Address Security Threats Quickly and Efficiently

Automated, continuous security event monitoring with Xerox® Managed Print Services.

INTRODUCTION

Companies face many security challenges in their daily operations, from hackers and malware to outdated technology and third-party services. This includes their printers. Security issues are not a matter of "if" but "when." Ignoring cybersecurity can lead to serious consequences like data theft, disruptions, legal issues, and loss of customer trust.

Responding quickly to security events is crucial in this risky landscape. Automated and continuous monitoring of security events is key to spotting and dealing with potential threats promptly. Integrating security event monitoring into the print infrastructure is a crucial part of a company's overall security plan. It ensures that even regular tasks like printing and document management are always being watched and protected from security risks and data breaches.

INTRODUCING SECURITY EVENT MONITORING, AVAILABLE THROUGH XEROX® MANAGED PRINT SERVICES

Security Event Monitoring Service, offered as part of Xerox® Managed Print Services, is a crucial component of an organization's comprehensive cybersecurity strategy. Networked printers and multifunction printers (MFPs) can be susceptible to security risks (such as unauthorized access to printers, unusual printing activities, or attempts to compromise the device's firmware or settings), making it crucial to identify and notify about security-related events.

This service offers continuous, real-time monitoring of your printers, reducing the time taken to detect security breaches and allowing for rapid incident response. Its main goals are to spot and address potential security threats and breaches as they happen or shortly thereafter.

HOW DOES IT WORK?

Information about device activity is collected from the printers and MFP's within the fleet. This data is then analyzed and categorized by severity, enabling proactive measures to address potential risks before they escalate into breaches. Additionally, devices running Trellix Whitelisting/Allowlisting provide extra layers of information. All this data is presented in a Security Event Monitoring Dashboard, a centralized platform to update actions and close open security events to ensure proper management and follow-up.

A noteworthy enhancement to the Security Event Monitoring Service is its capability to integrate with SIEM (Security Information and Event Management) solutions. This enhances the value of threat data by combining it with other IT data, providing a comprehensive overview of a client's infrastructure and all associated security incidents and events. Currently, integrations are available with platforms like Trellix, Splunk, and LogRhythm.

DEVICE SECURITY EVENT MONITORING CAPABILITIES INCLUDE

- Security events parsed and categorized based on severity
- Security events managed and presented back through a single security dashboard
- More detailed information provided for quick, efficient response, with the ability to attach notes/close any action related to resolution
- Transmission to configured SIEM solution for analysis

BENEFITS OF A SECURITY EVENT MONITORING/SIEM INTEGRATION INCLUDE

- Deliver meaningful, actionable threat data from the printer to SIEM software
- Detect suspicious behavior early
- Respond quickly to MFP security events and reduce the impact of security breaches on your business
- Increase the efficiency of your security teams to prevent potential breaches
- Provide better log collection, data analysis, and security policy compliance reporting
- Access a broad view of all client IT infrastructure

xerox™

Discover comprehensive security solutions that go beyond the basics.

Security Event Monitoring is one of 6 Security Services available through Xerox® Managed Print Services.

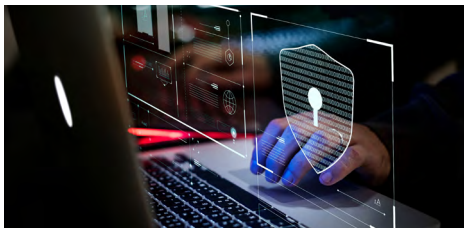
ADVANCED PROTECTION OF YOUR PRINT NETWORK WITH XEROX MPS

Printer Security Audit Service
Remotely manage configuration settings, security patches, firmware, and password.

Device Security Center
Snapshot of overall fleet health, relevant device security policies.

Certificate Management
Automation of the device certificate process including removal of expired certificates.

Workplace App Management
Remotely deploy and manage Xerox® ConnectKey® Apps across your entire printer fleet.



Security Event Monitoring
Security dashboard to review and manage events for proper handling.

SIEM Integration
Timely threat event communication with market-leading Security Information and Event Management (SIEM) tools.

CONCLUSION

The vigilant monitoring of the printer fleet serves as a crucial defense, safeguarding an organization's data, systems, and network infrastructure from a range of potential threats. This proactive investment in security is indispensable, protecting sensitive information, upholding operational continuity, and complying with data protection regulations.

For more information on how you can secure your organization's devices and data, visit **xerox.com/SecureMPSEvents.**