unisys

Enterprise cyber resilience

A guide for accelerating recovery from worst-case scenarios

Contents

The value of enterprise cyber resilience 3

Steps toward increased resilience 4

- **01** Assess your cyber environment 4
- **02** Develop a resilience strategy 5
- **03** Establish cybersecurity fundamentals 6

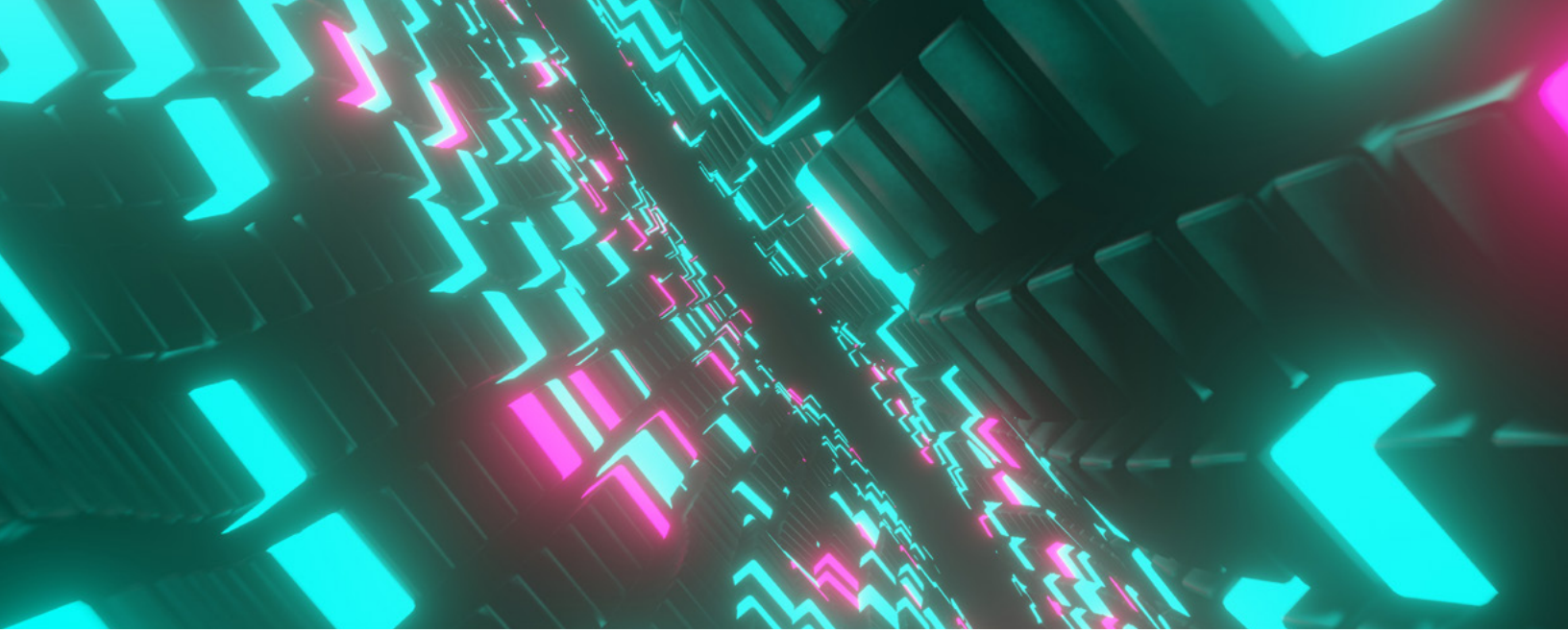
Benefits of enterprise cyber resilience 7

How Unisys can help 8

The value of enterprise cyber resilience

In the London Underground, signs reading "Mind the gap" caution train passengers to take care when moving from a station platform to a train doorway or the reverse. This phrase can be just as helpful when considering cybersecurity gaps and potential vulnerabilities in your cyber resilience strategies. Enterprise longevity can be measured in your organization's ability to weather unplanned storms. Cyber resilience is crucial to adapt and respond effectively to disruptions, risks and unexpected events that could impact operations.

Resilience allows you to maintain continuity, minimize downtime, recover quickly from cyber attacks and disasters and keep critical business processes functioning seamlessly. Investing in resilience measures can help you safeguard your reputation, build trust with employees, customers and partners and demonstrate your commitment to long-term sustainability and growth. Taking these three steps can get you started on the path toward resilience.



Steps toward increased resilience

01 Assess your cyber environment

The path to cyber resilience begins with evaluating your operations environment. An assessment gives you a thorough understanding of security risks and insights to develop a comprehensive strategy, fortifying your organization against cyber threats.

- Map out your critical assets, systems, dependencies and all other components of your cyber environment.
- Identify security threats, key risks and potential security vulnerabilities in your digital infrastructure.
- Assess the effectiveness of your organization's security measures, identifying gaps or weaknesses in your defenses, including those that have already resulted in an undetected compromise or have been potentially exploited.
- Use this intelligence to prioritize areas for improvement to tackle later as part of your strategic plan. Build ongoing assessments into your cybersecurity strategy to catch issues before they become problems.

Attack surface discovery

Attack surface discovery involves exploring all avenues an attacker could use to infiltrate your systems and network. This includes discovering security risks and instances of shadow IT when employees adopt technology without first getting IT permission. Catching shadow IT can reduce your organization's exposure to new security risks and reduce waste.

02 Develop a resilience strategy

Use the insights gleaned from the assessment to build a foundation for resilience. An effective strategy involves robust policies, controls and procedures in line with your organization's risk tolerance and business objectives. Solidifying your strategy makes it easier to implement risk mitigation measures, strengthen your resilience posture, prepare for a worst-case security scenario and stabilize business operations if one occurs.

Ingredients for strategy success

When developing a comprehensive cyber resilience plan to protect your organization against cyber threats, prioritize incorporating several vital components.

- **Preparation and prevention** that recognizes that resilience begins long before an attack occurs
- **Incident monitoring and response** that provides visibility into possible attacks and minimizes the impact on operations
- **Backup and recovery** that restores data and system functionality after an incident
- **Business continuity** after a cyber attack or disruption
- **Employee training** to educate employees about cybersecurity best practices and encourage a security-aware culture
- **Regulatory compliance** to align your cyber resilience strategy with relevant legal and regulatory requirements
- **Continuous improvement** of resilience capabilities through ongoing monitoring

03 Establish cybersecurity fundamentals

After plotting your strategy, it's time to transform your existing security measures by reassessing current security protocols, technologies and practices to address emerging threats and vulnerabilities. This allows you to better protect your assets, data and operations from cyber risks and disruptions. Another cybersecurity imperative is strengthening your organizational readiness and response capabilities with incident response protocols, business continuity plans and disaster recovery strategies.

Core solutions for resilience

- **Managed detection and response:**

  Identify cybersecurity incidents promptly and minimize their impact on operations and security posture. Round-the-clock monitoring and immediate response capabilities help to safeguard your organization against cyber threats and attacks proactively.

- **Attack surface discovery:**

  Gain continuous visibility of exposed assets, enabling proactive risk mitigation, faster incident response and agile defenses as the environment and threats evolve.

- **Cyber resilience, integration and continuous innovation:**

  Weave cybersecurity practices seamlessly into your organization's operations, risk management and business strategies. Cyber threats are dynamic, so it's crucial to advance cybersecurity measures to stay ahead of an evolving threat landscape.

- **Disaster recovery:**

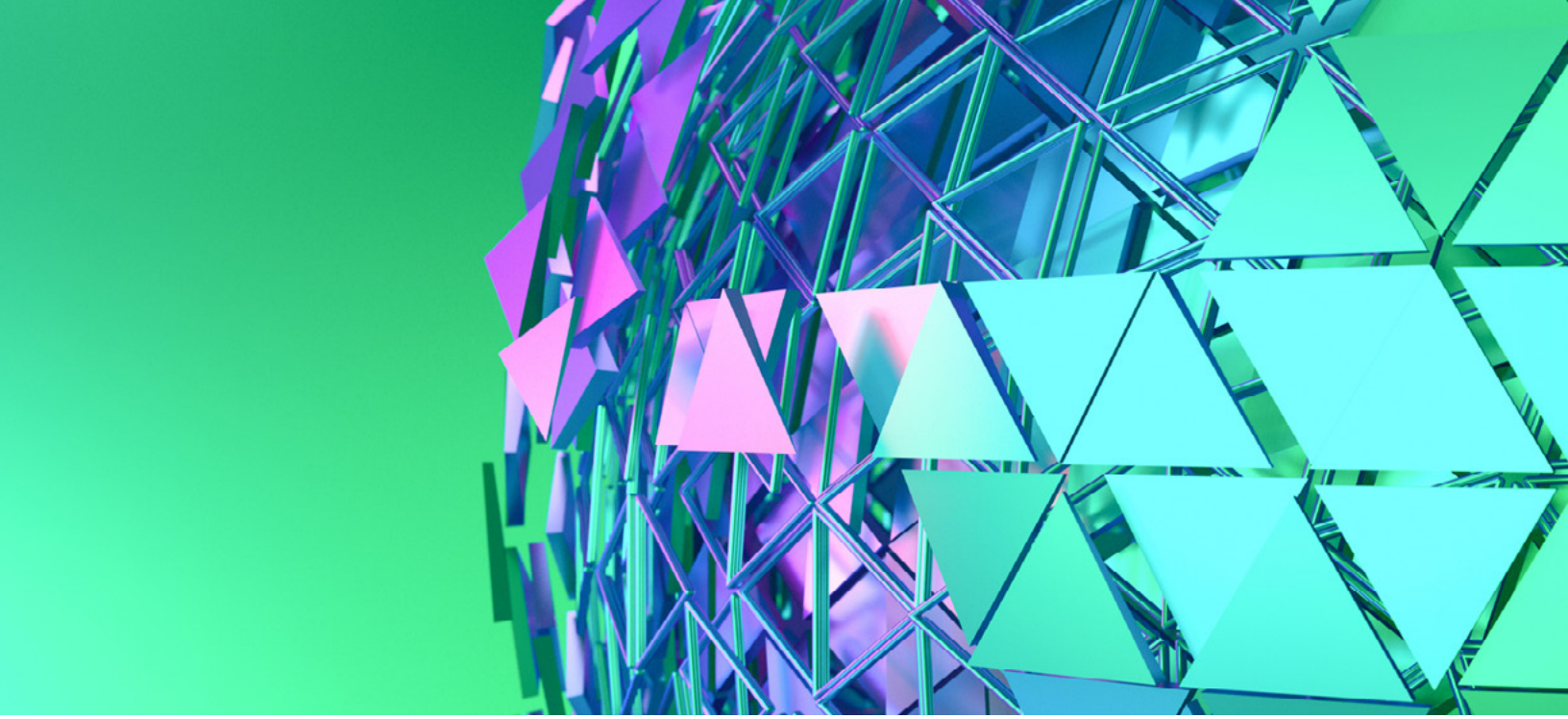
  Recover quickly from national disasters, like floods and earthquakes, and technological events, like server crashes, to minimize downtime and keep systems operable. Robust disaster recovery plans keep your business running smoothly after unexpected events.

- **Cyber recovery:**

  Maintain business continuity and limit your organization's time without critical assets like data access and communication systems after a cyber attack. Disaster recovery principles and practices, such as backup protocols, serve as a foundation for cyber recovery efforts while requiring additional resilience and protection measures like isolating affected systems.

- **Cybersecurity incident response:**

  Contain cyber attacks to prevent them from spreading and causing additional damage to your organization's systems and data. Incident response secures your data and restores affected systems to production.



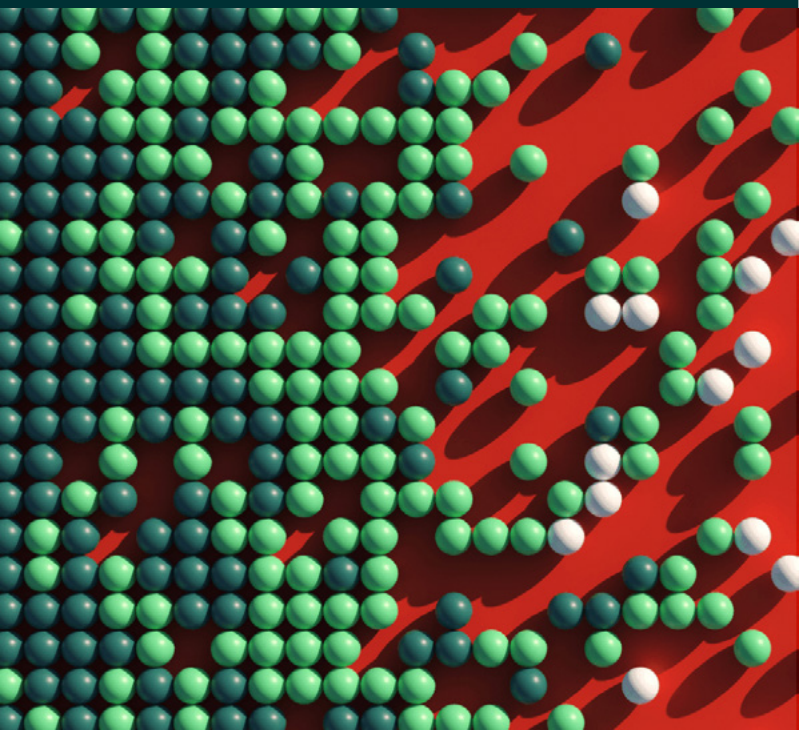
Benefits of enterprise cyber resilience

Adopting a resilient approach — especially when you prioritize risk avoidance — offers several advantages that bolster your organization's cybersecurity. These benefits contribute to building a robust framework for resilience that makes it easier to overcome potential challenges.

- **Risk identification:** Understand your organization's risks so you can tailor your resilience strategies to mitigate potential vulnerabilities effectively.
- **Risk management:** Address and mitigate risks strategically for resilience and continuity during disruptions.
- **Risk prevention:** Reduce the probability of successful attacks that can impact business operations.
- **Increased flexibility:** Gain agility in evolving with changing circumstances and adapting your approach to address emerging risks and mitigate threats, with minimal impact on operations.
- **Enhanced preparedness:** Prepare your organization for various scenarios, including cyber threats and system failures, with tools and strategies for effectively responding to disruptions.

How Unisys can help

Unisys cybersecurity experts can guide your efforts at enhancing enterprise resilience across all stages of your security journey, from initial assessment to ongoing management. Our comprehensive services allow you to build and maintain your resilience capabilities.



End-to-end support:

Benefit from expertise in identifying risks, determining tools to mitigate those risks, creating resilient infrastructure and managing operations effectively.

Customized solutions:

Gain solutions tailored to your organization's specific needs, current and future IT infrastructure, unique challenges and business requirements.

Continuous monitoring:

Gain visibility into potential threats or disruptions to business operations with ongoing systems monitoring.

Could your cyber resilience be stronger?

Visit unisys.com or contact us to schedule a consultation with our experts today.

unisys

unisys.com

08/26 7094-12721