability and, like all vulnerabilities, should be eliminated."[5] In a 2008 speech at a Montreal country club, Kindervag first used the term *zero trust* to describe a secure architecture strategy that removed the concept of trust as an access criterion. He later codified the approach in his landmark report, "No More Chewy Centers: Introducing the Zero Trust Model of Information Security," in 2010 while at Forrester Research. A decade later, zero trust has garnered growing support as a groundswell of enterprises across industries shift to its more stable footing. Zero trust is not a product but a systemic approach to information security that trusts no user, transaction, or network traffic unless verified. Zero trust ensures access is granted not just at the perimeter but at every layer, network, application, and data access point in the enterprise. An insider is scrutinized just as heavily as an outsider—no one is trusted.

DOING ZERO TRUST

When viewed through a zero trust lens, one can easily see the problem with the "identity is the new perimeter" movement. A much better mantra would be "identity is the new core." Continuous identity verification across all transactions, even those inside the perimeter, eliminates the need for trust. As Richard Bird of Ping Identity has stated, "If identity is the new perimeter, then Bob in accounting is the new Port 80."[6] Comic but true.

Traditional approaches seek to protect the "attack surface," the superset of all the enterprise's possible entry points. Unfortunately, this approach has proved impracticable since today's typical attack surface is dynamic, complex, and unknowable. Instead, zero trust seeks to secure the "protect surface," an enterprise's unique configuration of data, assets, applications, and services (DAAS). Because the protect surface consists only of those components important to the enterprise, it is typically drastically smaller than the attack surface—and, most importantly, completely knowable.[7]

Forrester and several implementers, such as the Palo Alto Network, have standardized on a five-step process to implement a zero trust architecture[7]:

- Identify the protect surface.
- Map the transaction flows.
- Build a zero trust architecture.
- Create zero trust policy.
- Monitor and maintain.

While it is very straightforward to state, the implementation of a zero trust architecture can take several years to bring to fruition. Nonetheless, 72% of organizations plan to implement zero trust capabilities in 2020.[8]

BEYOND ZERO TRUST

The zero trust framework lays out a security vision much better suited to the fluid cloud and mobile-centric world of today's enterprises than its perimeter-focused predecessor. But zero trust is just that—a vision, not a recipe—a strategy, not a toolset. More prescriptive methods have emerged over the past decade to add tactical legs to the zero trust's strategic platform, including the following.

Software defined perimeter

Stemming from work at the Defense Information Systems Agency, the Cloud Security Alliance developed a zero trust networking framework called the software defined perimeter (SDP). Following the paradigm pioneered by software-defined networking, in which the network's data and control planes are separated, SDP 2.0 restricts discoverability, visibility, and access to all network-connected DAAS. SDP authenticates identity (not network address) dynamically adjusts entitlements, and applies the principles of least privilege on a need-to-know basis (hmmm, sounds like Bletchley Park).

SDP creates a "black cloud" in which internal and external users are only able to discover and access a service if they have the right credentials. Only devices with the SDP client installed can access private apps and data. SDP expresses its objective as ABCD—"Assume nothing, Believe nobody, Check everything, Defeat threats."[9]

BeyondCorp

In 2015, Google introduced its BeyondCorp security model based on years of refactoring its own internal security architecture to a zero trust framework.

Early on, Google recognized the inherent risks of a perimeter-base security architecture in the increasingly mobile and cloud-centric world it was helping create.[10] BeyondCorp included browser context as part of its contextual identity verification. This allowed additional verification data points such as operating system and browser version, patch levels, and device management status to be factored into access control.

The BeyondCorp architecture also implemented a reverse proxy to hide the service details from the client. When a client makes a service request, the reverse proxy first encrypts the traffic and then checks device and user context. If all looks good, the proxy routes the client request to the service leaving the client blind to any characteristics of the server-side system.[10] Unlike a VPN or SDP, BeyondCorp's reverse proxy does not require the user to install or configure anything, making it a rather painless migration ... assuming you are using Google's cloud, of course.

ASA, CARTA, and ZTNA

In 2014, Gartner introduced its Adaptive Security Architecture (ASA) and extended it in 2017 with the continuous adaptive risk and trust assessment (CARTA) approach. CARTA refines the zero trust framework by extending identity verification to include context such as device, time, and location.[11] Since contextual identity is dynamic, access must be continuously evaluated, creating a gray "sometimes" area to the traditional black and white block-allow access model.

In 2019, Gartner extended ASA and CARTA into zero trust network access (ZTNA), which drew a distinction between client-initiated architectures, like SDP, and service-initiated architectures, like BeyondCorp. This latter category uses a connector in the same network as the protected service to take incoming requests from authenticated users or devices, verifies access to the target service, and then connects the client to the service. Today, ZTNA-based products and services are commonly used to phase out VPN-based access to high-risk services. Gartner predicts 60% of all VPN usage will be replaced by ZTNA by 2023.[12]

Zero Trust eXtended

In 2018, Forrester unveiled its Zero Trust eXtended (ZTX) ecosystem. While remaining true to its original zero trust roots, ZTX presents a control mapping framework that extends zero trust across an ecosystem of seven pillars: data, networks, people, workloads, devices, visibility and analytics, and automation and orchestration. For a product or service to be considered a ZTX platform, it must offer considerable capabilities on at least three of the pillars and provide an application programming interface to integrate with the remaining pillars. This framework provides reference points for security teams to analyze specific tools and technologies that best meet their unique business and operational needs.[13]

> Continuous identity verification across all transactions, even those inside the perimeter, eliminates the need for trust.

The zero trust security strategy, supported by a variety of implementation frameworks, has become a reality for a growing number of enterprises. A major impetus for zero trust adoption is breach prevention. As Kindervag quipped, "Executives don't get fired for ransomware attacks—they get fired for data breaches."[5] Zero trust spending will increase at 40% of companies in 2020, and 33% of enterprises are targeting zero trust adoption by early 2021.[8]

WHAT LIES AHEAD

Unfortunately, as zero trust initiatives climb up security priority lists, many (but certainly not all) security vendors have decided to update their marketing literature with a generous sprinkling of zero trust buzzwords before their engineering departments can create legitimate zero trust–based products. A common trend is to bend the zero trust definition to fit existing perimeter-centric products and services. As is often the case with many emerging technologies entering the market, the hype outruns the reality and customer confidence is eroded. Overmarketed fluff, coupled with a sparsity of experienced implementation expertise, has caused 43% of IT security teams to lack confidence in their ability to provide a zero trust architecture.[8] However, products will catch up, deployment expertise will grow, confidence will rise, and zero trust will move from avant-garde to mainstream.

Zero trust solutions will certainly evolve in the coming years as adoption grows. Kindervag predicts that "as tech gets better, the more fully the Zero Trust strategy can be realized."[5] We will see emerging technologies applied to zero trust frameworks to make it more automated, smart, and extendible.

Automated

As automation sweeps across all aspects of security operations, zero trust will be no exception. The recent popularity of security orchestration, automation and response (SOAR) products has paved the way for similar automation in zero trust implementation. SOAR already allows automated patching, systems, software and firmware updates, and automatic response to anomalous or known dangerous behavior. Zero trust architectures will extend this to automated user lifecycle management where user and non-human-entity identities are created, credentialed, de-credentialed, and deleted securely without operator intervention. Automated monitoring, visibility, and real-time dashboards will give

operators a live view of the security infrastructure, its behavior, trending, and identify possible threats. Ultimately, automation will allow for the point and click creation, alteration, and deletion of entire security infrastructures.

Smart

Artificial intelligence (AI) has found its way into every security use case, and zero trust solutions will be the next target. As identity verification becomes increasingly contextual, AI will play an expanding role to determine the dynamic risk of access. This will require a computational sophistication that a rules-based system simply cannot provide. Supervised and unsupervised deep learning, reinforcement learning, and genetic algorithms will not just apply lab-trained inference models but will also allow security solutions to adapt to changing enterprise behavior and learn from other companies as they encounter and defeat threats. Looking out further, generative adversarial networks will continuously verify the efficacy of zero trust protection by generating synthetic attacks and threats—chaos monkeys for security.

Extendible

Zero trust will increase its purview outside the enterprise. By design, zero trust is not limited by perimeters, which allows it to envelope a fuzzy and fluid security footprint. We already see zero trust extending beyond the traditional perimeter to protect cloud and mobile assets, but in the future, zero trust policies will span control into partner, supply chain, and regulatory platforms—no one is trusted.

As zero trust matures in the coming years, it will adjust to both new technologies and threats, but its elastic tenets and open framework will allow continual adaptation through the foreseeable future.

After a 10-year evolution, zero trust sees increased adoption across enterprises. Zero trust–based frameworks provide implementation roadmaps and enable security teams to make the paradigm shift from perimeter-centric architectures to default-deny, identify-based access regimes. Although zero trust solutions are today often clouded with marketing hype, they will mature and become the security strategy standard as they grow more automated, smart, and extended. Trust me.

REFERENCES

1. B. J. Copeland, *Colossus: The Secrets of Bletchley Park's Code-Breaking Computers*. Oxford, U.K.: Oxford Univ. Press, 2010.
2. J. Hawley, "Identity is the new perimeter," *PCWorld*, Sept. 17, 2012. [Online]. Available: https://www.pcworld.com/article/2010002/identity-is-the-new-perimeter.html
3. J. Kindervag, "No more chewy centers: The zero trust model of information security," Forrester Research Inc., Cambridge, MA, Rep. no. E-RES56682, 2010. [Online]. Available: https://www.forrester.com/report/No+More+Chewy+Centers+The+Zero+Trust+Model+Of+Information+Security/-/E-RES56682
4. S. Morgan, "Global cybercrime damages predicted to reach $6 trillion annually by 2021," *CyberCrime Magazine*, Dec. 7, 2018. [Online]. Available: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/#:~:text=Global%20Cybercrime%20Damages%20Predicted%20To%20Reach%20%246%20Trillion%20Annually%20By%202021,-Posted%20at%2016
5. M. Campbell, "Interview with J. Kindervag," unpublished, July 1, 2020.
6. R. Bird, "Identity is not the new cybersecurity perimeter: It's the very core," *Forbes*, June 14, 2019. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2019/06/14/identity-is-not-the-new-cybersecurity-perimeter-its-the-very-core/#45e19cc33abb
7. "What is zero trust?" Palo Alto Networks, Alviso, CA. Accessed on: July 6, 2020. [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture#:~:text=Zero%20Trust%20is%20not%20about,but%20instead%20about%20eliminating%20trust.&text=In%20Zero%20Trust%2C%20you%20identify,are%20unique%20to%20each%20organization
8. "2020 Zero Trust Progress report," Cybersecurity Insiders and Pulse Secure, Baltimore, MD, 2020. [Online]. Available: https://www.cybersecurity-insiders.com/portfolio/2020-zero-trust-progress-report-pulse-secure/
9. "Software defined perimeter," Cloud Security Alliance, Seattle, WA, 2020.
10. A. Wobler, "BeyondCorp: Borderless security for today's mobile workforce," TechRepublic, San Francisco, June 4, 2015. [Online]. Available: https://www.techrepublic.com/article/beyondcorp-borderless-security-for-todays-mobile-workforce/
11. C. Hines, "SDP, ZTNA, and CARTA: Making sense of the zero trust security buzz," ZScaler Blog, 2019. [Online]. Available: https://www.zscaler.com/blogs/corporate/sdp-ztna-and-carta
12. Gartner, "Zero trust architecture and solutions," Qi An Xin Group, Beijing, 2020. [Online]. Available: https://www.gartner.com/teamsiteanalytics/servePDF?g=/imagesrv/media-products/pdf/Qi-An-Xin/Qi-An-in-1-1OKONUN2.pdf
13. C. Cunningham, "The Zero Trust eXtended (ZTX) ecosystem," Forrester, Cambridge, MA, 2018. [Online]. Available: https://www.forrester.com/report/The+Zero+Trust+eXtended+ZTX+Ecosystem/-/E-RES137210

MARK CAMPBELL is the chief innovation officer for EVOTEK. Contact him at mark@evotek.com.