How to Evaluate Zero Trust Architecture

Zero trust is a unique architecture that provides secure, any-to-any connectivity without extending network access to anyone or anything. It is delivered as a service from a purpose-built cloud that acts as an intelligent switchboard, decoupling security and connectivity from the network.

As you explore zero trust offerings to modernize your organization's architecture, you're likely to wonder how you can choose the correct vendor. This can feel challenging given the architecture's broad, transformational nature, and its discontinuity with legacy methodologies and technologies that are at odds with zero trust.

Fortunately, you can base your research on the five pillars below as you shop for zero trust, empowering you to ensure that the platform you choose has everything you need for a complete, modern architecture.

Highly differentiated architecture 01

- **The ability to secure any-to-any connectivity**

  Organizations need a comprehensive zero trust architecture that secures any entity accessing any resource or application, including users, IoT/OT devices, workloads, branch sites, and third parties. But some vendors offer zero trust only for users accessing apps.

- **Fully brokered connections rather than route-based access**

  Zero trust requires fully brokered connections to ensure least-privileged access and keep entities off the network, where there is risk of lateral threat movement. Some vendors do not provide this for access scenarios involving SD-WAN and, instead, leverage routable IPs that are at odds with the principles of zero trust.

- **Comprehensive business continuity and resilience functionality**

  A zero trust platform must provide full business continuity capabilities across management and data planes to ensure resilient security and productivity. That's because a zero trust offering processes all of its customers' traffic and, as a result, is a mission-critical service for them.

Market leadership and innovation in cloud security

02

- **Ability to innovate and solve novel problems**

  Does the vendor have any “firsts” they can point to that demonstrate a history of consistent innovation? See if they paved the way with pioneering solutions that set the standard in their field and compelled others to follow their lead.

- **Concrete proof points for financial strength and stability**

  Publicly available financial data, like annual recurring revenue, free cash flow margin, and revenue growth year-over-year, will give a picture of a vendor’s market leadership and capacity to innovate, as well as its health, longevity, and ability to weather economic storms.

- **Investments dedicated to research and development**

  Innovation requires a great deal of financial focus. Learn how much money vendors dedicate to R&D each year to get a sense of their commitment to solving evolving problems and driving innovation in the cybersecurity space.

- **Third-party analyst praise about the vendor and their solution**

  Groups like Gartner and Forrester issue information about certain security vendors that lead in innovation. Look up reports and reviews from third parties to see if the zero trust platform you are considering has received recognition and awards.

Proven operational excellence

03

- **Architectural expertise with a proven track record**

  Proxying the entirety of an organization's traffic and delivering zero trust architecture as a service is a complex undertaking. Zero trust vendors must have a proven history of providing at-scale, inline security services.

- **Ample scalability that can handle both present and future demands**

  Zero trust offerings need high levels of scalability in order to secure the traffic (particularly the encrypted traffic) that large and growing organizations generate. Confirm the number of daily transactions processed by vendors’ platforms to understand their ability to scale.

- **Evidence that customers love the service**

  Quantifiable proof of customer satisfaction is a key requirement for any mission-critical service like zero trust architecture. Ask vendors for their Net Promoter Scores (NPS) in order to see and compare the average ratings from their customers.

Complete cyberthreat protection

04

Cybersecurity powered by cloud scale

Zero trust clouds that process large volumes of traffic can see and learn from countless cyberattacks targeting their customers. As such, they can quickly identify new threats targeting any customer and push updates to all customers to ensure they're safe from said threats. Make sure your platform of choice has this cloud scale.

Honeypots that lure hidden adversaries

For comprehensive threat protection, a zero trust platform must be able to detect attackers hiding in customers' ecosystems. Realistic decoys are needed to lure bad actors, generate high-fidelity alerts, and notify security teams of uncovered threats.

Identity threat detection and response

Cybercriminals frequently use compromised identities within organizations to launch cyberattacks. Zero trust platforms must provide continuous auditing of identity infrastructure, empower organizations to build identity hygiene, and detect identity threats in real time.

Built-in risk management

Zero trust architecture can only be complete if it includes holistic risk measurement and unified vulnerability management. In this way, organizations can visualize and understand their cyber risk and learn which weaknesses need to be remediated first.

Comprehensive data protection

05

AI-powered, automated data discovery

With AI, a leading zero trust platform can automatically find and classify sensitive data wherever it goes, across devices, networks, and clouds. Admins don’t need to configure any data loss prevention (DLP) dictionaries or classification policies, or duplicate rules across disjointed point products.

Agentless security for unmanaged devices accessing any application

Securing any-to-any connectivity includes securing BYOD and other unmanaged devices as they access any private or SaaS app. For maximum productivity and data protection, this should be done with agentless browser isolation, which prevents copying, pasting, printing, and downloading. Reverse proxies, the traditional approach, frequently break and have limited app catalogs.

Inline data protection for private applications

For a complete zero trust architecture, organizations need a platform that can enforce real-time data protection policies and prevent risky file downloads as users access private applications, whether they are hosted in the cloud or the data center.

Data security posture management across multi-cloud environments

Zero trust platforms need to be able to manage customers’ data security postures across public clouds. They must deliver granular insights into where data is stored, who can access it, how it is used, the risks and misconfigurations exposing it, and how said issues can be remediated.

Workflow automation

When data protection policies are violated, manual incident management is highly laborious. Zero trust offerings need workflow automation that streamlines incident response for all parties involved, and coaches end users so that they can learn to handle data more responsibly.

Armed with this guidance, you'll be able to sift through zero trust offerings that make attractive promises but struggle to fulfill them. Furthermore, Zscaler makes this selection process even more straightforward because it is the only zero trust platform that checks every box for modern organizations with modern needs. Zscaler is the original pioneer and continued innovator in zero trust, and its Zero Trust Exchange platform provides:

- Highly differentiated architecture
- Market leadership and innovation
- Proven operational excellence
- Complete cyberthreat protection
- Comprehensive data protection

Request a demo today to see zero trust in action with Zscaler.

Request a demo

To learn more about zero trust, sign up for the first installment in our webinar series: "Zero Trust, from Theory to Practice."

Learn more