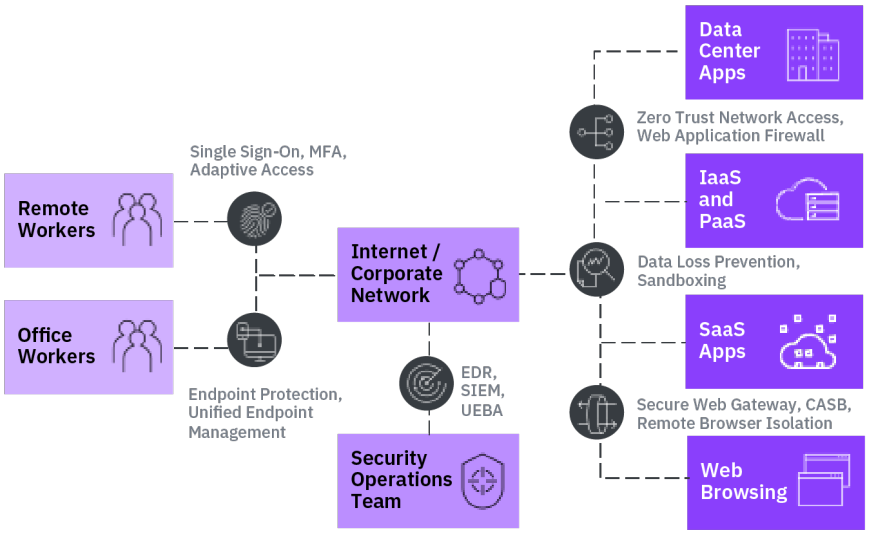
Secure Your Remote and Hybrid Workforce with Zero Trust

Operating a business now means supporting a workforce from any location on any device – connecting to resources hosted in multiple environments. A zero trust approach can help organizations empower their workforce by correlating security information across all security domains to quickly enforce conditional access based on a model of least privilege. This can help improve the user experience by reducing the barriers to access resources without sacrificing security.

"76 percent of participants said remote work would increase the time to identify and contain a data breach."

- Cost of a Data Breach[1]



Enable your anywhere workforce with everywhere security

1. Ponemon Institute, Cost of a Data Breach Report 2020, sponsored by IBM Security, July 2020

IBM Security Solution Blueprint

To put zero trust into action to secure the remote and hybrid workforce you'll want to address the following threat vectors by implementing critical capabilities indicated (●) for the specific security challenge you want to address.

Map hybrid workforce challenges to zero trust capabilities:

	Replace VPNs to reduce network access risks	Protect employees from phishing attacks	Secure risky internet behavior
Get Insights			
Application Discovery	●	○	●
Unified Endpoint Management	○	●	○
Vulnerability Management	○	●	○
Enforce Protection			
Adaptive Access	●	●	○
Cloud Access Security Broker	○	○	●
Data Loss Prevention	○	○	●
E-mail Filtering	○	●	○
Endpoint Protection	○	●	○
Multi-factor Authentication	●	●	○
Remote Browser Isolation (RBI)	○	●	●
Sandbox	○	○	●
Zero Trust Network Access	●	○	○
Detect & Respond			
Endpoint Detection and Response	○	●	●
User and Entity Behavior Analytics	●	●	○
Extended Detection and Response	●	●	●

Key metrics for success:

1. Ponemon Institute, Cost of a Data Breach Report 2020, sponsored by IBM Security, July 2020

1. What percentage of employees are adopting more than one form of authentication across all channels?
2. What percentage of devices and access points are being monitored and managed for security?
3. What percentage of applications have been migrated from a VPN-based remote access to ZTNA-based access?

Need assistance applying zero trust to your hybrid workforce initiatives?

Contact us to schedule a no-cost Framing and Discovery Workshop. With this garage-style workshop, our experts will work with you to:

- Map out your business goals and define a zero trust strategy tailored to your specific needs
- Understand the landscape and capabilities offered by your current investments and identify gaps
- Clarify and prioritize zero trust projects and initiatives to ensure demonstrable success.

Visit: https://www.ibm.com/garage and select *schedule a consult* to book your workshop. You'll walk away with a prioritized list of zero trust initiatives, a detailed journey map, actionable next steps, and all exercises organized in a PDF outcomes deck.

1. Ponemon Institute, Cost of a Data Breach Report 2020, sponsored by IBM Security, July 2020

Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

For more information

To learn more about IBM's zero trust approach, please contact your IBM representative or IBM Business Partner, or visit the following website: http://ibm.com/security/zero-trust