Enterprise Strategy Group by TechTarget

ECONOMIC VALIDATION

Economic Benefits of a Zero Trust Approach with Okta and Palo Alto Networks

See How Your Organization Can Reduce Operational Costs by 33% and Achieve a 122% ROI

By Jennifer Duey, Economic Validation Analyst
Enterprise Strategy Group

January 2025

Contents

Enterprise Strategy Group by TechTarget

Economic Validation: Key Findings Summary

Validated Benefits of Okta + Palo Alto Networks

Up to 33% lower operational costs

Increased visibility for fast identification of critical insights

122% Return on Investment (modeled)

- **Reduce business risk**: **Okta + Palo Alto Networks helped organizations reduce business risk by adopting a zero trust approach, integrating advanced identity management with comprehensive threat prevention. Organizations can achieve secure access controls, continuously verify users, and minimize vulnerabilities, delivering reliable protection against evolving threats.**
- **Improve operational efficiency: Okta + Palo Alto Networks helped customers increase operational efficiency, freeing up time for more strategic initiatives.**
- **Faster time to value: Okta + Palo Alto Networks helped organizations accelerate the deployment of identity services, automate threat remediation, and leverage cloud-native architecture, helping businesses achieve faster time to value and reduce delays in securing critical operations.**

Introduction

This Economic Validation from TechTarget's Enterprise Strategy Group focused on the quantitative and qualitative benefits organizations can expect by implementing zero trust across your hybrid IT environments with Okta and Palo Alto Networks rather than using many point solutions.

Challenges

Modernizing cybersecurity strategies is imperative to keep pace with IT advancements, and zero trust architecture has emerged as the leading approach to achieving this objective. According to research from the Enterprise Strategy Group, 50% of IT leaders identify the modernization of cybersecurity programs as a primary driver for adopting zero trust strategies, while 32% of organizations pursuing digital transformation increasingly rely on zero trust to support this transition.[1] However, achieving and maintaining zero trust presents significant challenges. The evolving nature of cyberthreats and the complexities of implementing multiple point solutions create substantial hurdles, further compounded by cybersecurity staffing shortages that make it difficult for organizations to maintain robust security measures. The rise of hybrid and remote workforces exacerbates these challenges, as employees demand seamless, anytime-anywhere access, requiring a delicate balance between accessibility and stringent security measures to ensure smooth business operations and data protection. Key issues complicating zero trust implementation include the security vulnerabilities introduced by remote and hybrid workforces, the risks posed by unmanaged devices and contractor access, and the operational complexity of managing interconnected network, cloud, and identity security policies. Addressing these challenges often increases IT ecosystem complexity, leading to higher costs, redundant systems, and administrative burdens, ultimately hindering business growth and elevating risk. Enterprise Strategy Group research shows that this rising complexity is attributed to cybersecurity landscape changes, adoption of emerging technologies, support for hybrid and remote work, and ongoing digital transformation initiatives.[2]

In response, organizations are channeling their investments to circumvent these problems. IT leaders are focusing on improved cybersecurity (44%), enhanced business processes and workflows (36%), and enabling digital transformation (33%) as justifications for their IT spending (see Figure 1).[3]

[1] Source: Enterprise Strategy Group Research Report, *Trends in Zero Trust Strategies and Practices Remain Fragmented, but Many are Seeing Success*, March 2024.
[2] Source: Enterprise Strategy Group Complete Survey Results, *2024 Technology Spending Intentions Survey*, February 2024.
[3] Ibid.

Figure 1. Top Drivers for Increased IT Complexity

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

While reducing overall complexity requires more than just adding the latest technology, many IT environments already possess the necessary components to streamline their operations. The challenge lies in integrating multiple point solutions into a cohesive framework that enhances simplicity and efficiency. Solutions that combine existing technologies can unify disparate systems and create a more streamlined and secure IT environment. By leveraging such integrated solutions, organizations can optimize their current investments and reduce complexity without the need for extensive new implementations.

The Solution: Zero Trust with Okta and Palo Alto Networks

Okta and Palo Alto Networks integrate their solutions to support organizations in implementing a zero trust security framework. This approach ensures that no entity, internal or external, receives implicit trust and that access to resources is granted only after verification.

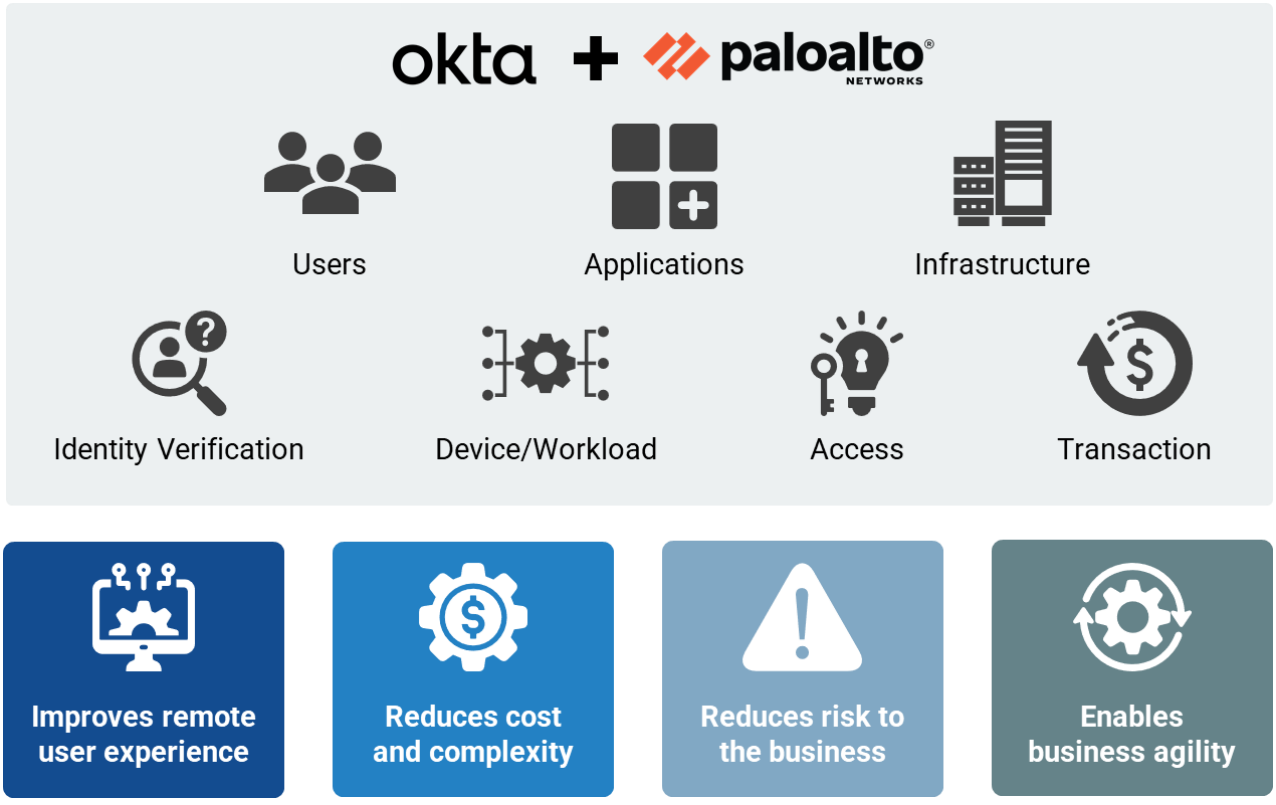
Okta provides identity-driven access control through centralized single sign-on, adaptive multi-factor authentication (MFA), and lifecycle management. These tools authenticate users based on factors such as location, security

posture, and behavior. Okta automates provisioning and deprovisioning to help reduce the risk of excessive privileges and to maintain a controlled attack surface.

Palo Alto Networks contributes to this framework with network and endpoint security capabilities. Its Next-Generation Firewalls apply user-specific policies, Prisma Access extends access controls to remote and hybrid environments, and Cortex XSIAM extended security intelligence and automation management (XSIAM) and extended detection and response (XDR) monitor endpoints to detect and mitigate threats. These tools work together to support continuous monitoring and enforcement across diverse environments.

Integrating Okta and Palo Alto Networks establishes workflows that align with zero trust principles. When a user attempts to access a resource, Okta verifies their identity using MFA and contextual data. Palo Alto Networks monitors the session, applying behavior analysis and threat intelligence to identify risks. If a threat is detected, the system can dynamically adjust policies, such as prompting the user for additional authentication or isolating the session. Microsegmentation limits user access to authorized resources, reducing the risk of lateral movement and enforcing least-privilege principles.

Figure 2. Okta + Palo Alto Networks



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Enterprise Strategy Group Economic Validation

Enterprise Strategy Group completed a quantitative economic analysis of implementing Okta and Palo Alto Networks for zero trust. Our process is a proven method for understanding, validating, quantifying, and modeling a product or solution's value propositions. The process leverages Enterprise Strategy Group's core competencies in market and industry analysis, forward-looking research, and technical/economic validation.

Enterprise Strategy Group conducted in-depth interviews with implementors/architects to assess and quantify the effect of Okta and Palo Alto Networks on advancing zero trust modernization within their organizations. We conducted a comprehensive evaluation encompassing vendor-generated technical documentation, established case studies, independent analyses, and our team's expert insights into the industry, markets, and alternative technologies. The qualitative and quantitative data were then used for a simple economic analysis comparing the costs and benefits of implementing the Okta and Palo Alto Networks zero trust strategy.

Why This Matters

Organizations have rapidly adopted tools and technologies to meet evolving cybersecurity demands, often creating fragmented, overly complex IT environments. This patchwork approach has left systems more vulnerable, providing opportunities for threats to exploit security gaps.

A zero trust strategy offers a parallel path, enabling organizations to streamline their IT landscape, close security vulnerabilities, and strengthen risk management.

Zero Trust with Okta and Palo Alto Networks Economic Overview

Enterprise Strategy Group's economic analysis of a zero trust strategy with Okta and Palo Alto Networks found that it provided its customers with significant savings and benefits in the following categories:

- **Reduced business risk.** Organizations can integrate advanced identity management with comprehensive threat prevention with Okta and Palo Alto Networks to secure resource access and reduce business risk.
- **Improved operational efficiency.** Okta and Palo Alto Networks required less effort from businesses by simplifying user authentication and access control while automating threat analysis and response.
- **Faster time to value.** By providing rapid identity services deployment, automated threat remediation, pre-integrated solutions, and cloud-native architecture, organizations can realize faster time to value.

Reduced Business Risk

Reducing business risk in hybrid and multi-cloud environments requires addressing the growing complexity of security threats and access management. As organizations expand, fragmented tools and processes can leave vulnerabilities unchecked, increasing the potential for breaches, data loss, and compliance violations. The constant evolution of user identities, devices, and applications demands seamless coordination among IT, security, and network teams to enforce access controls and mitigate risks effectively. Without unified solutions, organizations face inconsistent security policies, manual processes prone to errors, and a lack of visibility into critical systems. By implementing Okta for identity management and Palo Alto Networks for comprehensive security, organizations can adopt a zero trust approach, centralize threat detection and prevention, and enforce consistent security measures across environments. This unified strategy reduces vulnerabilities, protects sensitive data, and prevents unauthorized access, mitigating business risk. Customers reported savings and benefits in the following areas:

- **Reduced security incidents.** As businesses expand their digital operations and adopt hybrid and multi-cloud networks, their growing attack surface provides more opportunities for cybercriminals to exploit vulnerabilities and target identity-based threats. Advanced persistent threats, ransomware, and phishing campaigns increasingly overwhelm traditional security measures, significantly increasing the risk of breaches. Customers reported minimizing successful breaches and blocking malicious activities by combining Okta's Adaptive MFA capabilities with Palo Alto Networks' comprehensive security solutions. Okta's Adaptive MFA actively identifies potential threats by analyzing risk signals such as IP address, device, and geographic location, dynamically adjusting authentication policies by escalating MFA requirements for high-risk scenarios or by enabling passwordless access for low-risk cases. Palo Alto Networks secures hybrid

> **"These technologies give us the tools to manage security more effectively, helping us stay in control and better protect what matters most."**

environments, providing reliable threat protection and reducing security incidents, with customers reporting 92% of alerts automatically resolved to streamline operations and reduce alert fatigue.

- **Reduced risk of noncompliance.** The risk of noncompliance presents significant challenges for organizations, affecting financial stability, operational efficiency, and reputation. Regulatory violations can result in steep fines, legal fees, and resource-intensive audits, diverting attention from strategic priorities. Many enterprises require MFA to enhance security for critical systems or meet compliance mandates like HIPAA and PCI DSS. However, implementing MFA often involves time-consuming and disruptive rearchitecting of application login processes. By integrating Okta's identity management with Palo Alto Networks' security platform, organizations benefit from a unified security product that ensures a seamless user experience. Customers reported that the combined solutions enabled them to align their specific business requirements for audit and regulatory adherence, simplify reporting processes, and gain deep, accessible insights into their technical architecture, ultimately making compliance easier to achieve.
- **Reduced risk of business disruption.** Business disruption poses significant risks to an organization's operations, productivity, and stability. Palo Alto Networks and Okta actively mitigate these risks by delivering advanced security and streamlined identity management. Palo Alto Networks protects critical systems with robust threat detection and prevention capabilities, while Okta ensures seamless and secure access to resources, even during unexpected events. Their cloud-native architecture supports high availability and scalability, enabling organizations to adapt to changing demands and maintain operational resilience. With 99.99% platform availability, these solutions highlight how even a 0.20% improvement in uptime can translate to significant savings for businesses that rely on constant availability, preventing costly outages and lost revenue. By reducing vulnerabilities, enhancing threat response, and providing consistent security across environments, these solutions minimize the likelihood and effect of disruptions, helping organizations maintain continuity and focus on strategic goals.

> **"We experience 99.99% platform availability with these solutions, which is important for keeping everything running smoothly and avoiding disruptions."**

Improved Operational Efficiency

Managing operational efficiency in hybrid and multi-cloud environments is challenging, as fragmented tools and processes often lead to inefficiencies and gaps in coverage. With constantly changing user identities, devices, and applications, IT, security, and network teams must coordinate seamlessly to manage access, monitor activity, and respond to threats. Relying on disparate systems and manual workflows slows responses and increases the risk of errors. Utilizing Okta for identity management and security and Palo Alto Networks for security centralizes operations, automates key processes, and maintains consistent visibility, significantly enhancing operational efficiency. Palo Alto Networks' Cloud Identity Engine (CIE) further streamlines these efforts by centralizing user information, enabling consistent enforcement of identity and security policies across the portfolio. With CIE, organizations can unify identity and security strategies, reducing complexity and improving overall effectiveness. Customers reported savings and benefits in the following areas:

> **"With MFA, we've cut the time spent logging in by at least 60%."**

- **Total cost of operations.** Okta and Palo Alto Networks optimize security-related costs by consolidating and streamlining security environments. Fragmented systems often create overlapping tools, redundant processes, and excessive management overhead, driving up operational expenses. Palo Alto Networks increases efficiency with modern architecture designed for remote and hybrid workforces. It delivers an always-on connection for various operating systems and devices, removing the need for users to start a VPN or log into a secure web gateway. Its cloud-based design scales with demand and inspects all traffic for threats 24/7, providing comprehensive protection without added complexity. Integrating Okta's identity management platform with Palo Alto Networks' security solutions centralizes identity and access controls, automates threat

detection and response, and simplifies security operations. Customers shared they were able to retire their legacy identity management solutions and several security tools. Additionally, the transition to the cloud enabled them to eliminate redundant servers, reduce licensing and infrastructure costs, minimize administrative effort, and deliver strong protection while lowering the total cost of operations.

- **Improved user experience.** Okta and Palo Alto Networks improve user experience by reducing security-related interruptions and simplifying secure access across devices and environments. Users can log in from anywhere through a straightforward identity management process, whether accessing SaaS applications, the internet, or public, hybrid, and private clouds. The login process, devoid of passwords and with reduced MFA prompts, significantly improves the user experience, leading to heightened productivity. Risk-based authentication detects known devices, enabling seamless user authentication in the background through Okta without additional prompts. Passwordless authentication across enterprise applications further reduces the administrative burden of managing passwords and resolving account lockouts, streamlining access and improving operational efficiency.

Monthly help desk ticket volume for supporting passwords reduced by 48%.

- **Platform efficiency.** Customers can achieve greater platform efficiency by integrating Palo Alto Networks and Okta, simplifying IT management, reducing operational complexity, and centralizing control. This integration enables organizations to protect critical assets, adapt to evolving demands, and maintain resilience in an ever-changing threat landscape. Customers set and manage MFA policies across their networks without taking critical resources offline or disrupting users. IT teams enforce MFA for specific users and applications without modifying existing applications, meeting security requirements while avoiding added complexity. This streamlined approach minimizes downtime, reduces administrative effort, and strengthens both security and operational continuity.

Faster Time to Value

Complex deployments, fragmented systems, and time-intensive manual configurations often impede achieving faster value in hybrid and multi-cloud environments. Traditional approaches delay the implementation of critical security and identity solutions, leaving organizations vulnerable and slowing productivity. Leveraging Okta for identity management and Palo Alto Networks for security accelerates time to value by providing pre-integrated, cloud-native platforms that are easy to deploy, scale, and adapt. Streamlining setup, automating processes, and enabling immediate protection and access enables organizations to realize security and operational benefits more quickly and prepare them for future demands, ensuring their systems remain resilient and scalable in an evolving landscape. Customers reported savings and benefits in the following areas:

"We needed a solution that not only met our needs at the time but also gave us the flexibility to grow and adapt for the future."

- **Faster time to remediate.** Customers achieved faster threat remediation through the combination of Palo Alto Networks and Okta's identity-based security and advanced detection and response capabilities. The combined solutions provided security teams with greater visibility into authentication data, enabling them to identify unusual user activity, such as credential abuse, and prioritize threats like targeted attacks, insider abuse, and risky behavior. Customers also reported more efficient investigations through AI-driven analytics for root cause analysis, enabling them to respond to threats more effectively. By focusing security efforts on user identity and behavior, organizations saw an improved ability to provide safe, reliable access while quickly detecting and eliminating threats, significantly reducing the time to remediate and strengthening overall security posture.

- **Faster time to insights.** With full visibility into user activity, authentication events, and network traffic, customers were able to gain faster and more accurate insights into security risks. By consolidating identity and security data into a unified view, security teams could quickly identify unusual patterns, such as failed login attempts, unauthorized access, or anomalous network behavior. This enhanced visibility lets teams surface critical insights in real time, prioritize investigations, and effectively address high-impact threats. With centralized data and seamless integration, organizations shorten the time needed to analyze and respond to security events, strengthening their ability to protect assets and maintain operations.

> **"Before, we struggled with limited visibility into our systems. Now, we have full visibility, which helps us to respond to any event more effectively."**

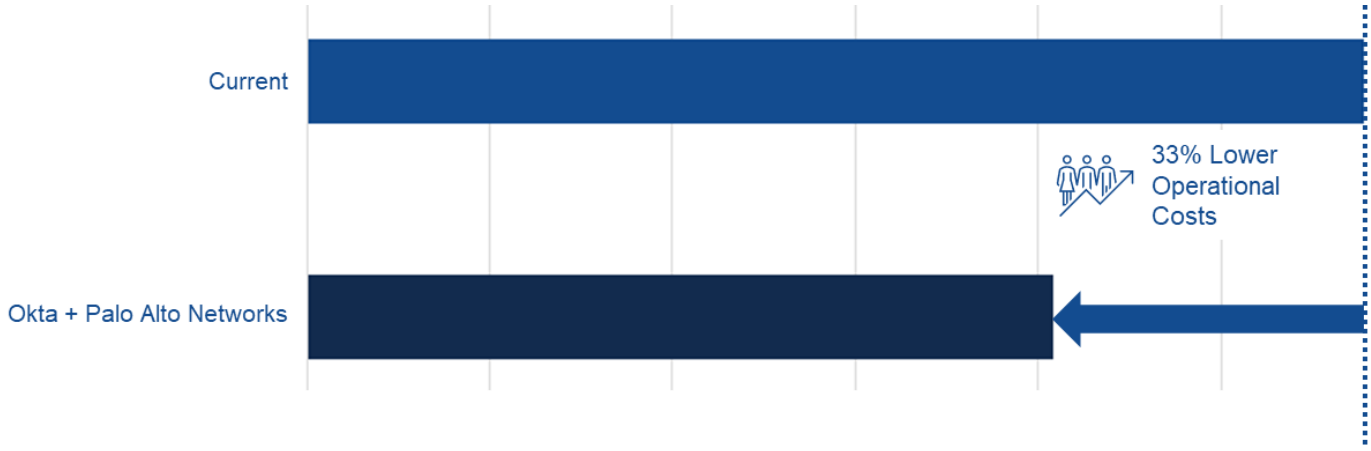
- **Faster time to operationalize.** Okta and Palo Alto Networks centralize identity and security management, helping IT teams address the challenges of managing exponentially growing application usage without additional staff. The integration provides an intuitive interface that offers comprehensive visibility into user activity, applications, and network security policies. IT teams use actionable insights to ensure their security implementations align with current policies, standards, and best practices. This solution simplifies workflows, improves coordination across tools, and accelerates the deployment of security policies and applications. Customers reported that their teams achieved a level of integration, visibility, and efficiency that would have been difficult with existing resources, enabling them to operationalize faster and adapt to evolving demands.

Enterprise Strategy Group Analysis

Enterprise Strategy Group leveraged the information collected through vendor-provided material, public and industry knowledge of economics and technologies, and the results of customer interviews to review, audit, and contribute to the ROI model that compares the current and future costs and benefits of implementing Okta and Palo Alto Networks as a zero trust strategy. Our interviews with customers who have recently transitioned to Okta and Palo Alto Networks, combined with experience and expertise in economic modeling, helped form the basis for our modeled scenario.

Enterprise Strategy Group developed a comprehensive model to evaluate the cost and efficiency benefits of implementing a zero trust solution with Okta's identity and access management (IAM) and security capabilities with Palo Alto Networks' security portfolio, compared with managing multiple disparate point security products. Focusing on a midsize public sector organization, the analysis revealed that this integrated solution could reduce operational costs by 33% while significantly improving efficiency. These savings are driven by several key factors, including the consolidation of security tools and the automation of IAM workflows, which reduce the need for IT personnel to manage redundant infrastructure and fragmented systems. Streamlined access protocols also lower the frequency of password reset requests and troubleshooting tickets, freeing up valuable time for helpdesk teams. Additionally, integration significantly decreases employees' time logging into multiple systems and switching between platforms, enabling them to focus on their core responsibilities. The synergy between Okta and Palo Alto Networks further accelerates the deployment of a zero trust architecture, enabling organizations to achieve security and efficiency benefits more rapidly. By reducing labor-intensive processes and enhancing system scalability, this solution enables organizations to achieve greater operational savings while delivering a superior user experience (see Figure 3).

Figure 3. Operational Savings



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The Enterprise Strategy Group modeled scenario leverages proprietary methods to estimate a conservative return on investment (ROI) in cases where direct risk-reduction metrics were unavailable from customers. This analysis highlights the financial and operational advantages of deploying a zero trust solution with Okta and Palo Alto Networks, compared to the inefficiencies of managing fragmented point solutions.

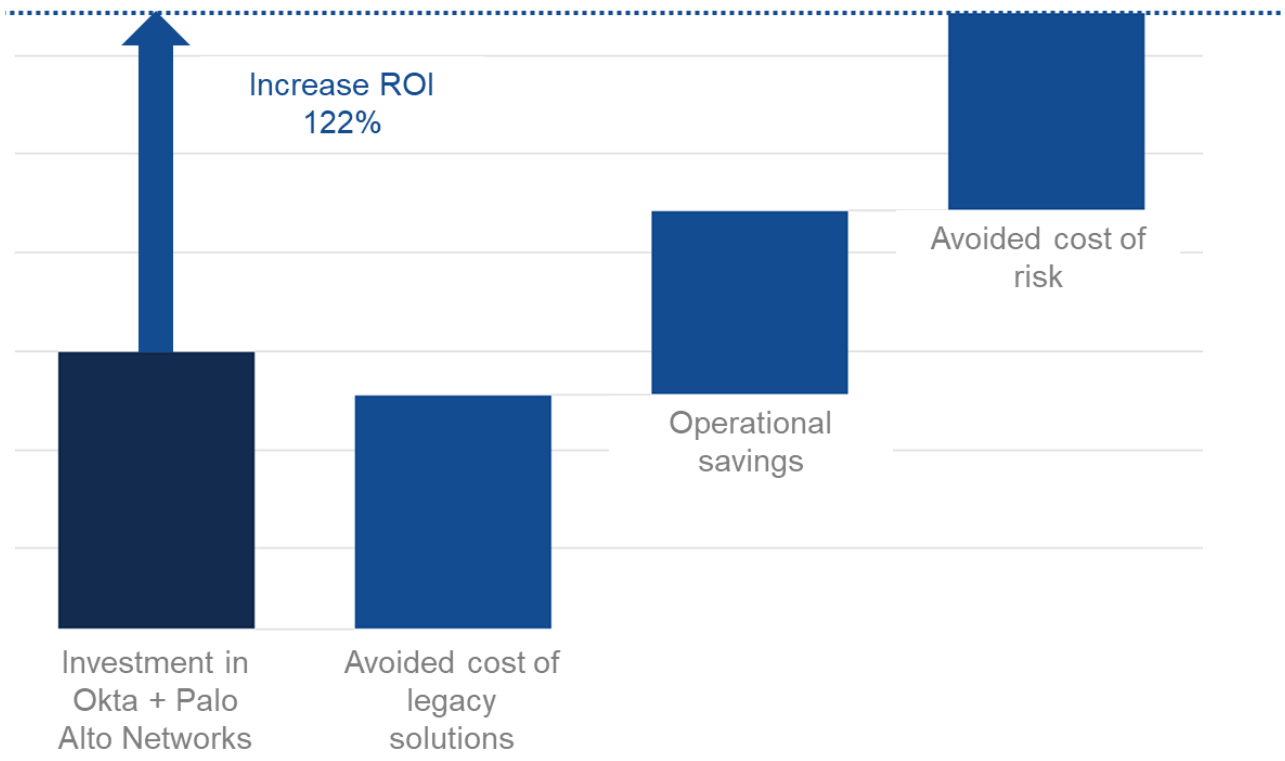
The model incorporates the estimated cost of implementing zero trust with Okta and Palo Alto Networks, which is considered the investment for this analysis. To account for the avoided cost of legacy solutions, the analysis identifies savings from reducing reliance on firewalls, minimizing the need for multiple security and identity tools and capitalizing on the efficiencies of the zero trust architecture. Operational savings calculations used information from customer interviews, which show reductions in administrative overhead, improved resource utilization, and streamlined administrative tasks that collectively boost operational efficiency.

The analysis uses Enterprise Strategy Group research[4] to calculate the avoided cost of risk. The findings indicate that organizations adopting zero trust reduce security costs by $675,000 annually, experience 32% fewer cybersecurity incidents, see a 34% decrease in data breaches, and shorten their MTTR by 10 days. These improvements stem from aggregating identity and security data, streamlining threat detection and response, and enforcing consistent security policies across hybrid environments.

Figure 4 illustrates the conservative yet comprehensive financial and operational benefits of this approach, including reduced costs, enhanced productivity, and mitigated risk over time. When considering all these factors, Enterprise Strategy Group calculated an expected ROI of 122%.

[4] Source: Enterprise Strategy Group Research Report, *Trends in Zero Trust Strategies and Practices Remain Fragmented, but Many are Seeing Success*, March 2024.

Figure 4. Return on Investment



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Issues to Consider

While Enterprise Strategy Group's models are built in good faith upon conservative, credible, and validated assumptions, no single modeled scenario will ever represent every potential environment. The costs and benefits received from Okta + Palo Alto Networks zero trust solutions will depend on the details of your requirements and practice. Enterprise Strategy Group recommends conducting your own analysis of available products and consulting your solution representative to review and compare the solutions evaluated during your proof-of-concept testing.

Conclusion

With resources becoming increasingly distributed and dynamic, static, perimeter-based approaches to cybersecurity are no longer sufficient. Zero trust has emerged as a critical strategy, offering an inside-out approach that prioritizes securing the systems, databases, applications, and other digital assets attackers target most. By shifting from traditional security models to continuous risk assessment and dynamic policy enforcement, zero trust ensures organizations can address modern threats effectively.

Rooted in the "never trust, always verify" philosophy, zero trust represents a significant shift from theoretical concepts to practical implementation as organizations prioritize identity and security initiatives. This approach strengthens security while streamlining operations by addressing inefficiencies in fragmented, perimeter-focused tools and by emphasizing adaptability.

Our validation with Okta and Palo Alto Networks customers revealed that implementing a zero trust strategy, compared with multiple point solutions, significantly reduced business risk, enhanced operational efficiency, and

delivered faster time to value. By providing an end-to-end platform, Okta and Palo Alto Networks enable organizations to adopt zero trust while optimizing the total cost of ownership and delivering exceptional user experiences.

The collaboration between Okta and Palo Alto Networks continues to evolve, ensuring the platform remains future-ready. Innovations like Palo Alto Networks' Prisma Access browser, which integrates seamlessly with Okta, further expand the capabilities of zero trust by enabling secure, identity-driven access to web applications and resources. These forward-looking advancements highlight how the partnership addresses today's security needs and anticipates future challenges, providing a scalable, unified solution that protects organizations while maintaining a frictionless user experience.

Adopting a zero trust strategy, supported by solutions like Okta's IAM and security tools with Palo Alto Networks' security platform, enables organizations to protect critical systems, adapt proactively to evolving risks, and maintain operational resilience in today's complex digital landscape. As such, Enterprise Strategy Group encourages you to evaluate how Okta and Palo Alto Networks can align with your organization's zero trust needs.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com