Microsoft

Pillars for cyber resiliency in government

Minimize security risks with a strong cyber resiliency foundation that covers infrastructure, services, and employees

Reduce surface attack area

Ransomware infections rely on access. Identify your most critical on-premises and online services, business processes, dependencies, personnel, vendors, and suppliers—and prioritize security based on risk.

In 75%

of human-operated ransomware attacks, bad actors leveraged compromised account credentials to gain unauthorized access and spread malicious payloads.

Modernize legacy systems

The cloud has native security capabilities that legacy systems lack. Plan and implement a strategy that protects from threats by moving to hyperscale, AI-based cloud security solutions.

Over 80%

of security incidents could be addressed through modern security approaches.

Enhance threat detection and response

Adversaries are overwhelming defenses using AI and service frameworks to increase their speed and scale. A comprehensive threat detection and response strategy requires machine learning tools to scale defensive capabilities.

60%

of organizations impacted by a ransomware attack had monitoring silos, limited ability to detect end-to-end threats, and inefficient security operations.

Automate recovery and redundancy

Any organization can be compromised. Redundancy and recovery plans must be planned to minimize downtime, ensure operational continuity, and safely return to normal healthy operations.

44%

of organizations impacted by a ransomware attack did not have immutable backups for the impacted systems.

Strengthen your agency's cyber resiliency foundation today.

Learn more.

All statistics sources from Microsoft Digital Defense Report 2022