LOGICALIS
Architects of Change

Platinum
Business
Partner
IBM

Solution Brief

Smarter, More Resilient Cyber Defenses

Building a cyber resilience strategy with IBM® Security Randori® and IBM® QRadar®.

Why Cyber Resilience Matters

Cyber attacks can not only be costly, they can cause significant harm to a business, harming profit margins, customer trust, and the brand's reputation. While cybersecurity is a critical first line of defense against these threats, it is equally important to have plans to mitigate risk and loss in the event of a damaging data event, which is where cyber resilience comes in.

Cyber resilience is an enterprise-wide risk-based strategy designed to manage risks, threats, vulnerabilities, and the effects on information and assets. It balances risk against business opportunities, and it must weigh the benefits and drawbacks of prevention, detection, and corrective controls.

One way to look at cyber resilience is through the lens of a lifecycle based on the Information Technology Infrastructure Library (ITIL) service lifecycle:

- **Strategy** identifies critical assets, such as information, systems, and services, that matter most
- **Design** work selects the controls, procedures, and training to prevent harm to those assets
- **Transition** work tests controls and refines incident detection to identify when critical assets are under stress
- **Operation** work controls, detects, and manages cyber events
- **Evolution** work continuously modifies procedures, training, design, and strategy to continually protect the changing IT environment

www.ibm.com/topics/cyber-resilience

To effectively develop, execute, and manage a cybersecurity resilience program depends, among other things, on having the necessary cybersecurity expertise and the right solutions.

Laying the Foundation for Cyber Resilience with IBM Security Randori and IBM QRadar

Security teams and security solution providers are only as effective as the tools they have to work with. Inefficient, outdated tools leave gaps in security, drain resources, waste time, and expose the organization to unnecessary risk. Modern, effective security tools, on the other hand, are the necessary building blocks of a modern and effective cyber resilience program.

Two solutions from the IBM Security portfolio, Randori and QRadar, offer the features and coverage needed to lay the foundation for a successful, future-ready, and adaptable cyber resilience strategy: they allow you to understand and protect your attack surface, while detecting, preventing, and responding to threats in advance.

Attack Surface Management with IBM Security Randori Recon

IBM Security Randori Recon is an attack surface management (ASM) SaaS solution designed to uncover external exposures through the lens of an adversary. It scans, maps, and monitors your attack surface, exposing hidden and unknown assets, shadow IT, vulnerabilities, misconfigurations, and other potential risks. These risks are then prioritized based on adversarial temptation and the risk posed to your organization, so your team can answer one of the top challenges facing cybersecurity teams: where to focus your efforts.

303%
return investment of over 3 years.

90%
fewer hours of vulnerability scanning per year.

85%
reduction in losses due to external attack.

www.ibm.com/products/randori-recon

Understand Your Cyber Risk

Make more informed decisions with continuous asset discovery and risk-based prioritization.

Improve Efficiency

Reduce the time and effort your security team spends on vulnerability scanning and attack surface exposure analysis.

Streamline Operations

Eliminate data silos with bidirectional integrations that work with your security stack.

Continuous Automated Red Teaming with IBM Security Randori Attack Targeted

IBM Security Randori Attack Targeted performs continuous automated red teaming (CART) to test, validate, and improve your security posture. An add-on to Randori Recon, it extends the benefits of ASM by adding objective-driven campaigns and after-action reporting. Through continuous assessment and validation, you can maintain the effectiveness of your cybersecurity measures, proactively manage threats, and truly understand your organization's risk landscape.

30%
30% reduction in time to triage exposures for remediation.

90%
90% reduction in exposure analysis efforts.

75%
labor savings of up to 75% from augmented red team activities.

www.ibm.com/products/randori-recon/add-ons/attack-targeted

Test Your Whole Security Program

Shift your mindset from find-and-fix to resilience by testing people, processes, and technologies.

Validate Security at Scale

Outpace change and outthink attackers through iterative validation that targets security blind spots.

Deepen Your Insights

Reduce resource constraints and extend your team's insights through automated runbooks, remediation guidance, and monthly reports.

Threat Detection and Response with IBM QRadar

IBM Security QRadar Suite is a modern threat detection and response solution that unifies and accelerates the security analyst experience. Enterprise-grade AI and automation dramatically increase productivity, and a common user interface integrates products for endpoint security (EDR, XDR, MDR), log management, SIEM, and SOAR.

Unified Analyst Experience

Analysts work more quickly and efficiently with shared insights, automated actions, and an intuitive user interface.

Cloud Delivery, Speed, and Scale

Delivered as a service on AWS, the suite allows for simplified deployment across cloud environments and integration with public cloud and SaaS log data.

Open Platform with Pre-Built Integrations

Built on an open platform and a wide partner ecosystem, the suite brings together core technologies and 900+ prebuilt integrations for flexibility and choice.

The IBM QRadar product suite includes the most essential products to help teams stay ahead of threats and build a foundation for cybersecurity and cyber resilience.

IBM QRadar EDR

Protect endpoints against zero-day threats with automation, machine learning, and behavioral models that detect anomalies and respond in real time.

IBM QRadar Log Insights

Easily perform analytics on terabytes of data with greater speed and efficiency thanks to simplified data ingestion and rapid search, investigations, and visualizations.

IBM QRadar SIEM

Access more accurate, contextualized, and prioritized alerts with an SIEM that uses AI, network and user behavior analytics, and real-world threat intelligence.

IBM QRadar SOAR

Automate and orchestrate incident response workflows and ensure processes are followed in a consistent, optimized, and measurable way.

www.ibm.com/qradar

Together, these three security solutions from IBM can help identify critical assets, prevent harm to those assets, and continuously evolve your cybersecurity program through automated improvements. With the proper implementation, they can form important components of both a cybersecurity strategy and a cyber resilience strategy.

Create a Resilient, Future-Ready Cyber Resilience Program

with Logicalis and the IBM Security Portfolio

Cyber resilience and cybersecurity depend on having modern tools that can meet modern threats - and designing, implementing, and managing these programs depends on having sufficient expertise and resources.
For today's busy and budget-constrained IT teams, evaluating, evolving, and maintaining an effective, robust cybersecurity and cyber resilience program can be a tall order.

Fortunately, Logicalis is here to help.

As an IBM Platinum Partner with a deep bench of cybersecurity specialists, we can help you leverage the IBM Security portfolio to create, implement, and manage a modern cyber resilience strategy, so your team can focus on what matters most: your business.

Logicalis Cybersecurity Services Include:

- Cybersecurity and cyber resilience assessments
- Endpoint security
- Network security
- Cloud security
- Advisory services

Schedule Your Free Executive Briefing
logicalis-hub.com/IBM