Kyocera Business Solutions: Cybersecurity Services

Kyocera helps reduce your risk for data loss, cyber threats, and provide business continuity with our comprehensive cybersecurity solutions—designed to keep your organization secure, resilient, and future-ready.

1 SentinelOne End-point Detection and Response Platform (EDR)

2 Managed Detection and Response (MDR)

3 Business Continuity and Disaster Recovery (BCDR)

4 Email security

5 MFA via DUO, Google Authenticator and Microsoft Authenticator

6 Cybersecurity training

7 Firewall Security

1. SentinelOne EDR Platform

Is one of the top three EDR (Endpoint Detection and Response) platforms worldwide, providing AI-powered protection for laptops, servers, and IoT.

Improved Security: Provides advanced benefits over traditional antivirus (AV) by offering continuous, behavior-based monitoring and response for both known and unknown threats.

Operational Efficiency: Automates security tasks, reducing manual workload.

Scalability: Easily adapts to growing environments and remote workforces.

Compliance Support: Helps meet regulatory requirements through detailed logging and reporting.

2. Managed Detection and Response (MDR)

MDR combines advanced EDR technology with human expertise to monitor, detect, investigate, and respond to threats 24/7/365.
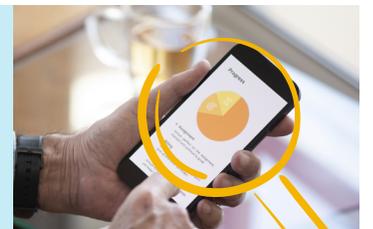
Rapid Incident Response: Cuts detection and response time.

Cost-Effective: More affordable than staffing a full security team.

Scalable Security: Adapts to businesses of all sizes and industries.

Improved Compliance: Helps meet regulatory requirements (e.g., HIPAA, GDPR, PCI-DSS) with detailed logs, reports, and incident documentation.

Expert Support: Skilled analysts investigate threats quickly to minimize damage and downtime.

Advanced Threat Detection: AI and behavioral analytics catch attacks traditional tools miss.

Enhanced Visibility: Clear insight into network activity and threat patterns.

3. Business Continuity and Disaster Recovery (BCDR)

Combines backup and disaster recovery to keep operations running smoothly. With failover systems and rapid recovery objectives built in, BCDR provides the ability to restore critical systems and data in hours, not days.

Business Continuity: Keeps critical operations running during outages, cyberattacks, or natural disasters.

Cybersecurity Resilience: Defends against ransomware with isolated backups and clean restores.

Integrated Protection: Works with endpoint and threat detection tools.

Compliance & Audit Readiness: Meets HIPAA, GDPR, PCI-DSS and provides detailed logs for audits.

Scalability: Adapts to growing data volumes and evolving cloud or hybrid environments.

Cost Efficiency: Reduces downtime and data breaches. Avoids costly emergency IT interventions.

4. Email Security

A comprehensive, cloud-based solution that protects against phishing, malware, ransomware, and business email compromise (BEC). Proofpoint email security uses AI, machine learning, and behavioral analysis along with targeted attack protection and reputation analysis to block threats and filter spam.

Reduces Risk of Data Breaches: By blocking threats before they reach users.

Enhances User Experience: Filters out spam and malicious content with minimal disruption.

Improves Compliance: Helps meet standards like HIPAA, GDPR, and PCI-DSS.

Supports Incident Response: With detailed logs and message tracing for forensic analysis.

5. Multi-Factor Authentication (MFA)

A security method that requires two or more verification factors to make unauthorized access far harder. Kyocera partners with Duo, Microsoft, and Google to deliver flexible, secure authentication across devices and apps.

Stronger Protection: Passwords are vulnerable to phishing and breaches; MFA adds layers that make it harder for attackers to gain access.

Minimizes Impact of Data Breaches: Stops attackers from using stolen credentials to reach sensitive systems.

Secure Remote Access: Essential for protecting cloud services, VPNs, and remote work environments.

Reduces Risk of Identity Theft: Even if a password is stolen, MFA blocks access by requiring a second factor only the real user has.

Compliance Ready: Meets HIPAA, GDPR, PCI-DSS requirements.

Builds Trust: Shows commitment to safeguarding users and sensitive data.

6. Breach Prevention Training Platform

A cybersecurity and compliance training platform for Managed Service Providers (MSPs) and small to medium-sized businesses (SMBs), designed to strengthen the human side of security. It delivers employee-focused training, compliance support, and risk monitoring with tools like Simulated Phishing Tests, Dark Web Monitoring, HIPAA & Regulatory Compliance Support, Employee Risk Scoring, AI Awareness Training and Microsoft 365 Productivity Training.
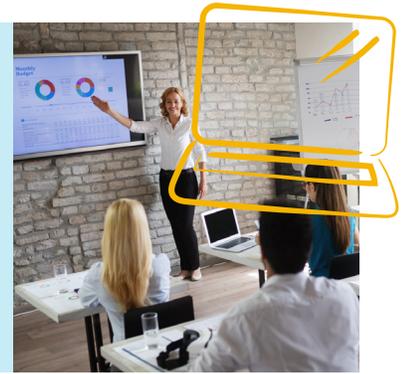
Reduces Cyber Risk: Empowers employees to act as a "human firewall."

Boosts Productivity: Enhances employee efficiency with targeted training.

Cost-Effective: Designed for organizations with limited budgets.

Improves Compliance: Simplifies regulatory requirements and audit readiness.

Supports MSPs: Adds scalable, client-friendly solutions.

7. Firewall Security

Kyocera partners with the world's leading firewall providers to block unauthorized access and cyber threats.

Threat Prevention: Blocks malware, ransomware and phishing before they reach your network.

Access Control: Define who can access networks and resources.

Compliance Support: Helps meet HIPAA, PCI-DSS, and GDPR requirements by enforcing security policies.

Application Control: Manages app use to reduce misuse and improve productivity.

Data Protection: Safeguard sensitive business data, customer information, and intellectual property.

Traffic Monitoring: Provides visibility into network activity and suspicious behavior.

Remote Access Security: Enables secure VPN connections, ensuring encrypted communication.

For more information please contact:

KYOCERA

kyoceradocumentsolutions.us