

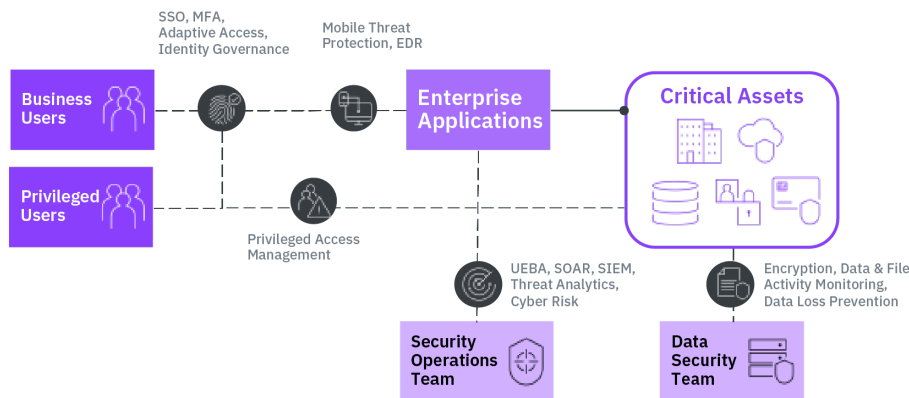


Reduce the Risk of Insider Threats with Zero Trust

Insider threats can be costly and disruptive to the business. A zero trust approach helps isolate threats and insulate your most valuable resources. It can also help with dynamic enforcement of security controls and automating responses to the threats targeting your business. When you proactively manage these cybersecurity risks with a zero trust approach you can limit disruption to critical operations and strengthen resiliency.

The average annual total cost of insider threats rose to \$11.45M.

- Ponemon Institute¹



Reduce the risk of insider threats with a zero trust approach

¹ Ponemon Institute, 2020 Cost of Insider Threats Global Report, 2020.



IBM Security Solution Blueprint

To put zero trust into action to reduce the risk of insider threats you'll want to consider each of the critical capabilities indicated (●) for the specific security challenge you want to address.

Map insider threat challenges to zero trust capabilities:

	Compromised credentials and mobile phishing	Data exfiltration from malicious insiders	Privileged account misuse
Get Insights			
Cyber Risk Management	●	●	●
Data Discovery & Classification	○	●	○
Unified Endpoint Management	●	●	○
Enforce Protection			
Activity Monitoring	●	●	●
Adaptive Access	●	●	○
Identity & Data Governance	●	●	●
Multi-Factor Authentication	●	○	●
Privileged Access Management	○	●	●
Detect & Respond			
Endpoint Detection and Response	●	○	○
Network Detection	●	●	○
Security Information and Event Management	●	●	●
Security Orchestration Automation and Response	●	●	●
User and Entity Behavior Analytics	●	●	●

1 Ponemon Institute, 2020 Cost of Insider Threats Global Report, 2020.



Key metrics for success:

1. Have you seen a decrease in the number of known exploits on critical systems in the last year? If so, what is the percentage of change?
2. What percentage of your incident response are you able to automate, and what is your average time to contain an insider incident?
3. What percentage of your privileged users are required to use privileged access management tools?

Need assistance applying zero trust to your insider threat 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.



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.

© Copyright IBM Corporation 2021.

IBM, the IBM logo, and 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 <https://www.ibm.com/legal/us/en/copytrade.shtml>, and select third party trademarks that might be referenced in this document is available at https://www.ibm.com/legal/us/en/copytrade.shtml#section_4.

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:



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>