Is Zero Trust Attainable if You’re Not Google?

September 2021

By Justin Whitaker

Zero Trust as a concept has become almost fashionable, if not perceived to be routine, with the consequence of setting an unrealistic expectation that it is a table-stakes capability for any organization serious about cybersecurity. In part this is driven by the natural erosion of the security perimeter as more users work from anywhere and more applications live in the cloud. Popularized further by Google's Beyond Corp, CIOs, CTOs and CISOs have begun embracing its tenets and adding it to their strategic initiative roadmaps. We believe all organizations would be wise to pursue Zero Trust, but how practical is it to deploy at scale, at a reasonable speed, if you are not Google i.e., not a major tech giant or a large enterprise with deep pockets, within reach of a convenient pool of highly skilled computer scientists with PhDs, and a near evangelical appetite to invest heavily in this model?

Zero Trust is Complicated

The complication with Zero Trust starts with its definitions, and to a greater extent, not clearly defining what it is or means for your organization. While there are various flavors, they do share the following common characteristics: 1. Focus on assets and resources over network-based perimeters, 2. Continuous authorization and authentication in the form of sessions to access assets and resources, and 3. That trust is a vulnerability so "never trust, always verify". As the definition may imply, the goal is to continuously authenticate access and move away from traditional perimeter defenses that offer attackers the ability to more easily move laterally through an organization's systems once the network perimeter has been breached.

Zero Trust's complication gets further amplified as it sits alongside, and often competes with, hundreds of other controls that a cybersecurity organization must contemplate, many of which are equally complex and arguably as important. Is there greater risk reduction by investing in ZT or allocating spend towards security training and awareness since humans tend to be the weakest link? What about investment in advanced detection capabilities, resilience engineering, threat hunting, bug bounty programs, red teaming, adversarial emulation, supply chain and third-party management, and so on. To stress the point, NIST's popular CSF has more than one hundred controls (sub-categories) while their more exhaustive SP 800-53 series has nearly one thousand controls across 20 control families. Their latest publication's "summary table" is 37 pages long! We have yet to encounter an IT, Engineering, or Product organization that did not have cyber-allocated budget spread thinly across many of these controls, making many cybersecurity initiatives ineffective if not cleverly deployed and maintained. Consequently, this hinders progress towards Zero Trust at any reasonable pace or scale.

Zero Trust at Scale (“ZTS”) is complex to get right. The necessary ingredient list is exhausting, with many components and dependencies quite complicated on their own. The smattering of solutions, methods, components, systems, protocols and workflows working in harmony requires a wide variety of highly skilled teams each consisting of product owners, app owners, engineers, architects, developers, security practitioners, and system administrators working collaboratively across multiple business units.

Zero Trust has many options, ingredients, and dependencies

Single Sign-on (SSO)	Multi-factor Authn (2FA, MFA, Adaptive)	Device Trust	Endpoint Protection	Access Models (e.g., RBAC/ABAC)
Identity Management / Identity Provider (IdP)	Access Gateways / Reverse Proxies (HTTP/HTTPS)	Trust Inference / Trust Algorithms	Micro-segmentation / Micro-perimeters	Access Construct Taxonomy & Ontology
Active Directory (AD) / Modern AD	E2E Encryption (SSH, TLS)	Authn Protocols (OIDC, OAuth2, SAML, etc.)	Session Management	Users & Group Definition
Asset Management / CMDB	Cloud Access Security Broker (CASB)	Mobile Device Mgmt (MDM) / Enterprise Mobility Mgmt (EMM)	Virtual OS	Access Policy / Policy Engine
Protect Surface vs. Attack Surface	Crown Jewels Analysis	Visibility / Dynamic Workload Analysis (Layer 3 & 4 vs. 7)	Next-Gen Firewalls (NGFW)	Software Defined-WAN / Secure Access Service Edge (SASE)
Asset, App, Resource & Data Classification	E2E Encryption	Authn Types i.e., What you know, have, are, etc.	Principle of Least Privilege (PoLP)	User Lifecycle Management & Use Cases (J-M-L)
Application Enrollment & Offboarding	Authoritative Sources	Non-Authoritative Sources for Data Enrichment	Connections / Integrations	Roles & Entitlements / Privileges
On-Prem vs. Public & Private Cloud (Multi, Hybrid, etc.)	User vs. Headless Service Accounts	User Lifecycle Management & Use Cases (J-M-L)	Access / Audit Campaigns	Employees vs. Contractor vs. 3rd Party Access Rulesets

Figure 1. *Assortment of options, ingredients and dependencies to be contemplated on the road to ZTS*

Additionally, large organizations often have hundreds, if not thousands, of applications, systems, and resources that require protection - both on-prem and in the cloud - with access granted to, or being requested by, tens to hundreds of thousands of users. Layer on headless service accounts (systems that require access to other systems), and you have a security capability that to scale is massive to construct, deploy, and then care and feed for in a sustainable manner. Net: It is expensive!

Zero Trust is not Insurmountable

While a daunting challenge, ZTS is not insurmountable. Our observation across several organizations is they stumble in their ZTS journey by trying to do too much too fast across too large an attack surface, resulting in watered-down capabilities with highly porous defenses. In almost every case, spend could be better targeted and initiatives sequenced to attain a higher efficacy of risk reduction for the ZTS initiatives pursued. With that in mind, and assuming you are not Google-like, we recommend being hyper surgical in picking what is most important to protect, choosing solutions with the highest protection efficacy, while scaling and piecing together capabilities thoughtfully over time.

1. **Establish a Zero Trust Function:** The path to Zero Trust at Scale will require coordination and investment from multiple groups and stakeholders across the enterprise. However, there should be a single group accountable for establishing and owning the organization's Zero Trust strategy, governance and overall program. Whether it is in the form of a pillar, center of excellence, or other variation, there must be a group that owns the Zero Trust mission and is supplied with the resources, skilled talent, and leadership buy-in required to successfully drive a program of this scale and complexity.
2. **Hyper Focused on High Impact Assets:** Successful programs begin by knowing your most sensitive assets and data in terms of operational criticality, data sensitivity, as well as legal and regulatory obligations. Crown jewel analysis is stressed ad nauseum for almost all things cyber, but it remains absolutely critical for those who have limited budgets for cyber security. Focusing Zero Trust first on your most important assets (or more importantly consciously NOT doing zero trust for everything else) offers exponential risk reduction while optimizing spend. We have yet to meet an organization with a perfect CMDB or asset management function (often a federated mix of multiple solutions), so simply get started with those assets that are obviously high impact and of high importance.
3. **Single Sign On & Multi Factor Authentication:** SSO/MFA is a basic ingredient of Zero Trust. Aggressively front-end all high impact systems with SSO and MFA but manage

the change carefully as it introduces friction that will initially receive pushback which we have witnessed from the highest levels of an organization. Do not forget this also includes authentication controls for headless service accounts. If you are excited about this, then adaptive and passive MFA provide for a better user experience with less friction. In any case, if 2FA/MFA is not already deployed, this should be considered as a foundational priority.

4. **Device Trust:** Mobile devices are now ubiquitous with bring-your-own-device (BYOD) a trend that is likely to continue to grow at a rate faster than can be adequately protected. This has only been exacerbated by work-from-home where personal devices are used alongside work devices. Device trust has quickly moved up the ranks as one of the key requirements for enabling Zero Trust. Solutions such as enterprise mobility management (EMM), mobile device management (MDM), virtual mobility and endpoint protection, among others, should be a top priority for any Zero Trust program.

5. **Stop the Bleeding:** Legacy infrastructure and apps present many challenges on the journey to Zero Trust. We wish you luck with this class of resources as these solutions are often at, or near, end-of-life, brittle, with little desire to invest in them further. If they are part of the "crown jewels" then cyber risk mitigation and resiliency engineering is a must. In contrast, the introduction of any new resources is an opportunity to stop the bleeding by ensuring they are on-boarded "day 1" conforming to the organization's Zero Trust model and policy. This may require taking a relatively hard stance on the ability for business units and stakeholders to onboard applications and assets independently. The best organizations will solve for strict policy requirements by complementing this with highly streamlined and rapid processes for onboarding solutions, in accordance with policy, that begins upstream with procurement and incentives to curb shadow IT.

6. **Micro-segmentation:** Keep the walls up in perpetuity where practical, but surgically using micro perimeters. There is an argument to be made that there is still a place for perimeter defense as part of a defense-in-depth strategy, but likely in the form of micro-perimeters. Emerging is the concept of Secure Access Service Edge (SASE), Software Defined WAN (SD-WAN) and using Next-Generation Firewalls (NGFW) to filter and analyze traffic at the application layer. At a minimum it preserves yet another obstacle the baddies must breach. Tear them down when you are certain ZT can be maintained on an asset-by-asset resource-by-resource basis. Any sunsetting of these solutions would presumably be done when it has been determined that the spend exceeds the value of having multiple or redundant layers of security solutions as the care and feeding for these is not trivial.

7. **Access Architecture:** Mature the organization's access modeling (aka: RBAC, ABAC, etc.) capability iteratively, refining the construct as new use cases are presented. Emphasis should be placed on core and common access use cases to start, that can evolve as edge cases surface. Thoughtful taxonomy and ontology are a main ingredient in architecting a scalable solution, so careful examination and study here will go a long way.
8. **Principle of Least privilege:** Adoption of PoLP is a cornerstone of Zero Trust. This begins with policy and is then actualized by having a robust access model (RBAC and ABAC) coupled with a continuous stream of access campaigns, ideally executed more frequently for your highest priority assets.

The growing popularity and momentum behind Zero Trust should in no way assume it comes with an “easy button” and that any one solution is the solution. Assuming you are not Google-like, your organization will presumably be faced with much harder decisions in forming strategy, selecting solutions, and accepting larger trade-offs given the amount of investment that can reasonably be allocated. That said, how thoughtfully you consider selecting solutions based on security efficacy, how they are pieced together, in what order, and limiting this to what really matters, can act to accelerate risk reduction while inching closer towards Zero Trust at Scale.

For further information on this topic, please see “Governments Need to Stop Trying to Secure Their Networks” in the MIT Sloan Management Review, “Implementing a Zero Trust Architecture” from NIST, and/or “New Approach to Enterprise Security” from Google’s BeyondCorp website.

About the Author

Justin Whitaker is a Partner and Practice Lead of the DayBlink Consulting Cybersecurity Center of Excellence and is based in the McLean Virginia office.

Co-Authors

Michael Morgenstern is a Partner and Practice Lead of DayBlink's Cybersecurity Center of Excellence

Jacob Armijo is a Manager in DayBlink's Cybersecurity Center of Excellence

Please direct questions and comments about this report to cyber@dayblink.com

About DayBlink

In today's cybersecurity environment, the threat landscape is rapidly evolving.
It's outpacing the current defensive resources and skill sets of most corporations – meaning many companies are falling victim to attacks by malicious agents.

The way we do business is also changing – with more data stored, living in the cloud, and constantly demand on the go. Breaches can mean losing clients and customers overnight.

DayBlink works with clients to improve their security posture. We assess threats and vulnerabilities, identify organizational risk, prioritize remediation efforts, and implement solutions to secure IT environments and critical assets from sophisticated cyber-attacks.

DAYBLINK

For more information;
Visit: www.dayblink.com/services/technology/cybersecurity
Email: info@dayblink.com
Call: 1 (866) 281-4403