KEYNOTE INTERVIEW

Never trust, always verify

Changing your cyber-approach from simple network security to zero trust can reduce risk, improve EBITDA and lead to value creation, say Zscaler's Akshay Grover and AJ Watson

SPONSOR
ZSCALER

Q Why has cybersecurity taken center stage for private equity firms?

Akshay Grover: Let's start with some startling statistics. An average PE firm suffers a minimum of two to three cyber-incidents each month, at least one exploit per year, and it is predicted that an average of one in four middle-market firms will fall victim to a cyber-breach each year. Clearly, there is an increasing prevalence of cyber-threats which is driving a focus on cybersecurity.

PE firms handle sensitive information and data, making them an attractive target for cyber-criminals. Additionally, cybersecurity threats are evolving and becoming more complex. Regulations and standards around data protection and cybersecurity have also been increasing in recent years. Failure to comply can result in significant financial and reputational damage.

A large portion of the risk exists at the portfolio company level, as they are diverse in terms of industry, size, geographic location and maturity. PE firms have an expanded risk profile as they are responsible for ensuring that portfolio companies are secure and protected from cyber-threats.

Most progressive PE firms are also realizing that effective cybersecurity can create value for portfolio companies through cost savings and accelerated time-to-value. By improving cybersecurity measures, PE firms can improve a company's overall resilience and protect its employees, assets, reputation, business and investment, thereby enhancing the company's value and generating higher returns on exit.

Q What approach is private equity taking to mitigate and control cyber-risk?

AG: PE firms are generally taking a proactive and multi-faceted approach. In due diligence, for example, firms will typically embark on a thorough review of a target company's cybersecurity practices, which may include an assessment of the target's cybersecurity policies and procedures, and analysis of past cyber-incidents.

Post-acquisition, PE firms then work with portfolio companies to develop and implement strong cybersecurity policies, procedures and controls that are tailored to the specific risks and needs of the business. This may include training employees on best practices for maintaining security, establishing incident response plans and implementing technical controls such as firewalls, encryption and multi-factor authentication.

Additionally, regular monitoring and testing of existing measures is common and ensures they remain effective, including security audits and vulnerability assessments, as well as ongoing training and awareness efforts. Firms may also invest in cybersecurity technologies and expertise to help their portfolio companies stay ahead of threats and maintain a strong security posture, either using outside consultants or by hiring dedicated cybersecurity staff. But, of course, despite best efforts, PE firms and their portfolio companies may still be targeted. To mitigate the impact of these incidents, firms may develop and maintain detailed incident response plans that outline how to respond to and recover from a cyberattack. Having said that, the easiest way for PE firms and portfolio companies to prevent cyberattacks and achieve cyber-resiliency goals is to implement a zero-trust model.

Q What is zero trust and why is it so beneficial?

AG: True zero trust is a cybersecurity strategy whereby security policy is applied based on context established through least-privileged access control, strict user authentication and business policy enforcement, rather than assumed trust. It's an overhaul of the old proverb "never trust, always verify."

However, today companies across the industry are misusing the term zero trust, which is causing confusion. There are some fundamental differentiators to a true zero-trust platform: First, true zero trust takes a proxy approach, meaning all connections are terminated at the platform level. Second, all traffic is inspected, and user identity is verified. Third, users will only be connected to the application – based on business policies – and never to the network. Fourth, many analyst firms recommend zero-trust architecture should be cloud native.

AJ Watson: The reality is that very few companies currently adhere to all facets of that definition of zero trust. Yet it is becoming increasingly relevant in an era of working from anywhere and applications moving to the cloud. Five to 10 years ago, everyone would have been connecting from HQ or a branch office through their corporate network.

Q What are the impediments to adopting zero trust?

AG: The number one impediment to adopting zero trust is a legacy mindset. There is a dogma associated with the past 30 to 40 years of network security that prevents a new way of thinking. There are also several misconceptions around zero trust, including the idea that it can't or won't work with homegrown and legacy applications; that it comes with high costs; creates a poor user experience; and requires substantial change management. Those misconceptions can lead some organizations to call it quits before they have even got started. However, none of the misconceptions are true and the potential benefits in terms of risk mitigation, better user experience, reduced costs and value creation are huge.

Q How does a zero-trust approach add value?

AW: From a value creation perspective, the zero-trust approach is a huge contributor to EBITDA improvement. There are several key drivers of cost savings, including minimizing MPLS spend and consolidating or replacing point products. Second, this approach reduces IT overhead by eliminating the need for unique skills required to maintain point products. Third, it reduces operational complexity and cyber-insurance premiums by using simple, direct-to-app connectivity and automating repeatable tasks. Finally, zero trust can speed up time-to-value for PE bolt-on acquisitions or carve-out stand-ups.

Q What advice would you offer private equity firms preparing to embark on a zero-trust journey?

AG: First off, PE firms and their portfolio companies are not alone – our recent survey showed that 90 percent of organizations migrating to the cloud have implemented or are implementing a zero-trust strategy in the next year.

Implementing zero-trust architecture should not be a daunting experience. Yes, it does challenge the status quo of existing infrastructure and IT functions, but undertaking a zero-trust journey should not be so large and all-encompassing that it makes your organization freeze up.

When designing zero-trust architecture, security and IT teams should first focus on answering two questions: what are you trying to protect and from whom are you trying to protect it? The most effective approach is to layer technologies and processes on top of your strategy and not the other way around.

It is important to take a phased approach, which may take months or quarters. Start with your most critical assets – your crown jewels – before implementing zero trust more broadly. It won't happen with the flip of a switch.

AW: Education is a critical part of the journey, as is change management. We find it helpful for PE firms to bring their portfolio companies together to learn about zero trust. The chances are that many fellow portfolio companies would have explored or implemented zero trust and could share best practices. Ask any enterprise undergoing its zero-trust journey where to start and the answer will be: "Start somewhere, anywhere, but just start." ■

Akshay Grover is global M&A, divestitures, and private equity practice lead and AJ Watson is a senior manager in the private equity practice at Zscaler