White Paper

Private Equity and Cyber Resiliency: A Zero Trust Approach

For more than 80% of public and private companies, it's not a question of if a data breach will happen—it's when. Beyond that, most companies are likely to suffer more than one breach. These come at a high cost, with estimates ranging from US$4.3 to 9.4 million per significant breach.[1]

Corporations worldwide face increasingly frequent and sophisticated cyberattacks, especially with the involvement of nation-states and organized cybercrime syndicates. While public company breaches make headlines, the risk is equally prevalent in the Private Equity (PE) industry, and growing, as threat actors pursue target-rich zones[2] and explore vulnerabilities in their mostly mid-market, underprepared, and less sophisticated portfolio companies.

In the last two decades, the PE industry has evolved into a force to be reckoned with. Record fundraising and $2.5 trillion[3] in dry powder availability have allowed PE firms to expand their portfolios at an unprecedented pace. In 2021, some 27,000 out of 62,000 reported M&A and carve-out transactions (around 45%) were PE-led. In 2022, PE firms manage more than $5 trillion in capital and own more than 20,000 businesses around the globe that employ an estimated 25 million people.

With the increasing deal volume, rapid expansion, and global reach of private equity, PE limited partners (LPs) and portfolio company management teams are overwhelmed to address the business continuity, reputational, brand, and investment risks resulting from anticipated cyberattacks.

Today, most PE firms and PE-backed portfolio companies have a fragmented approach to cybersecurity. Some firms have implemented baseline security controls (multifactor authentication [MFA], VPNs, firewalls, etc.), but there is a lack of uniformity and consistency. Moreover, these firms continue to lag behind on end user security awareness and training.

More progressive PE firms and their LPs are prioritizing cyber risk management and evaluating various approaches to prevent successful attacks, such as zero trust and compliance with various standards like NIST and COBIT. These proactive measures include introducing portfolio-wide cyber resiliency programs, investing in monitoring tools, establishing baseline standards, performing quarterly reviews, and partnering with advisory and technology providers.

Security industry experts agree, however, that the most effective approach is to prevent an attack from happening in the first place. This has led PE firms to take up a zero trust approach to secure their users, devices, and applications. Based on the maxim "never trust, always verify," trust is never implicit in a zero trust model, and access is granted on a need-to-know, least-privileged basis defined by granular policies. According to Dell research, only 12% of companies have fully implemented zero trust, while 79% are discussing or in the process of driving toward it.[4]

[1] IBM, Cost of a data breach 2022.

[2] Erie Street Growth Partners, As Cyber Risks Increase for Private Equity, Performance Improvement Partners, an Erie Street Company, Launches Cybersecurity Guide for the Private Equity Sector.

[3] Ibid.

[4] Dell, Global Data Protection Index Report.

The National Institute of Standards and Technology (NIST), an agency of the US Department of Commerce, has defined the core tenets of zero trust[5]:

Network Identity Governance

- All resource authentication and authorization are dynamic and strictly enforced before access is allowed.

Endpoint Protection

- All data sources and computing services are considered resources.
- The enterprise monitors and measures the integrity and security posture of all owned and associated resources.

Data Flow

- All communication is secured regardless of network location.
- Access to individual enterprise resources is granted on a per-session basis.
- Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
- The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

This definition and NIST Special Publication 800-207 aim to help security architects and other security stakeholders understand the key components of a zero trust architecture so they can design and implement similar processes in their organizations. Various federal agencies have long been urged to move away from perimeter-based security to a security strategy based on zero trust. With today's technologies and capabilities, it is more feasible to control access based on granular and dynamic conditions, and more organizations are opting for this approach.

The Zscaler zero trust architecture aligns with these core principles by ensuring that organizations can:

- **Verify identity based on context (Network Identity Governance):** The Zscaler platform provides access to users based on identity and context, which can include IdP, location, device, device posture, and other characteristics.
- **Control and monitor risk across users and devices (Endpoint Protection):** The Zscaler platform validates endpoint device identity, monitors access, and checks endpoint security posture before allowing an inside-out connection (e.g., application-to-user microtunnel).
- **Sit in line with traffic and enforce policy (Data Flow):** Sitting in line with traffic, the Zscaler platform can enforce appropriate policies and perform full TLS/SSL inspection to ensure any data flow between source and destination is secure. Concurrently, Zscaler can also collect and report on various characteristics of an endpoint to ensure it meets organizational standards.

[5] NIST, Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators.

Why Zscaler?

The Zscaler zero trust architecture is ideal for PE firms and their portfolio companies, providing a robust framework to design security with a consistent approach for organizations of all sizes.

The following table shows some common elements of PE firms and portfolio companies, mapped to how Zscaler helps in each of these areas.

PE PortCo Initiatives & Objectives	How Zscaler Helps
Drive consistent security controls and security posture across the Portfolio	Standardize security controls and drive harmonization across individual PortCos through a singular cloud native control plane
Identify and implement value creation initiatives	Consolidates individual point products e.g. VPN, firewalls, MPLS and improves EBITDA / underlying IT costs
Adopt a cloud first strategy	Platform enables cloud transformation and eliminates legacy network infrastructure
Scale and grow platform investments through bolt-on or add-on acquisitions	Enables rapid integration of bolt-on acquisitions to help PE-backed PortCos grow and scale

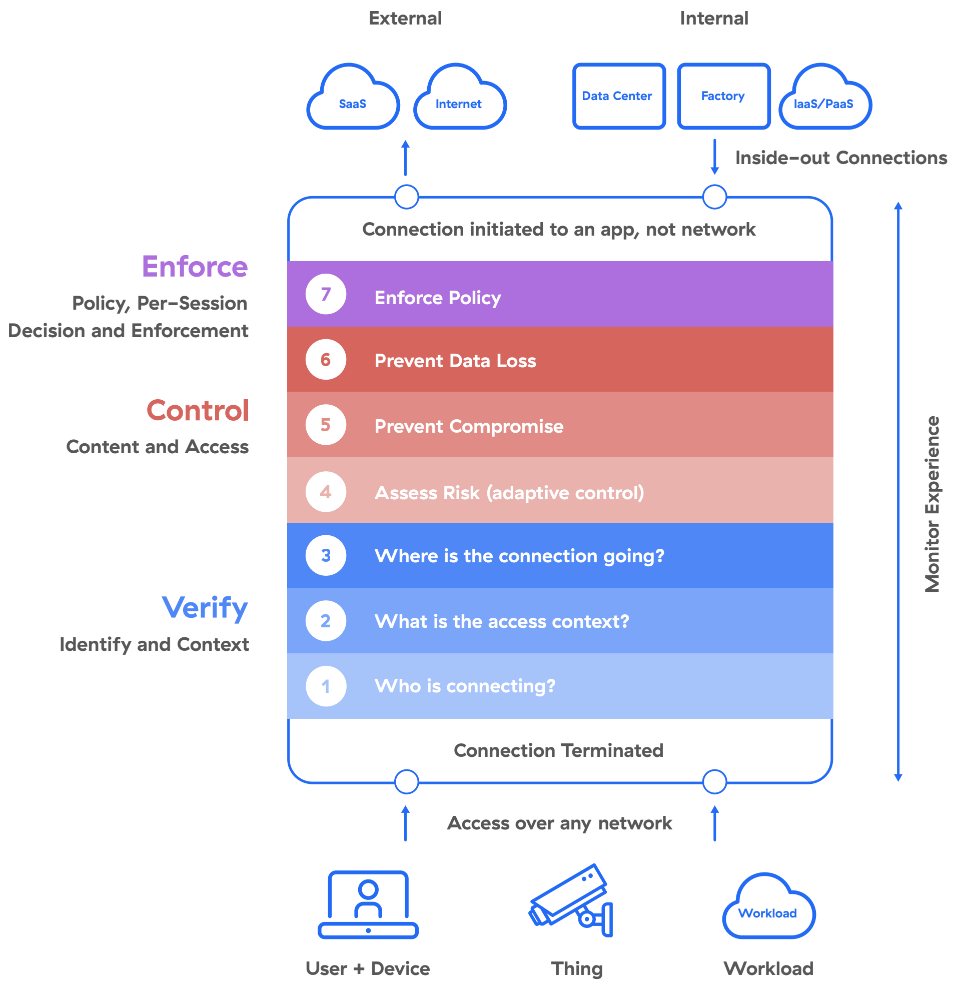

Figure 1: The Zscaler zero trust architecture

The value of Zscaler

For more than 15 years, Zscaler has helped PE firms and PE-backed portfolio companies become more cyber resilient and drive value creation opportunities. Specifically, Zscaler has helped PE-backed portfolio companies:

- **Mitigate and control cyber risks:** Many Zscaler customers have seen their attack surface shrink by as much as 85%. For PE-backed PortCos, Zscaler for Users enables rapid improvement in security posture to protect the company's crown jewels.
- **Drive digital value creation:** Zscaler helps PE-backed PortCos reduce IT spend on legacy network and security point solutions, which can improve EBITDA—customers have reduced their network and security spend by as much as 30—40% after removing MPLS, VPN, and other point products.
- **Accelerate time to value:** By leveraging Zscaler to connect users to applications without combining networks, PortCos can rapidly integrate platform-type acquisitions to achieve scale. Customers have seen overall integration timelines cut in half by eliminating the IT/network integration component.

As the threat landscape continues to evolve and macroeconomic pressures mount, PE firms and their portfolio companies will need to prioritize value creation and preservation. The Zscaler zero trust architecture has proven to enable cyber resiliency and secure digital value creation like no other approach.

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.