

Benchmark Insights

—

IBM Institute for
Business Value

Getting started with zero trust security

A guide for building
cyber resilience

IBM®

How IBM can help

IBM Security is putting zero trust into action with a modern, open approach to security that aligns with your business priorities. For more information, please visit: ibm.com/security/zero-trust

To better understand how organizations are implementing zero trust security, the IBM Institute for Business Value (IBV) partnered with Oxford Economics to survey more than 1000 operations and security executives from organizations in 15 industries across the globe (see “Research methodology” on page 16).

By Chris McCurdy,
Shue-Jane Thompson,
Lisa Fisher,
and Gerald Parham

Key takeaways

New business models are accelerating security transformation.

As risks evolve and new threats emerge, traditional security models that rely on defined perimeters and implicit trust are becoming obsolete. Organizations transcending traditional functional and organizational boundaries require a security model that is more holistic, multilayered, and event-driven.

Zero trust security offers clear operational benefits.

“Zero trust” is a dynamic approach to security wherein requests are validated using a combination of access controls, identity management, and contextual data. Organizations with the most mature zero trust capabilities—“zero trust pacesetters”—have reduced expenditures, increased their cybersecurity effectiveness, and enjoy higher cyber resource retention rates.

Zero trust leaders excel in 4 core competencies.

Zero trust security enhances cyber resilience by transforming trust into an operational variable. Proficiency in 4 core competencies and associated practices drive zero trust success.

The price of progress

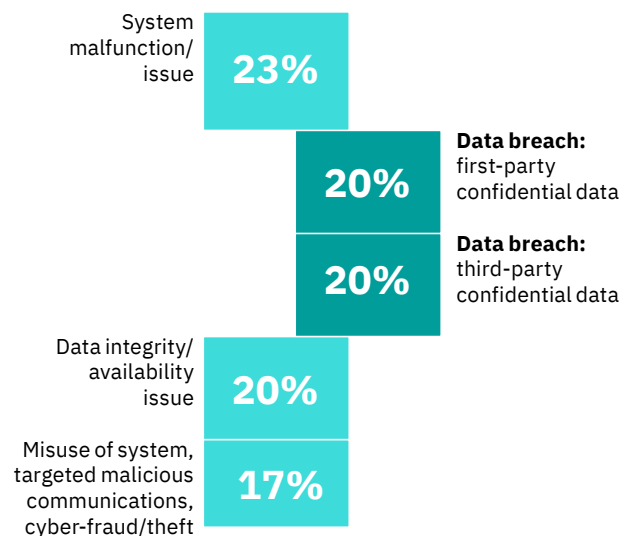
Organizations have responded to the COVID-19 pandemic by accelerating digital business transformation, expanding cloud footprints, increasing their remote workforces, and integrating their supply chains. As a result, our research indicates the percentage of remote workers serviced by the security function increased by 41% between the end of 2019 and through 2020.

But moving communication, business, and personal interactions online has also significantly increased potential attack surfaces, resulting in a dramatic surge in cybersecurity incidents and exposed records (see Figure 1).¹ As workloads move to the cloud, threats move with them. Our research indicates that in 2020, upwards of 90% of cyber-related incidents originated in cloud environments.

Figure 1

Data exposed

Expanded online interactions make data breaches more common



Q. Of the total cybersecurity incidents detected by your organization, what was the distribution by type?



70%

of organizations are unable to secure data that moves across multiple cloud and on-premises environments, a profound deterrent to value realization.



92%

of organizations lack the ability to securely enable and extend new cloud-native capabilities to their internal and external partners.



150 days—

the time it takes to fill cyber talent vacancies with qualified candidates, leading to gaps in awareness and accountability that can elevate risk exposure.

While cloud-based shared services and collaborative work environments are vital to delivering business outcomes, these environments require a new approach to security operations—one that is more flexible, responsive, and cooperative. Seeking to capitalize on the merits of this new approach, leaders are modernizing their IT and OT operations based on the principles of zero trust (see “Perspective: What makes zero trust security different?”).

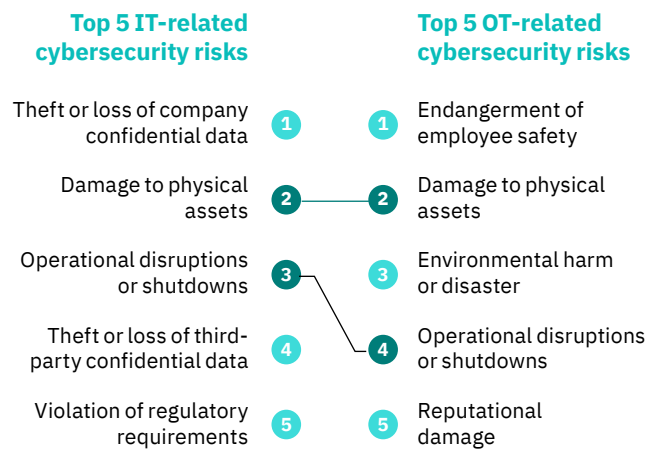
Valuable yet vulnerable: Securing critical infrastructure

The very nature of critical infrastructure implies a dynamic relationship between trust and risk. As operations move online, both IT and operational technology (OT) networks are subject to compromise. The July 2021 Kaseya ransomware attack, for example, affected up to 2,000 organizations and carried ransom demands in excess of \$70 million. Our reliance on IT and OT environments means mission-critical infrastructure is increasingly vulnerable to new threats (see Figure 2).²

Figure 2

Interconnected risk

IT and OT risks are complex and interdependent



Q. How would you rate the above cybersecurity risks? Figure shows responses of high and very high.

Traditional cybersecurity approaches rely on permissions and discrete network boundaries, but today's networks are defined by dynamic services and diffuse boundaries.

Trust is the basis for collaboration and partnership. As these capabilities become essential to delivering value, how we think about trust is rapidly changing. While traditional approaches to cybersecurity relied on permissions and discrete network boundaries, today's networks are defined by dynamic services and diffuse boundaries. Today's digital platforms generate value by virtue of being interconnected and sharing information across multiple parties.

Tensions may be inevitable. Many OT systems have traditionally relied on system isolation, yet the demand for insights from connected devices and smart systems makes such practices difficult to sustain. If anything, a lack of connectivity can render existing vulnerabilities more difficult to remediate.

Making matters worse, risks can cascade: a failure in one system often results in the failure of others. Threat actors are becoming more sophisticated in their ability to capitalize on shortcomings in IT and OT security controls (see "Perspective: The convergence of IT and OT systems elevates risk exposure").³ While the potential impacts are significant, such risks can be difficult to anticipate.

Cybercrime-as-a-service is an unsettling new trend.⁴ These services—sold through hacker forums, direct web sales, and on the dark web using cryptocurrency—rely upon sophisticated, often coordinated cybercrime exploits, such as botnets, distributed denial of service attacks (DDoS), credit card fraud, malware, spam, and phishing attacks.

In fact, in the wake of the Colonial pipeline cyberattack, US President Joseph Biden issued an executive order to improve the cybersecurity posture of critical industries and infrastructure. Included is a directive that federal agencies draft plans for implementing zero trust architectures within 60 days of the order.⁶

Perspective: What makes zero trust security different?

In principle, zero trust is a preventive approach to security that presumes malicious actors have already penetrated the organization's network defenses. IT and cybersecurity operations are recognized as functionally interdependent. As a result, the organization's ability to sense, evaluate, and respond to events is much more dynamic, often occurring in near real time. This holistic awareness that spans IT and cyber operations makes zero trust capabilities truly transformative.

In practice, zero trust bridges operational and cybersecurity domains by requiring authentication and verification for every exchange of value. Since a zero trust operating model doesn't rely on secure perimeters, it's well-suited to shared ecosystems where organizational boundaries are diffuse and value is exchanged in the form of services. By making trust an operational and transactional variable, third parties can support even the most sensitive workloads and mission-critical capabilities.

Perspective: The convergence of IT and OT systems elevates risk exposure

Executives' primary IT-related concerns are the exposure of sensitive data, the long-term implications of successful breaches, and regulatory compliance. Their primary OT-related concerns are the safety of individuals, physical assets, and the environment, as well as any resulting impact on the organization's operations and reputation.

While the cybersecurity risks related to IT and OT environments are not always the same, they often reinforce each other. As the Colonial Pipeline hack has demonstrated, failure in one area, such as a compromised password from an IT system, can lead to failures in others, such as diminished OT platform availability and reliability.⁵

Seizing the zero trust advantage

Our analysis reveals 23% of organizations—a group we refer to as “zero trust pacesetters”—are ahead of their peers in deploying zero trust capabilities across their IT and OT environments and in their interactions with ecosystem partners.

These organizations have fashioned their IT and security operations as a single estate. They are proficient in partnering internally and externally to manage cybersecurity risk. They have modernized their security operations related to interdependent governance, risk, and compliance frameworks. They apply cloud, AI-driven analytics, and automation extensively. And they recruit, develop, and retain skilled cybersecurity resources to enable zero trust capabilities across their digital estates.

Most importantly, their security operations can adapt to the complexity of the current business environment—whether it’s enabling a remote workforce; monitoring endpoints, applications, data, and network traffic; or analyzing the behaviors of employees, customers, and partners to identify emergent threats.

What sets zero trust pacesetters apart?

Zero trust pacesetters tell us they dedicate a similar percentage of their IT budgets and resources as their peers to cybersecurity, yet they are deriving significantly greater business and security benefits from their approach to security.

In fact, twice as many pacesetters say they have significantly reduced their security capital and operational expenditures, while at the same time increasing the effectiveness of their cybersecurity capabilities. In particular, they have:

- Improved their detection and response capabilities, dramatically reducing the exfiltration of sensitive data. In the event of breaches, their ability to limit malware propagation reduces the impact to the organization.
- Prioritized the ability to establish and maintain secure connections between ecosystem partners, allowing them to better capitalize on their cloud investments.
- Invested more of their cybersecurity budget in upskilling resources. As a result, their cyber resource retention rates are 10% higher than those of other organizations.

The success of zero trust pacesetters offers compelling evidence for the merits of a comprehensive zero trust strategy. These organizations are favorably positioned to achieve greater operational efficiencies and better business outcomes. Other organizations can realize similar benefits by understanding what operational capabilities are essential to zero trust success and then applying them.

Zero trust pacesetters dedicate a similar percentage of their IT budgets to cybersecurity, yet they derive significantly greater benefits.

Getting started: Defining a zero trust roadmap

Zero trust pacesetters are nearly twice as far along in implementing 4 core competencies:

1. A strong foundation for zero trust security operations guided by governance, risk, and compliance controls and reinforced with AI-driven analytics.
2. Security automation and orchestration capabilities that increase the scope, scale, visibility, and efficiency of security operations across hybrid cloud operating environments.

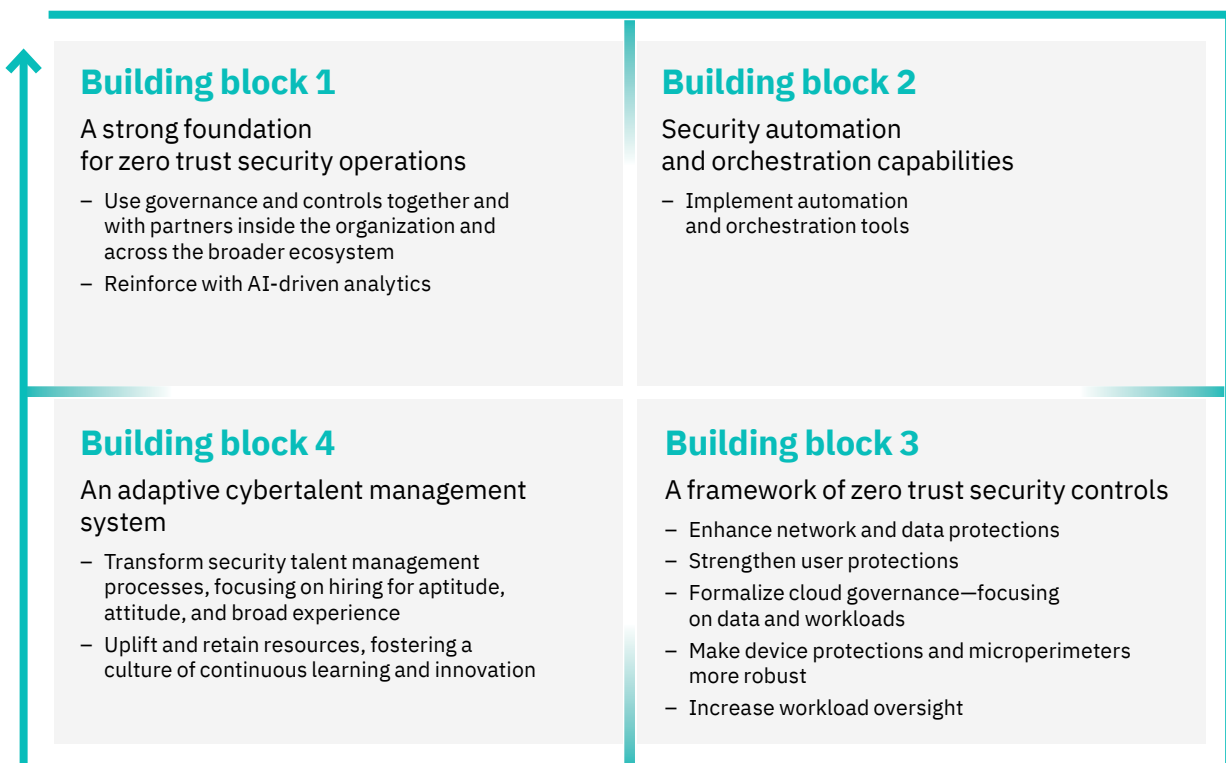
3. A framework of zero trust security controls to monitor, manage, and help defend critical resources—encompassing users, data, networks, devices, and workloads.
4. An adaptive cyber talent management system that prioritizes the combination of talent and technology to achieve better security outcomes.

Each of these building blocks is enacted via a series of mutually reinforcing practices and activities. Of particular importance, our data analysis underscores the extent to which these practices and activities rely upon each other. In other words, all 4 core competencies work in concert to achieve the benefits associated with zero trust (see Figure 3).

Figure 3

Security by design

Zero trust capabilities reinforce each other



Source: IBM Institute for Business Value data analysis.

Heightened risk awareness and malware propagation controls significantly reduce exposure to cyberattacks.

Because each organization’s IT and cyber estates reflect distinct needs, each journey to zero trust will be unique. Factors that will influence an organization’s journey include its business strategy and operating models; the availability of budget and resources; the breadth and depth of partner relationships; existing technology implementations and constraints; and industry and geo-specific regulatory and competitive demands.

Acknowledging the diversity of these factors, our approach prioritizes practicality, flexibility, and the virtue of building upon existing capabilities. Our recommendations, derived from operational performance insights, are based on real-world outcomes across a range of operating environments—spanning young organizations focused on growth to mature organizations focused on transformation.

For each building block, we provide an explanation, the benefits associated with it, and the practices and activities required to realize it.

Building block 1: Establish a strong foundation for zero trust security operations

Zero trust pacesetters have integrated zero trust capabilities into their prevailing security architectures and operations. The capabilities augment—rather than replace—existing technologies, processes, and skills.

These organizations have developed a culture of security awareness based on modern security practices and automated security controls. This culture increases awareness of security risks via policies that define who and what can access common network, application, and data assets.

These policies are supplemented by the technical security solutions that enforce them systematically. Such an environment can help identify devices, applications, services, and behaviors subject to compromise, then use automated controls to help remediate threats and vulnerabilities.

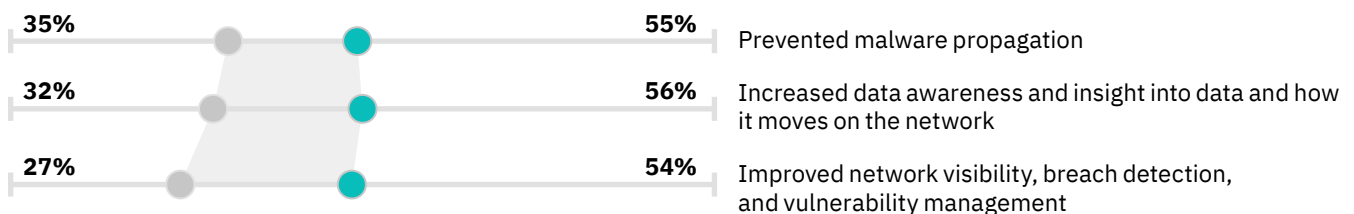
In the event of breaches, a pacesetters’ ability to prevent malware propagation helps to contain risks, limiting the likelihood of follow-on failures (see Figure 4). Together, heightened risk awareness and malware propagation controls significantly reduce exposure to cyberattacks.

—

Figure 4

Seeing and understanding

Better network visibility, better results



All others | Zero trust pacesetters

Q. To what extent has your organization realized each of the above benefits from its approach to security? Percentages reflect respondents selecting a significant or very great extent.

In addition, zero trust pacesetters work with partners to streamline the management and reporting of cyber risk. Guided by governance, risk, and compliance frameworks, they proactively communicate new threats across the enterprise and with strategic partners and third-party suppliers. Their use of standard system development lifecycle (SDLC) and DevSecOps methodologies standardizes critical capabilities for security operations and governance, further facilitating efficiency.

Through extensive application of advanced cybersecurity analytics for incident detection and response, zero trust pacesetters monitor a higher percentage of network communications (55%) and endpoint devices (68%) for vulnerabilities and policy violations, compared to 45% and 60% of peers, respectively. The more an organization sees—network communications traffic and endpoint devices, for example—the greater its ability to identify and remediate potential threats. Greater visibility increases the probability of success.

Most pacesetters indicate they have significantly increased insights into how data moves across their networks. 1.5 times more pacesetters have improved their network visibility, breach detection, and vulnerability management capabilities than their peers (see Figure 4).



Building block 1

Establish a strong foundation for zero trust security operations

Monitor network communications for suspicious activity



45% All others | 55% Zero trust pacesetters

Monitor endpoint devices for vulnerabilities and policy violations



60% All others | 68% Zero trust pacesetters

How to do it



Use IT governance and controls with partners inside the organization and across the broader ecosystem



Use AI-driven analytics to flag exceptions and trigger automated controls

Automated AI security models can recognize abnormal behaviors, assess vulnerabilities, and flag new threats.



In particular, 2 pacesetter practices can help organizations establish a strong foundation for zero trust security operations:

- 1. Use IT governance and controls with partners inside the organization and across the broader ecosystem to increase the visibility and effectiveness of cyber risk mitigation efforts:**
 - Provide security education and awareness training for employees—the knowledge, skills, and abilities needed to defend the organization.
 - Apply governance, risk management, and compliance frameworks and programs to identify, assess, and mitigate cyber risk. Balance acceptable risk levels with business objectives and compliance requirements. Coordinate these efforts with ecosystem partners to achieve better economies of scale.
 - Implement a data loss prevention (DLP) policy. Define how your organization can share and protect data to guide implementation of tools that prevent users from sending sensitive or critical information outside the core network. Coordinate these efforts with partners using shared infrastructure.
 - Integrate security into the software development process. Cloud-native methodologies such as DevSecOps allow organizations to work with partners more efficiently, notably through the adoption of common approaches to security operations and governance.⁷

- 2. Use AI-driven analytics to flag exceptions, trigger remediation controls, and prevent threat actors from using automated scan-and-exploit techniques:**
 - Implement advanced cybersecurity telemetry capabilities, including monitoring and analytics for incident detection and remediation. Reduce reliance on manual threat detection by using AI-driven, automated investigation processes for high-value data, assets, network segments, and cloud services.

Threats can be classified and prioritized to trigger alerts based on attack signatures and indicators of compromise (IOC). To improve operational efficiency, organizations may wish to complement existing telemetry solutions with endpoint detection and response (EDR) and cross-layer detection and response (XDR) capabilities.
 - Apply AI to automate model building, track normal behavior, and flag anomalous activity. Automated AI security models can recognize normal (versus abnormal) behaviors, assess vulnerabilities dynamically, and flag anomalous activity that can indicate new threats. Models can then use these inputs to qualify and quantify potential risk exposure.



Building block 2

Make operations robust with security automation and orchestration capabilities

Significantly reduced security capital and operational costs

Dramatically reduced the scope and cost of compliance initiatives



61%
Zero trust pacesetters



50%
Zero trust pacesetters

How to do it



Establish an ecosystem-wide security operations center (SOC)



Implement a single cloud-agnostic platform with visibility across providers



Apply AI-enabled security intelligence to detect abnormal behavior

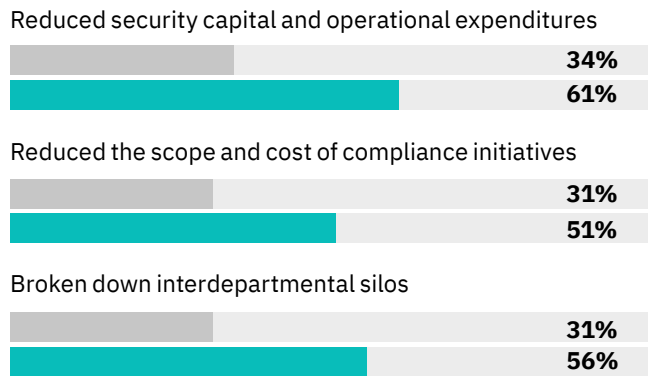
Building block 2: Make operations robust with security automation and orchestration capabilities

Zero trust pacesetters have embraced security automation and orchestration, increasing the scope, scale, and efficiency of their security operations. 61% of zero trust pacesetters indicate this has significantly reduced their security capital and operational costs, while half of them indicate this has dramatically reduced the scope and cost of compliance initiatives (see Figure 5).

Figure 5

The cost advantage

Automation and orchestration increase scope, scale and efficiency



All others | Zero trust pacesetters

Q. To what extent has your organization realized each of the above benefits from its approach to security? Percentages reflect respondents selecting a significant or very great extent.

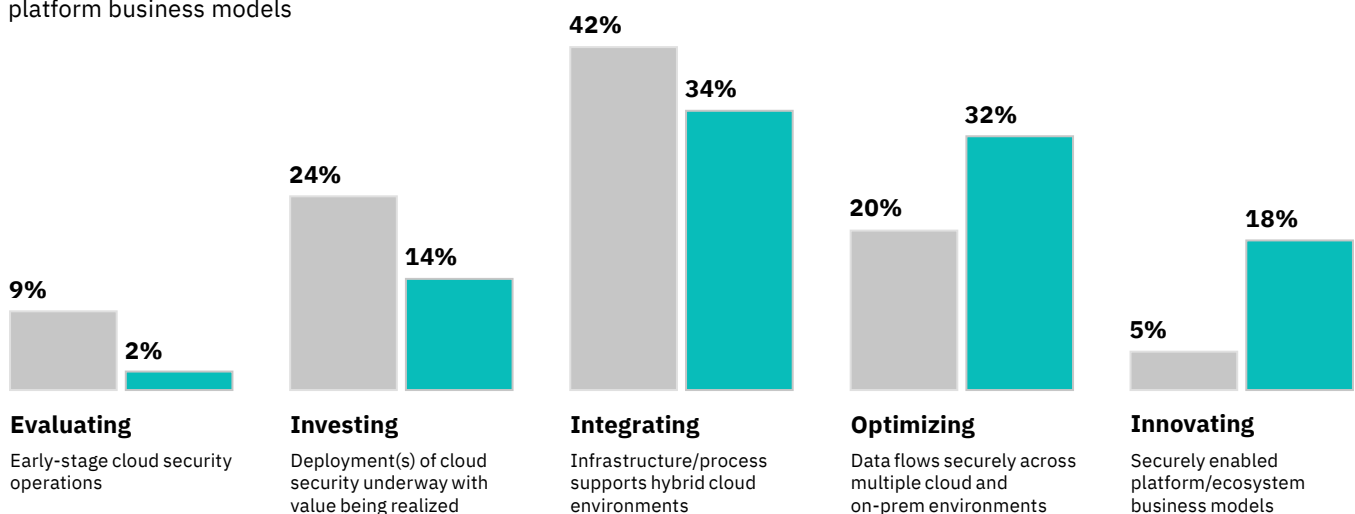
Automation and orchestration solutions like security incident and event management (SIEM); security orchestration, automation, and response (SOAR); and XDR provide a holistic view of threats. By seeing threats in the context of enterprise data, applications, networks, and devices, these solutions enhance security investigations, making it easier for pacesetters to increase the agility of their security operations and improve their incident response capabilities.

In addition, zero trust pacesetters' cloud security capabilities are comprehensive. 1 in 3 can support hybrid cloud environments and are taking full advantage of data flowing securely across and between multiple cloud and on-premises environments. 1 in 5 can take this even further (see Figure 6). They have the capabilities to securely enable and extend new cloud-native business and operational capabilities to internal and external partners.

Figure 6

The cloud advantage

Mature cloud security capabilities enable new platform business models



All others | **Zero trust pacesetters**

Q. Which statement best describes the maturity of your organization's cloud security capabilities? Select one.

60% of pacesetters agree their security approach has significantly enabled digital transformation, 54% that it has increased trust and secure connections to external partners.

But what really sets zero trust pacesetters apart? It's their degree of cyber resilience, and their ability to capitalize on operational efficiencies and economies of scale. They harness the full reach of their cloud environments to enable new capabilities and new business models in conjunction with their ecosystem partners.

One pacesetter practice, in particular, can help organizations achieve greater security resilience and operational efficiencies:

1. Implement automation and orchestration tools to improve the scope, scale, visibility, and efficiency of zero trust security operations:

- Continually assess the organization's security posture using an ecosystem-wide security operations center (SOC) with coordinated incident management and crisis response capabilities.⁸ Prioritize tools that provide visibility across the SOC. Enable real-time visibility across all on-premises and cloud environments, including networks, devices, applications, users, and data. This can help decision makers understand the current state of critical assets and services.
- Deploy security solutions that work across multiple clouds and integrate with solutions from multiple vendors. The SOC team should have a single cloud-agnostic platform with visibility across providers for starting investigations of any cloud-based incident at any place within the ecosystem.
- Implement AI-enabled security intelligence to analyze data streams to detect abnormal behavior. Combine security information from multiple domains, as well as external sources, to enrich the contextual data/metadata of interactions and to enforce security policies. Extend log capture capabilities by applying the same procedures across cloud environments, scanning for irregular configurations that may point to indicators of compromise.

Building block 3: Deploy a framework of zero trust security controls

Zero trust pacesetters are integrating zero trust controls into their existing security operations. Pacesetters use security telemetry, real-time traffic analysis, and automation and orchestration capabilities to enhance security insights.

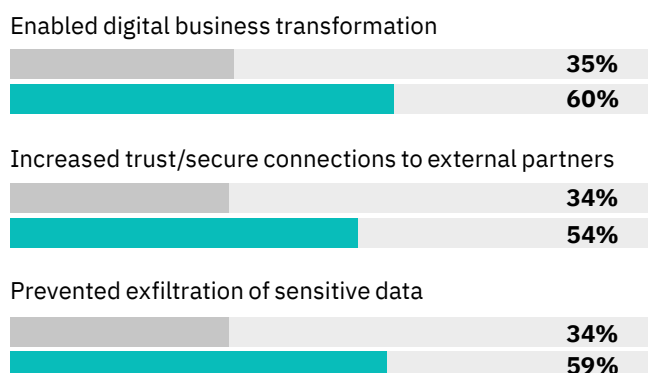
This encompasses critical resources such as users, devices, data, networks, and workloads. Because these resources operate in concert—typically in conjunction with ecosystem partners—pacesetters are better positioned to act on insights. This enhances cyber resilience and their ability to drive new value propositions.

The benefits associated with this are evident. For zero trust pacesetters, 60% agree this approach has significantly enabled their organizations' digital transformations, while 54% agree it has increased trust and secure connections to external partners (see Figure 7).

Figure 7

The power of trust

Zero trust improves resilience and enhances digital transformation efforts



All others | Zero trust pacesetters

Q. To what extent has your organization realized each of the above benefits from its approach to security? Percentages reflect respondents selecting a significant or very great extent.



Building block 3

Deploy a framework of zero trust security controls

Enabled digital business transformation

Increased trust and secure connections to external partners



60%
Zero trust pacesetters



54%
Zero trust pacesetters

How to do it



Enhance network and data protections



Control access to data and manage digital identities



Formalize cloud governance



Extend visibility to every endpoint attempting to access critical resources



Increase oversight for workloads

Transforming trust into a transactional variable enhances the integrity of the operations environment. With greater visibility into mission-critical resources, pacesetters operate more efficiently. By placing security controls closer to critical resources—for example, by creating microperimeters around specific assets and services—they can extend authentication and validation controls without introducing unnecessary friction. Doing so enhances resilience by preventing unauthorized access and the exfiltration of sensitive data (see Figure 7).

When considered as a whole, this change in operations is subtle yet significant. By establishing trust at pre-defined intervals—using validation and authentication controls for specific events and behaviors—the ability to negotiate trust becomes a dynamic, real-time capability. Because trust can be adjusted based on circumstance or context, it can enable new forms of collaboration and new exchanges of value.

The following 5 practices and associated activities are critical to establishing a framework of zero trust controls:

1. Enhance network and data protections, starting with the establishment of a segmentation gateway to enable more granular access controls:

- Use next-generation firewalls (NGFWs) to augment cloud security controls. Define rules and policies for NGFWs, email and cloud security gateways, and DLP solutions to enforce data security and access policies. These should be capable of operating across hosting models, locations, users, and devices.
- Regularly perform sensitive data discovery and classification—on premises, at the endpoint, in transit, and in the cloud. Capture sufficient data and metadata to be able to recreate the full context for any given interaction.

Understand where your most sensitive data resides, who has access to it (and how), who is accessing it (and when), and what they’re doing with it. This can help you meet standards for data privacy and regulatory compliance, as well as monitor and control access to highly sensitive data.

As techniques to bypass authentication emerge—notably the abuse of trust mechanisms—examine identity management as a potential source of vulnerability.

 **2. Strengthen user protections by controlling access to data and managing digital identities:**

- Regularly review user access entitlements. Establish role-based controls for access to data. Operate on the principle of least privilege, with access restricted to the information and resources required to perform a specific task based on a recognized legitimate need.

Brief privileged users on relevant cybersecurity controls and practices. Document who has entitlements to access sensitive resources, then monitor behaviors and conduct audits to improve visibility and flag anomalies and potential malicious actions.


- Implement multifactor authentication (MFA) for critical apps and data assets. Employees should use two-factor authentication (2FA) or MFA to identify areas upon which security staff should focus, as well as to prevent insider attacks.⁹ These should be complemented by a privileged identity management (PIM) solution and strong processes for identity management and governance (IMG).

As techniques to bypass MFA emerge—notably the abuse of trust mechanisms such as OAuth and SAML—place greater emphasis on identity management as a potential source of vulnerability.¹⁰ Enhance policies and controls related to credentials management and secrets management.

 **3. Formalize cloud governance to promote openness and interoperability:**


- Establish a formal cloud governance process. Build your cloud governance model on standardized governance policies and frameworks to help cloud-related security expenditures drive business objectives related to cloud adoption.
- Establish governance and oversight for cloud data and workloads. When migrating to cloud, clearly define how responsibilities are distributed between your organization and your cloud provider(s).

In a shared responsibility model, the provider is typically responsible for securing and managing the infrastructure and the customer for securing the data and workloads operating on it. To mitigate the risk of data loss, as well as noncompliance with regulations, use specialized security services from your cloud provider(s).

 **4. Make device protections and microperimeters more robust by extending visibility to every endpoint attempting to access critical resources:**

- Conduct health checks on endpoints before allowing them to connect to the corporate IT network or access systems. Use automated solutions that scan and inventory new endpoint devices.

Add new endpoints to a registry, along with contextual data detailing associated users, resources, and events. Unauthorized users and unmanaged devices should be identified, profiled, and prevented from gaining access.

 **5. Increase oversight for workloads:**

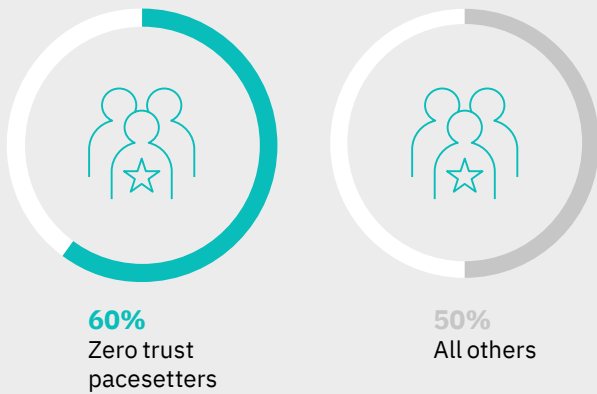
- Inventory and monitor workload configurations. Implement a multicloud security solution that provides centralized oversight of cloud platform instances, workloads, configuration settings, authorized services, and credentials.



Building block 4

Develop an adaptive cyber talent management system

Zero trust pacesetters have cyber talent retention rates 10% higher than their peers



How to do it



Hire for aptitude, attitude, and broad experience



Foster a culture of continuous learning and innovation that values the propensity to learn

Building block 4: Develop an adaptive cyber talent management system

Regardless of how organizations choose to implement their zero trust capabilities, without skilled cyber resources they can face challenges in delivering lasting security and business outcomes.¹¹ But many organizations are struggling to recruit and retain these skills. On average, it takes 150 days to fill a vacancy with a qualified candidate.

In response, zero trust pacesetters are using a more dynamic cyber talent management system that can adapt to changes in skills and demand. Most notably, they hire for latent potential, recognizing it's as important to have people who can learn as it is to have those with specific skills.

Because organizations are competing for the same high-value talent, those with deeper or more diverse talent pools have a decided advantage. Instead of being unable to fill critical openings, skill development programs can provide viable prospects, helping a company maintain an effective security posture.¹²

Zero trust pacesetters dedicate a higher percentage of their cybersecurity budget to developing the skills of cyber resources via a culture of continuous learning. This is reflected in their cyber talent retention rates, which are 10% higher than other organizations (60% versus 50%).

Two practices can inform an adaptive cyber talent management system:

1. Transform security talent management processes to focus on hiring for aptitude, attitude, and broad experience:

- Define requirements for skills, aptitudes, and abilities for each cybersecurity role. Combined with broader performance management objectives, this can make it easier for managers to identify skill gaps to address through recruitment and training initiatives. Consider investing in talent solutions that provide regular updates to skills, roles, and development criteria so that talent variables are updated alongside new technologies and operational requirements.
- When hiring, prioritize assessment of behavior and competency more than experience. With the advent of cloud, security events are multiplying faster than many teams can manage. Cybersecurity professionals must be flexible, evolving their skills to adapt to emergent risks. They must also be proficient in working alongside automated security solutions. For new threats, a familiarity with tactics, techniques, and business processes may supersede cybersecurity operations experience.
- Apply cyber aptitude tests to identify latent potential in the candidate selection process. Assess the underlying cybersecurity skills, attitudes, and behaviors of successful candidates, then use these insights to expand the potential talent pool beyond the security organization. This can add greater diversity to the workforce, introduce new ways of thinking, and expand options for addressing challenges in different ways.

2. Develop and retain people by fostering a culture of continuous learning and innovation. Enhance zero trust security operations by engaging talent in new ways:

- Establish a training program for security staff to learn other parts of the business. Provide deeper operational insight into critical business processes so they better understand any associated risks.
- Implement AI and other tools to inform continuous learning efforts across the human resource lifecycle. Recognize potential talent identified during recruitment and optimize it through customized learning and development. This can rapidly bring new employees up to speed, foster teamwork across specialty areas, create a secondary resource pool for backup coverage, and keep security operations teams up to date as new threats arise and new technologies emerge.
- Foster a culture that values not just knowledge, but the propensity to learn. Provide opportunities for professional development and growth to improve staff retention. Define success criteria and career paths for specific roles. Create incentives that encourage top talent to share their expertise with others and grow with the organization.

Consider these questions to become a zero trust pacesetter:

- How can we supplement our existing security architecture with zero trust capabilities? What is fundamentally different and requires a new approach?
- Through what methods is our organization developing an integrated view of threats to enhance visibility, increase the agility of our security operations, and improve incident response capabilities?
- How have we incorporated zero trust controls across our entire digital estate, including networks, data, users, workloads, and devices?
- In what ways can we adapt cyber talent practices to make the most of our zero trust strategy?

Research methodology

In the fourth quarter of 2020, the IBM Institute for Business Value, in collaboration with Oxford Economics, surveyed over 1,000 security and operations leaders across industries and geographies to gain an in-depth understanding of what constitutes an effective zero trust security strategy and how zero trust capabilities are being implemented.

To understand threats to critical infrastructure, the survey collected data about IT- and OT-related cybersecurity risks and the maturity, performance, and effectiveness of organizations' capabilities to manage and mitigate them. This included the adoption of leading practices, as well as future priorities and initiatives. It also explored the benefits respondents have realized from their approach to security operations.

Analysis of data revealed that 23% of organizations—a group we named “zero trust pacesetters”—are ahead of peers in implementing zero trust capabilities to protect critical resources across operational environments. By assessing performance measures and leading practices, we concluded they are deriving significant business and security benefits from this approach.

A confirmatory factor analysis (CFA) provided insights into which factors are driving benefits. These include operational cyber risk and security practices; AI-driven analytics and automation; and zero trust practices to secure data, networks, users, devices, and workloads. From this, we derived an approach to zero trust operations based on 4 essential building blocks and a set of mutually reinforcing practices.

About the authors



Chris McCurdy

Vice President and General Manager
IBM Security Services
cmccurdy@us.ibm.com

Chris has more than 25 years in IT consulting and has helped large enterprise and government clients with the design, deployment, and management of their complex information technology programs. He drives the worldwide go-to-market strategy for IBM Security and is responsible for managing sales globally. He has grown IBM Security business revenue to double-digit growth over the past 5 years. Chris holds a Bachelor of Business Administration in Information Systems from Baylor University and is a Certified Information Systems Auditor.



Dr. Shue-Jane Thompson

Senior Partner, Security Strategy & Growth—Distinguished Industry Leader
IBM Global Business Services
shuejane@us.ibm.com
linkedin.com/in/shuejane

Shue-Jane oversees cybersecurity solution innovation, integration, and services sales and delivery for clients worldwide. She has more than 30 years of experience in academia, commercial, government, and international technology and business management environments, including managing many large-scale IT, cyber, cloud, and mission-operation programs.



Lisa Fisher

Global Benchmark Research Leader
—Industrial, EE&U, T&T and MEA
IBM Institute for Business Value
linkedin.com/in/lisa-giane-fisher
lfisher@za.ibm.com

Lisa is responsible for producing benchmarking research, for all industries and regions, to envision and articulate the impact of technologies on business from cyber risk and cybersecurity perspectives. Lisa is based in South Africa.



Gerald Parham

Global Research Leader—
Security & CIO
IBM Institute for Business Value (IBV)
linkedin.com/in/gerryparham/
gparham@us.ibm.com

Gerald leads the Security and CIO research portfolios within the IBM Institute for Business Value. He focuses on security strategy and cyber value chains, in particular the relationship between strategy, risk, security operations, identity, privacy, and trust. He has more than 20 years of experience in executive leadership, innovation, and intellectual property development.

Related IBV reports

Parham, Gerald, Shue-Jane Thomson, Shawn Dsouza, and Shamla Naidoo. "The new era of cloud security: Use trust networks to strengthen cyber resilience." IBM Institute for Business Value. March 26, 2021. <http://ibm.co/cloud-security-cyber-resilience>

Comfort, Jim, Blaine Dolph, Steve Robinson, Lynn Kesterson-Townes, and Anthony Marshall. "The hybrid cloud platform advantage." IBM Institute for Business Value. 2020. <https://www.ibm.com/thought-leadership/institute-business-value/report/hybrid-cloud-platform>

"2021 CEO Study: Find your essential: How to thrive in a post-pandemic reality." IBM Institute for Business Value. 2021. <https://www.ibm.com/thought-leadership/institute-business-value/c-suite-study/ceo>

Payraudeau, Jean-Stéphane, Anthony Marshall, and Jacob Dencik. "Digital Acceleration." IBM Institute for Business Value. 2021. <https://www.ibm.com/thought-leadership/institute-business-value/report/digital-acceleration>

IBM Institute for Business Value

The IBM Institute for Business Value, part of IBM Services, develops fact-based, strategic insights for senior business executives on critical public and private sector issues.

For more information

To learn more about this study or the IBM Institute for Business Value, please contact us at iibv@us.ibm.com. Follow @IBMIHV on Twitter, and, for a full catalog of our research or to subscribe to our monthly newsletter, visit: ibm.com/ibv.

Notes and sources

- 1 “IBM 2021 X-Force Threat Intelligence Index.” IBM Security. February 24, 2021. <https://www.ibm.com/security/data-breach/threat-intelligence>
- 2 Paul, Kari. “Who’s behind the Kaseya ransomware attack – and why is it so dangerous?” *The Guardian*. July 7, 2021. <https://www.theguardian.com/technology/2021/jul/06/kaseya-ransomware-attack-explained-russia-hackers>; Kenny, Caroline and Pamela Brown. “Greater focus on defense of critical infrastructure against cyberattacks is needed, says cyber agency chief.” CNN. June 27, 2021. <https://www.cnn.com/2021/06/27/politics/brandon-wales-cyber-security-cnntv/index.html>
- 3 Marks, Joseph “The Cybersecurity 202: The Kaseya attack is a revolution in sophistication for ransomware hackers” *The Washington Post*. July 8, 2021. <https://www.washingtonpost.com/politics/2021/07/08/cybersecurity-202-kaseya-attack-is-revolution-sophistication-ransomware-hackers/>; Caltagirone, Sergio, Dr. Tom Winston, and Kyle O’Meara. “2020 ICS Cybersecurity Year in Review.” Dragos. <https://www.dragos.com/year-in-review/>
- 4 Kramer, Andrew E., Michael Schwirtz, and Anton Troianovski. “Secret Chats Show How Cybergang Became a Ransomware Powerhouse.” *The New York Times*. May 29, 2021. <https://www.nytimes.com/2021/05/29/world/europe/ransomware-russia-darkside.html>
- 5 Osborne, Charlie. “Colonial Pipeline attack: Everything you need to know.” ZDNet (US Edition). May 13, 2021. <https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/>
- 6 “Executive Order on Improving the Nation’s Cybersecurity.” The White House Briefing Room website. May 12, 2021. <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>
- 7 Parham, Gerald, Shue-Jane Thomson, Shawn DeSouza, and Shamla Naidoo. “The new era of cloud security: Use trust networks to strengthen cyber resilience.” IBM Institute for Business Value. March 26, 2021. <http://ibm.co/cloud-security-cyber-resilience>
- 8 Ibid.
- 9 Pollard, Jeff and Stephanie Balaouras. “Craft Zero Trust Security Metrics That Matter - Performance Management: The Zero Trust Security Playbook.” Forrester. March 24, 2020. <https://www.forrester.com/report/Craft+Zero+Trust+Security+Metrics+That+Matter/-/E-RES136188?objectid=RES136188>
- 10 OAuth, or Open Authorization, is an authorization process. It allows third-party services to exchange user information without users having to give away their passwords. SAML, or Security Assertion Markup Language, is an authentication process. Both applications can be used for web single sign-on (SSO), but SAML tends to be specific to a user, while OAuth tends to be specific to an application. They are both required and work together.
- 11 Johnson, David, Samuel Stern, et al. “Focus On Employees’ Daily Journeys To Improve Employee Experience.” Forrester. April 20, 2018. <https://www.forrester.com/report/Focus+On+Employees+Daily+Journeys+To+Improve+Employee+Experience/-/E-RES126042?objectid=RES126042>
- 12 Parham, Gerald, Shue-Jane Thomson, Shawn DeSouza, and Shamla Naidoo. “The new era of cloud security: Use trust networks to strengthen cyber resilience.” IBM Institute for Business Value. March 26, 2021. <http://ibm.co/cloud-security-cyber-resilience>

About Benchmark Insights

Benchmark Insights feature insights for executives on important business and related technology topics. They are based on analysis of performance data and other benchmarking measures. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

© Copyright IBM Corporation 2021

IBM Corporation
New Orchard Road
Armonk, NY 10504
Produced in the United States of America
July 2021

IBM, the IBM logo, ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at: ibm.com/legal/copytrade.shtml.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

This report is intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. IBM shall not be responsible for any loss whatsoever sustained by any organization or person who relies on this publication.

The data used in this report may be derived from third-party sources and IBM does not independently verify, validate or audit such data. The results from the use of such data are provided on an “as is” basis and IBM makes no representations or warranties, express or implied.

