Assessing Security Architectures: Zero Trust vs. Network-Centric Models

As you explore security offerings for your organization, you'll come across the term "zero trust." Without a full understanding of both zero trust and the traditional, network-centric style of security that it displaces, you risk choosing a security architecture that fails to support your organization's digital transformation.

Zero trust architecture

Zero trust delivers secure, any-to-any connectivity without extending network access to anyone or anything. It cannot be built with network-centric tools like firewalls and VPNs. It functions based on the principle of least-privileged access, whereby users can only connect to the resources they need to do their jobs. A true zero trust platform is cloud-native and directly addresses the weaknesses of the network-centric model through a global, purpose-built cloud that serves as an intelligent switchboard, brokering direct connections between users, locations, and applications.

Network-centric architecture

Network-centric security is built primarily with tools like firewalls and VPNs. With this approach, a trusted network connects users, sites, and apps to facilitate access, and a secure perimeter is built to defend it—which is why it is sometimes referred to as "perimeter-based" architecture. As organizations undergo digital transformation, continuing to use this model requires extending the network perimeter to ever-growing numbers of remote workers, cloud apps, and more. However, this strategy creates significant complexity, cyber risk, and other problems as well.

There are many security offerings that may be labeled zero trust or cloud but still entail an underlying network-centric architecture. Learn how to accurately assess security architectures in this checklist so you can ensure you choose a platform that delivers on the promises of zero trust.

Key areas to assess for zero trust

There are five key aspects of zero trust architecture that you should evaluate during your selection process.

01

Attack surface reduction

- [ ] **No network extension required**

  Zero trust architecture provides direct-to-app connectivity. In other words, it does not need to extend network access to facilitate access to IT resources. Network-centric architectures extend the network to users, locations, devices, and clouds so they can access apps. That leads to a ballooning network with countless entry points that can be exploited by cybercriminals.

- [ ] **Elimination of public IPs**

  Unlike firewalls, zero trust does not require public IP addresses, which can be found by attackers on the web. Instead of using inbound connections and expanding the attack surface, zero trust uses inside-out connections. These involve connectors that sit in front of apps and reach out to a zero trust cloud, which then forges full connections between users and apps. Avoid platforms with connectors that can't support inside-out connections for all user connectivity scenarios (e.g., those involving agents, browser isolation, and branch traffic).

02

Compromise prevention

- [ ] **Proxy-based architecture**

  Zero trust is delivered through a proxy-based architecture that can perform full traffic inspection, discern access context and risk, and enforce real-time security policies to stop compromise. Network-centric, firewall-based architectures perform cursory scans instead of full traffic inspection, lack visibility into important contextual factors, and often allow connections to pass through unsecured. This results in reactive threat detection and response.

- [ ] **Cloud-native scalability to stop threats in encrypted traffic**

  A cloud-native zero trust platform offers the scalability needed to inspect encrypted traffic at scale and stop threats therein. This is important because more than 95% of web traffic today is encrypted, and inspecting it takes a high degree of performance. Network-centric models relying on fixed-capacity appliances (whether hardware or virtual) lack sufficient scalability and struggle to inspect encrypted traffic at scale, potentially resulting in undetected compromise.

03

Lateral movement prevention

- **Direct-to-application connectivity**

  Zero trust architecture provides access directly to apps rather than to the corporate network. This is critical to ensuring least-privileged access because threats that enter a network can move laterally across connected resources and expand the reach of their breaches. As the name implies, network-centric architecture involves network access and, as a result, enables lateral threat movement across that network.

- **Fully brokered connections**

  With fully brokered connections, a zero trust cloud plays the role of middleman for all enterprise traffic. It acts as an intelligent switchboard and stitches connections together so that authorized entities can access IT resources in a secure, one-to-one fashion. On the other hand, route-based connections and routable IPs indicate an architecture that puts users on the network, facilitating lateral movement.

04

Comprehensive data protection

- **Cloud-native scalability to secure data in encrypted traffic**

  As mentioned above, a cloud-native zero trust platform offers the performance required to inspect encrypted web traffic at scale. This allows it to find and secure sensitive data within said traffic that might otherwise leak. Network-centric architectures and appliances (whether hardware or virtual) struggle to inspect encrypted traffic at scale, meaning they fail to protect data within it.

- **Security for all data leakage paths**

  Data can be stolen or accidentally leaked through many channels other than encrypted web traffic, including email, endpoints, BYOD, SaaS, IaaS, and private applications. As part of securing any entity accessing any IT resource, a zero trust platform must be able to protect data in a least-privileged fashion across all of these leakage paths.

05

Cloud-native architecture

A cloud-born platform

Zero trust is delivered as a service from a purpose-built cloud that handles change implementation, ensures resilience, and provides rapid, automated service upgrades. This is markedly different from security offerings built on next-gen firewall VMs deployed in the public cloud. These entail laborious change implementation, manual resilience efforts, and time-intensive service upgrades that also require admin intervention when offerings are managed on-premises. Additionally, building a platform on top of firewalls inevitably constitutes a network-centric architecture—not zero trust.

Designed as a cohesive, comprehensive platform

When a cloud service is designed to be a comprehensive zero trust platform, new, integrated functionality is easy for the vendor to build and for the customer to deploy—eliminating point product appliances and complexity. So-called "zero trust" offerings built on top of NGFWs involve bolt-on point products that increase complexity and management overhead without actually delivering zero trust architecture.

Multitenancy

Multitenancy allows zero trust platforms to dynamically scale as needed to handle surging traffic loads. Additionally, policy updates propagate across the entire cloud in milliseconds, following users anywhere. Single-tenant offerings struggle to handle surge loads (even with auto scaling) and can take minutes to propagate policy changes across tenants at different sites, increasing risk exposure time.

Minimized private bandwidth requirements

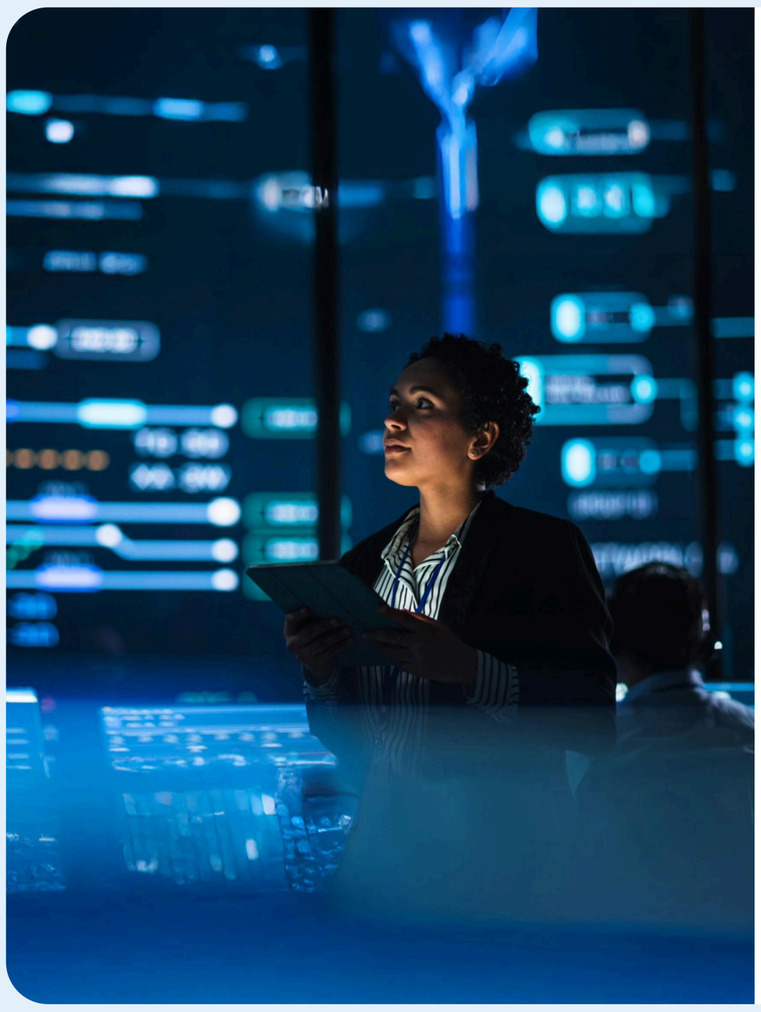
Unlike network-centric architectures, zero trust decouples connectivity and security from the network. By providing least-privileged, direct-to-app connectivity instead of backhauling traffic, organizations can use the internet as their network. This allows them to minimize the need for expensive private connections like MPLS, Azure ExpressRoute, and AWS Direct Connect.

Full compute points of presence (PoPs) at the edge

Zero trust is delivered as a service via full compute points of presence that process traffic and enforce policy at the edge. Ensure that your vendor of choice does not merely have on-ramp service edges that onboard traffic to their network so they can backhaul it to a distant compute site (which increases latency). Additionally, confirm that they provide digital experience monitoring (DEM) with full visibility across users' connections to further enhance digital experiences.

The Zscaler Zero Trust Exchange™ platform

Only Zscaler delivers a true zero trust architecture that checks every one of the above boxes. Zscaler is both the original pioneer and the continued driver of innovation in zero trust, with an extensible, cloud-native platform that was designed from the beginning to provide that architecture. This is drastically different from competing platforms with "zero trust" offerings built on top of firewalls and VPNs, which are telltale signs of a network-centric architecture that is inherently at odds with zero trust.



With Zscaler, organizations undergoing digital transformation receive a modern architecture that empowers them to:

01 Minimize the attack surface exposed to criminals

02 Stop any compromise in real time

03 Prevent lateral threat movement on the network

04 Protect all of their data wherever it goes

05 Leverage the benefits of a cloud-native platform

If you would like to see the Zscaler Zero Trust Exchange™ platform in action, request a custom demo today.

REQUEST A DEMO

To learn more about zero trust, join us for our webinar series, "Zero Trust, from Theory to Practice."

LEARN MORE