FORRESTER®

Bolster Your Company Defenses With Zero Trust Edge

Get started ⟶

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY IBOSS | SEPTEMBER 2022

Overview

A company can never have too much protection, and network security can never be fully optimized. Firms that have laid a robust framework surrounding access and security monitoring gain a competitive edge; they mitigate costly security threats and breaches and garner more business agility and trust from customers and employees alike. Zero Trust Edge (ZTE) is a solution that delivers cloud-based network security management (e.g., security service edge [SSE]) and uses Zero Trust access principles, which includes monitoring and inspection of all activity and explicit policies granting access to resources.[1]

In May 2022, iboss commissioned Forrester Consulting to understand how US and UK leaders understand and approach Zero Trust and ZTE.

Key Findings

Most network security leaders recognize that Zero Trust is critical to their organization's success, but 63% say their firm struggles to operationalize Zero Trust into its existing architecture.

There is market confusion on how to best adopt Zero Trust given the solutions available, but security professionals are receptive to consumption as a service and managed services.

Respondents link Zero Trust Edge adoption to organizationwide benefits, including accelerated digital transformation and better, more cost-effective security.

Dialing Into Zero Trust Is An Exercise In Proactive Prevention

During the next 12 months, security professionals will place heavy emphasis on protecting their organizations against outsider and insider threats and establishing cloud security strategies. Yet, this stance shows that leaders are responding reactively, rather than acting proactively.

Instead, security leaders should be implementing or improving on their organizations' Zero Trust strategies. In this way, security decision-makers will strengthen their organizations by preemptively and simultaneously addressing top strategic security objectives.

"Which of the following are your organization's top strategic priorities over the next 12 months?"

84%	Protecting the network against outsider threats
75%	Establishing security strategies for cloud
74%	Protecting the network from insider threats
71%	Improving security operations strategy
66%	Implementing a Zero Trust security strategy
63%	Ensuring our compliance with business partners' security requirements
61%	Establishing security strategies for supporting a distributed workforce (i.e., more employees working remote)
59%	Ensuring our compliance with government security requirements

Base: 155 US and UK network security strategy decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of iboss, May 2022

Security Professionals Recognize The Need For ZTE

Network and security leaders recognize the potential that ZTE can offer to their business. Most respondents agree that establishing Zero Trust is critical to organizational success, and two-thirds agree their company needs to update its architecture with a single edge to secure information while keeping users connected.

Specifically, respondents' organizations are motivated to adopt Zero Trust to improve customer experience (CX) while simultaneously decreasing the number of security incidents and data breaches. More than 50% are also motivated by company and external changes including cloud initiatives, growing hybrid workforces, and government mandates.

"Which of the following are motivating your organization's Zero Trust initiatives?"

66%	Improving customer experience (CX)
63%	Increasing number of security/ransomware incidents
60%	Increasing number of data breaches
55%	Cloud migrations
54%	Expanding hybrid workforce
50%	Increasing organizational emphasis on compliance initiatives
50%	Government mandates/guidelines

Base: 155 US and UK network security strategy decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of iboss, May 2022

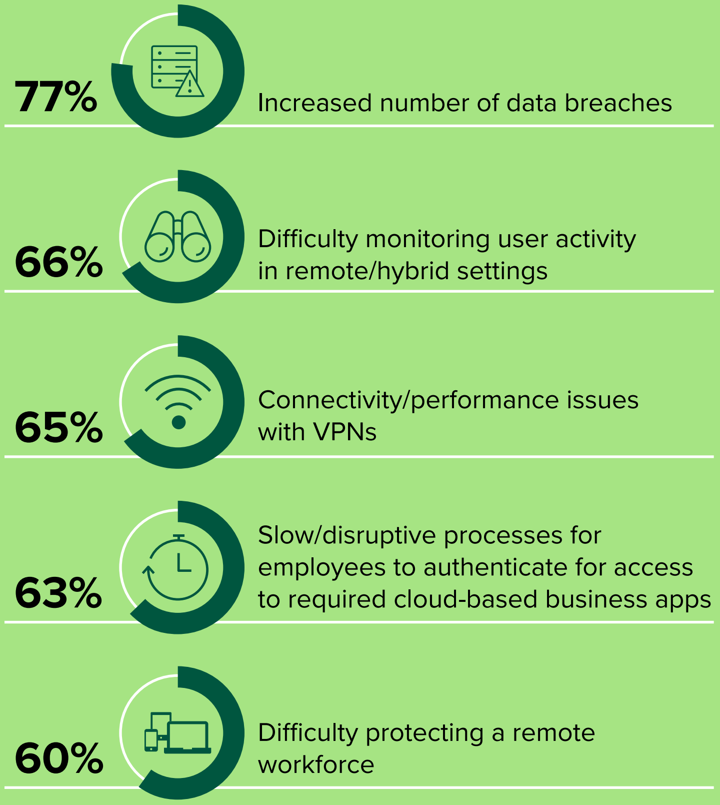
Overview
Situation
Challenges
Opportunity
Conclusion

Security Leaders Are Pulled In All Directions

Security professionals have much to contend with as network threats, technology, and work environments continue to evolve. With so many constantly shifting priorities, these leaders often must resort to triage on their organizations' most dire and immediate challenges while new problems are constantly just around the corner.

For example, more than 60% of surveyed network security strategy decision-makers said their organization struggles with VPN connectivity and with monitoring, protecting, and efficiently authenticating their workforce. Yet, the most significant challenge for nearly 80% of respondents' organizations is combating an increased number of data breaches. Zero Trust via a single service edge can help solve monitoring, access, and security.

"How significant are the following challenges for your organization?"



Base: 155 US and UK network security strategy decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of iboss, May 2022

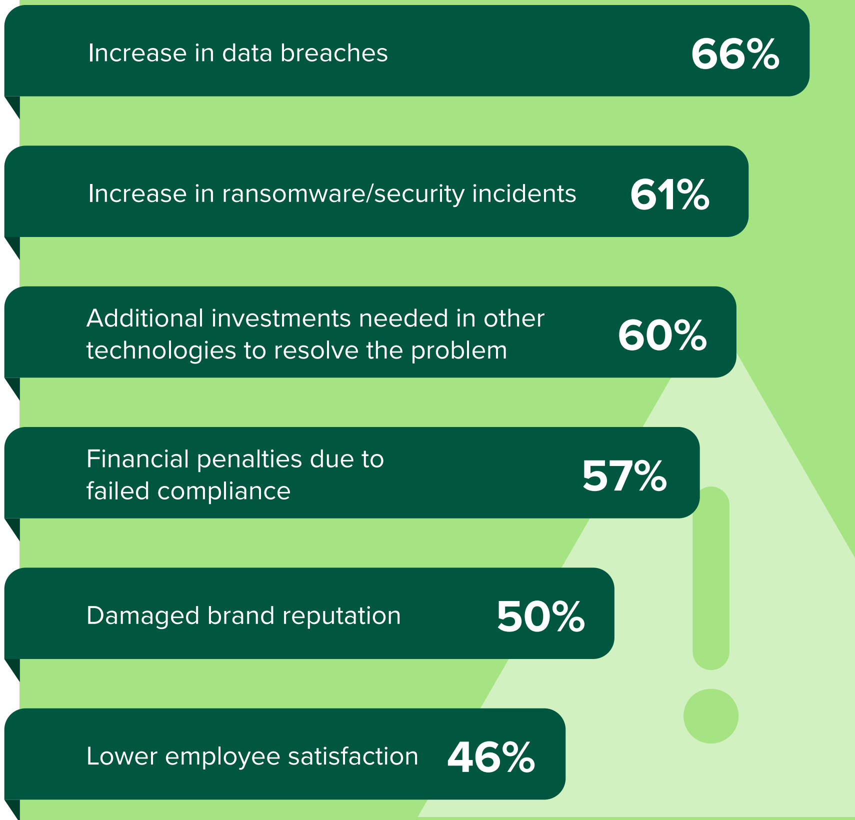
Overview
Situation
Challenges
Opportunity
Conclusion

Firms Will Bleed Money Without Zero Trust

All surveyed respondents recognize there are ramifications for not adopting Zero Trust principles. Data breaches and ransomware/security incidents are top of mind as the most salient ramifications, and they are persistent challenges that firms currently face. With all those security incidents, severe financial repercussions are not far behind. Organizations will need additional technological investments to mitigate security threats and incidents, pay financial penalties when they fail compliance, and face financial losses and damaged reputations as security incidents occur. An insufficiently protected ecosystem will at best undercut company growth and hurt the bottom line; at worst, it can ruin the business.

Furthermore, if access remains cumbersome and activity monitoring is not relayed to teams properly, firms will struggle to maintain employee satisfaction, morale, and ultimately, retention. Firms need to adopt Zero Trust to protect the business.

“What would be the ramifications of not adopting Zero Trust principles?”



Base: 155 US and UK network security strategy decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of iboss, May 2022

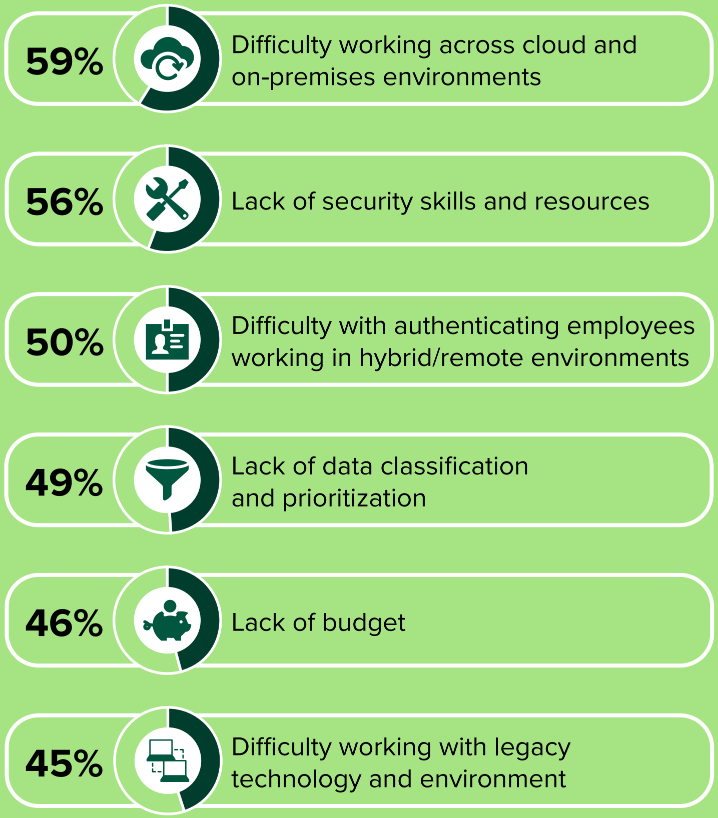
Overview
Situation
Challenges
Opportunity
Conclusion

Firms Are Struggling To Implement Zero Trust

Security leaders are motivated to adopt Zero Trust, but they don't know where to start. Nearly two-thirds of respondents agree their organization struggles to even understand how to operationalize Zero Trust into its existing architecture.

Additionally, all respondents' organizations have experienced at least one roadblock while implementing Zero Trust. Top challenges are related to lack of talent. Decision-makers are struggling with different cloud and hybrid work environments and lack security skills and resources. Piled on top of this knowledge gap, firms need policy governance and technical and organizational support to implement Zero Trust. Cybersecurity is tough; consistent cybersecurity, like Zero Trust, across multiple environments is doubly so. Security leaders need help with its implementation.

"Which of the following challenges have impacted your company's ability to implement Zero Trust?"



59% Difficulty working across cloud and on-premises environments

56% Lack of security skills and resources

50% Difficulty with authenticating employees working in hybrid/remote environments

49% Lack of data classification and prioritization

46% Lack of budget

45% Difficulty working with legacy technology and environment

Base: 155 US and UK network security strategy decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of iboss, May 2022

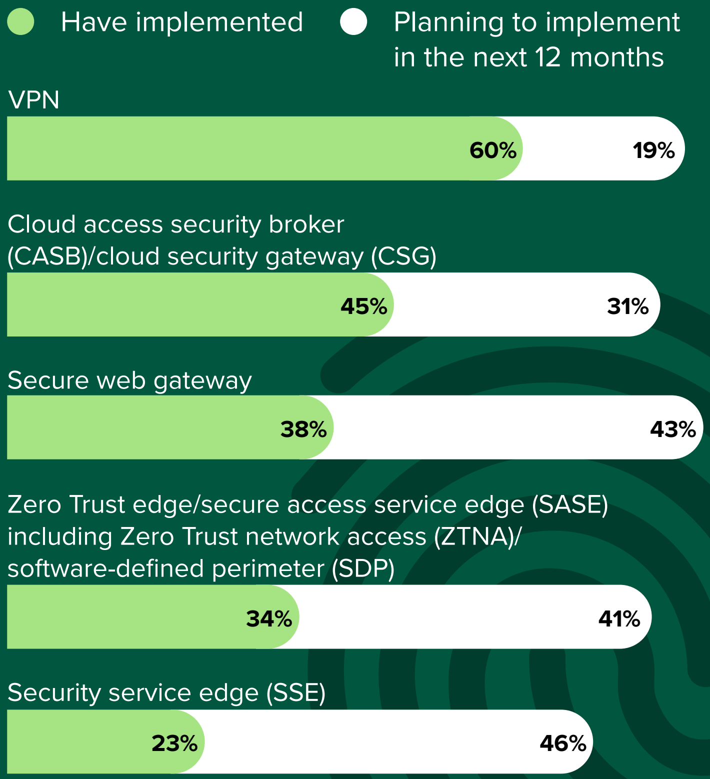
Overview
Situation
Challenges
Opportunity
Conclusion

Firms Will Adopt Zero Trust Edge And Integrated Solution Suites Moving Forward

Firms are all over the map on network security solution adoption. There is confusion on what to do, what to use, how to best adopt Zero Trust given the solutions available, and whether firms should even be using security service edge. Sixty percent of survey respondents' organizations have implemented VPNs as their network security technology, and 61% prefer to select best-of-breed solutions to support network security.

Decision-makers need education on understanding Zero Trust offerings and identifying if their organization's security solution is sufficient. As workforces became more remote in the past few years, a forward-thinking minority started moving away from VPNs toward Zero Trust.[2] According to our study, increasingly more organizations plan on implementing ZTE instead of VPNs in the next 12 months, which also means they will need to switch to integrated solution suites from here on out.

"What are your company's plans when it comes to the following network security and security operations technologies?"



Base: 155 US and UK network security strategy decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of iboss, May 2022

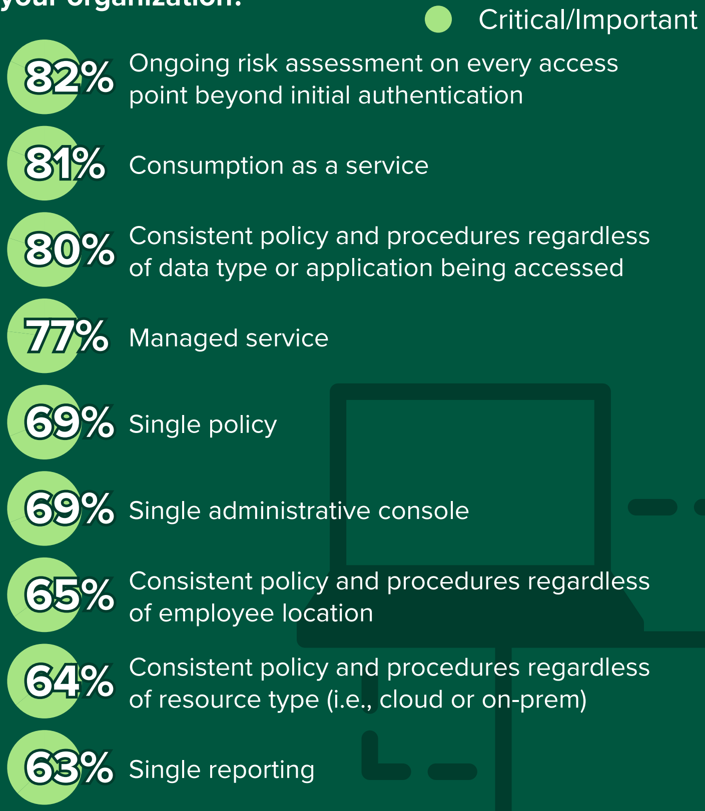
Overview
Situation
Challenges
Opportunity
Conclusion

Security Leaders Want Help Implementing Zero Trust

Despite the market confusion, decision-makers know what capabilities they want to help their organizations adopt Zero Trust. They need help understanding the gaps in their defenses and with laying a more robust foundation to their security. More than 80% want ongoing risk assessments and consistent policies and procedures.

Firms need a trusted partner that knows Zero Trust, and that can deliver this from the cloud. Security leaders are open to capabilities delivered through a consumption-as-a-service model and by a managed service, which a trusted partner can provide. Furthermore, a partner can provide offerings that security leaders might not know to ask for while implementing Zero Trust. Implementing Zero Trust is no easy task that will require organizations to transform their businesses in phases.[3] Security professionals know to ask for help, and they require guidance quickly!

“When implementing a Zero Trust architecture, how important are the following capabilities to your organization?”



Base: 155 US and UK network security strategy decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of iboss, May 2022

Overview
Situation
Challenges
Opportunity
Conclusion

Zero Trust Edge Is Good For Business

Adopting Zero Trust is the way of the future, but elevating your organization's Zero Trust strategy with cloud-based network security (e.g., single security service edge) gives firms a competitive edge. Firms will contain breaches more quickly, allow employees more freedom and flexibility to get their jobs done, improve trust with customers and partners, and enable more business initiatives.[4] Security leaders can set themselves apart by being business leaders, too.[5] Nearly 70% of respondents said the number one advantage of ZTE is that digital transformation initiatives will accelerate. It is the biggest benefit, surpassing expected benefits such as improved security and lower security expenditures. Firms can grow their businesses faster with accelerated digital transformation, expand their ecosystems, and elevate customer and employee experiences and satisfaction.

"What advantages do you see in implementing a single security service edge to support the Zero Trust architecture strategy?"

68%
Accelerated digital transformation initiatives

61%
Improved breach detection and vulnerability management

54%
Lower capital and operational expenditures on security

50%
Mitigated vulnerability

50%
Better organizational accountability and coordination

50%
Improved network visibility

Base: 155 US and UK network security strategy decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of iboss, May 2022

Conclusion

As technology ecosystems evolve, network security decision-makers must juggle risks including third-party partners, multiple clouds, hybrid workforces, and internal and external threats. Specific and consistent access policies and monitoring can preemptively mitigate data breaches, ransomware, and security incidents that are plaguing firms. Cloud-based delivery security management can fortify that protection further. Firms can use ZTE not only to help alleviate the growing pains they face as businesses become more digital and adopt more hybrid work environments, but they can also use those points of change to strengthen their companies and bolster the trust of employees, partners, and customers. Firms are struggling with the complicated aspects of implementing Zero Trust, yet they must adapt. Those organizations that lag behind will suffer without it.

Project Director:

Sandy Liang,
Market Impact Consultant

Contributing Research:

Forrester’s security and risk research group

Overview
Situation
Challenges
Opportunity
Conclusion

Methodology

This Opportunity Snapshot was commissioned by iboss. To create this profile, Forrester Consulting surveyed 155 US and UK network security strategy decision-makers who are developing, in the process of implementing, or are improving their organization's Zero Trust strategy. The custom survey began and was completed in May 2022.

ENDNOTES

[1] Source: "Introducing The Zero Trust Edge Model For Security And Network Services," Forrester Research, Inc., August 2, 2021.

[2] Ibid.

[3] Source: "A Practical Guide To A Zero Trust Implementation," Forrester Research, Inc., August 2, 2021.

[4] Source: "The Definition Of Modern Zero Trust," Forrester Research, Inc., January 24, 2022.

[5] Ibid.

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and ensures lasting impact. For more information, visit forrester.com/consulting.

Demographics

COUNTRY	
United States	66%
United Kingdom	34%

INDUSTRIES	
Government	32%
Retail	19%
Financial services and/or insurance	18%
Healthcare	16%
Telecommunications services	15%

NUMBER OF EMPLOYEES	
1,000 to 4,999	58%
5,000 to 19,999	34%
20,000 or more	8%

TITLE	
C-level	8%
Vice president	43%
Director	50%

Note: Percentages may not total 100 because of rounding.

FORRESTER®