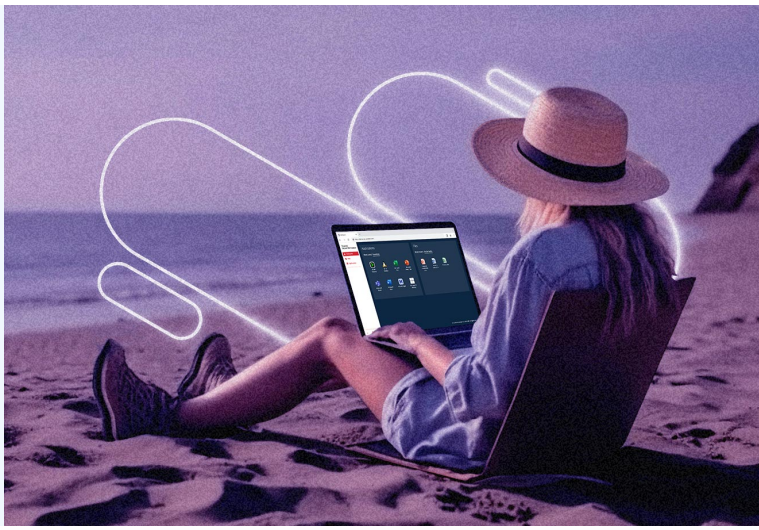
Parallels® Secure Workspace

The evolution of Zero Trust in 2024 and beyond

Adoption trends, budgetary insights, and essential technologies for organizations at any stage on their Zero Trust journey.



The Zero Trust landscape

Zero Trust, once a straightforward cybersecurity concept, has transformed into a strategic imperative for businesses of all sizes and scales.

This paper delves into the ever-changing landscape of Zero Trust, offering insights into its evolution, adoption trends, budgetary considerations, and essential technologies.

The evolution of Zero Trust

Zero Trust, initially coined by Forrester Research in 2010, has witnessed a remarkable evolution over the years. The concept was born as a response to the outdated security perimeter model, focusing on the principle of "never trust, always verify."

Over the years, the foundation of Zero Trust has solidified, emphasizing continuous monitoring, strict access controls, and a data-centric security approach.

Adoption trends

Zero Trust adoption has surged across industries, fueled by the growing awareness of evolving threats. According to a recent survey conducted by Cybersecurity Insiders, 72% of organizations have either implemented or are actively planning to implement Zero Trust principles into their cybersecurity strategies.

This momentum is consistent with Gartner's findings and prediction that by 2025, more than 60% of enterprises will phase out their network-centric strategies in favor of Zero Trust.

Budgetary data

Budget allocations reflect the increasing importance of Zero Trust. In a study by Enterprise Strategy Group (ESG), 58% of organizations reported that they had already increased their cybersecurity budgets to accommodate Zero Trust initiatives.

Moreover, a survey by IDC found that companies were willing to spend 13% of their total cybersecurity budgets on Zero Trust technologies in 2022, a number that is likely to grow as organizations understand how Zero Trust protects revenue and more. This budgetary shift underscores the acknowledgment of Zero Trust's significance in modern cybersecurity.

Essential technologies for all businesses

The following technologies and concepts all play a role in a comprehensive, strategic approach to Zero Trust.

Multi-factor authentication (MFA): MFA remains a cornerstone of Zero Trust, ensuring that user identities are verified through multiple authentication factors. In fact, the Verizon 2022 Data Breach Investigations Report found that 85% of breaches involve compromised credentials, highlighting the critical role MFA plays in securing access.

Micro-segmentation: Segmentation at the network level is fundamental to Zero Trust. Implementing micro-segmentation helps in minimizing lateral movement within the network, enhancing security. A study by Gartner reveals that 60% of organizations will adopt micro-segmentation as part of their Zero Trust strategy.

Continuous monitoring and behavioral analytics: Real-time monitoring and the use of behavioral analytics are critical to identify anomalies and suspicious activities. Businesses should invest in tools that provide insights into user behavior. The 2022 State of Cybersecurity report by ISACA highlights that 67% of organizations plan to increase investments in behavioral analytics.

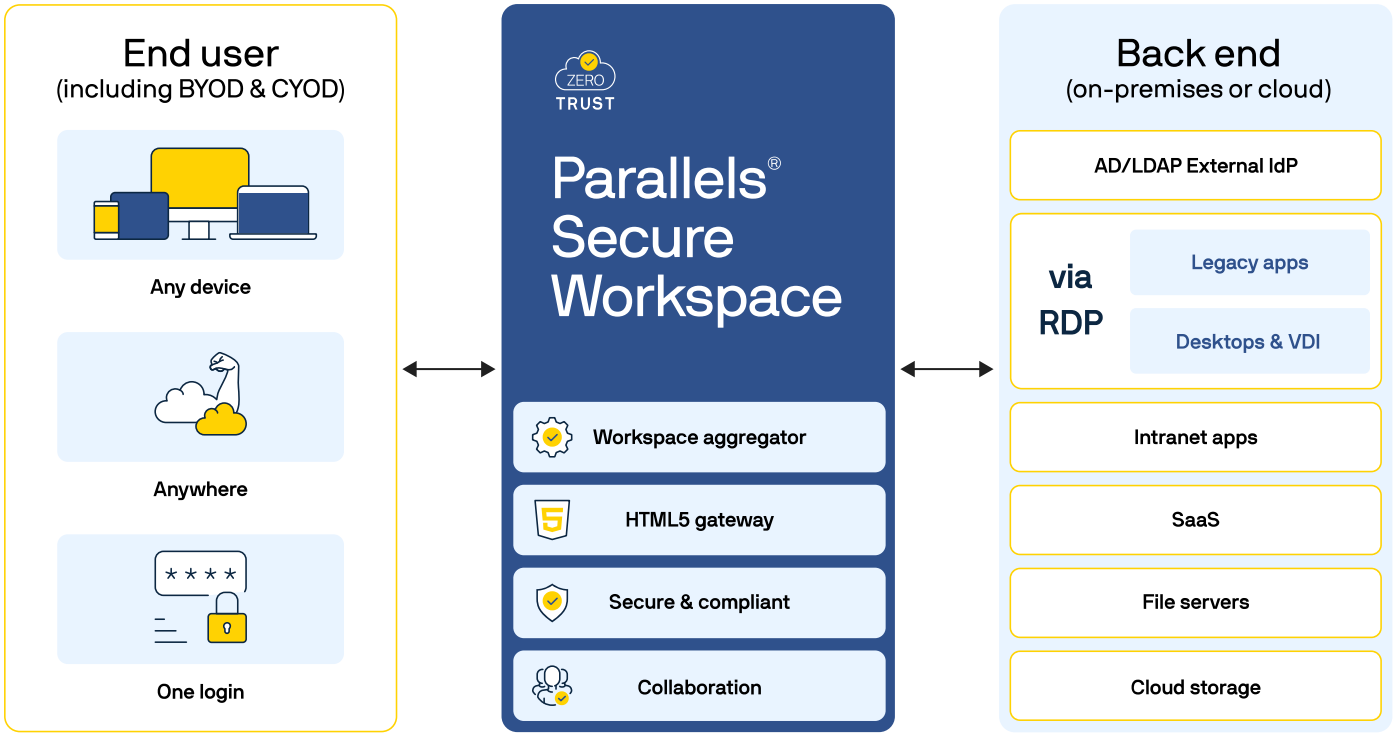
Endpoint detection and response (EDR): EDR solutions are essential for protecting endpoints and rapidly responding to threats. Small businesses can opt for cloud based EDR solutions, while larger enterprises may prefer more comprehensive offerings. According to CrowdStrike's 2022 Global Threat Report, EDR solutions detected 68% of all targeted intrusion activity.

Data encryption and tokenization: Protecting data at rest and in transit is paramount. Encryption and tokenization technologies ensure data remains secure even if accessed by unauthorized parties, making them indispensable for businesses of all sizes. The 2022 Cost of a Data Breach Report by IBM states that businesses with encryption experienced $340,000 less in data breach costs.

Identity and access management (IAM): Robust IAM solutions are essential for managing user access privileges efficiently. Businesses should adopt IAM systems to ensure only authorized users access critical resources. A study by Gartner predicts that 90% of organizations will implement at least one form of advanced IAM by 2024.

Zero Trust network access (ZTNA): ZTNA solutions replace traditional VPNs, allowing secure remote access without compromising security. This technology is vital for businesses adapting to remote or hybrid work models. According to Gartner, by 2023, 60% of enterprises will have replaced their remote access VPNs with ZTNA.

Securing end users on the internet



In addition to securing internal networks, Zero Trust must extend its focus to securing end users as they traverse the internet. This includes implementing Secure Access Service Edge (SASE) solutions that combine network security and wide-area networking to ensure consistent security for remote users.

Value of Zero Trust vs. cyber education and training

While cyber education and training are crucial components of a comprehensive cybersecurity strategy, data and trends indicate that a Zero Trust approach is more effective in today's threat landscape.

Despite education and training efforts, human error remains a significant factor in security breaches. Zero Trust, on the other hand, enforces strict access controls and continuous monitoring, reducing the impact of human-related vulnerabilities.

This is evident in the fact that 85% of security breaches involve compromised credentials, underscoring the need for robust access controls and authentication mechanisms provided by Zero Trust.

The future of Zero Trust

Zero Trust is characterized by rapid evolution, widespread adoption, and a fundamental shift in budgetary priorities. It is no longer just a buzzword, but a necessity for businesses of all sizes and scales to protect their digital assets in an increasingly hostile cyber landscape.

By investing in the essential technologies mentioned above and adhering to Zero Trust principles, organizations can enhance their cybersecurity posture. With Zero Trust, organizations can better secure end users on the internet and adapt to the ever-changing threat landscape with confidence.

Ready to start, continue, or further enhance your Zero Trust journey?

Get your free trial of Parallels Secure Workspace now.