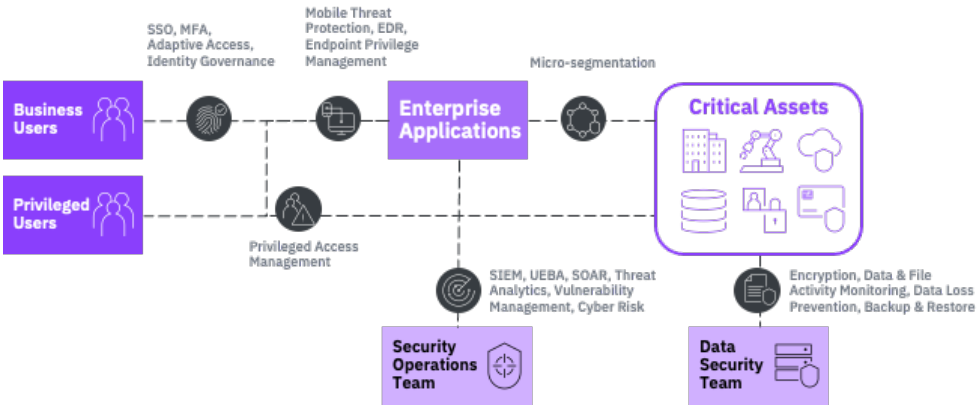
Reduce the Risk of Business Disruption and Ransomware with Zero Trust

Persistent attacks like ransomware 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 financial damage,[2] reduce disruption to critical operations and strengthen resilience.

> 23% of all security attacks in 2020 were the result of ransomware, up 15% from 2019.
>
> - IBM Security X-Force[1]



Reduce the risk of business disruption with a zero trust approach

[1] IBM Security, *2021 X-Force Threat Intelligence Report, 2021*
[2] IBM Security, *Cost of a Data Breach Report 2021*

IBM Security Solution Blueprint

To put zero trust into action to reduce the risk of business disruption you'll want to consider each of the critical capabilities (rows) indicated (●) for the specific use cases (columns) you want to address.

Map business disruption use cases to zero trust capabilities:

	Ransomware:		Compromised credentials and account takeover	Data exfiltration from malicious insiders
	Preparation and protection	Detection, response, and recovery		
Get Insights				
Cyber Risk Management	●	○	●	●
Data Discovery & Classification	●	○	○	●
Unified Endpoint Management	○	●	●	●
Vulnerability Management	●	●	○	○
Enforce Protection				
Activity Monitoring	●	○	●	●
Adaptive Access	●	●	●	●
Endpoint Privilege Management	●	○	○	○
Identity & Data Governance	●	○	●	●
Multi-Factor Authentication	●	○	●	○
Micro-segmentation	●	●	○	○
Privileged Access Management	●	○	○	●
Detect & Respond				
Data Resilience	●	●	○	○
Endpoint Detection and Response	●	●	●	○
Network Detection	○	●	●	●
Security Information and Event Management	○	●	●	●
Security Orchestration Automation and Response	○	●	●	●
Threat Intelligence	○	●	○	○
User and Entity Behavior Analytics	○	●	●	●

Key metrics for success:

1. What percentage of endpoint devices and network communications are monitored for suspicious activity, vulnerabilities, and policy violations?
2. What percentage of your incident response are you able to automate, and what is your average time to contain an incident?
3. What percentage of your privileged users are required to use privileged access management tools?
4. What percentage of your backup system is protected with an isolated environment to ensure data cannot be compromised?

Need assistance applying zero trust to your business resiliency 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 and cyber resilience 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.

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

---