IBM Security QRadar EDR

Secure endpoints from cyberattacks

A modernized endpoint threat detection and response solution (EDR) designed to unify the security analyst experience and accelerate their speed across the full incident lifecycle. The portfolio is embedded with enterprise-grade AI and automation to increase analyst productivity, helping resource-strained security teams work more effectively across core technologies.

IBM Security® QRadar® EDR provides a more holistic EDR approach that:

Remediate Endpoint Threats

Remediates known and unknown endpoint threats in near real time with intelligent automation.

Attack Path Visualization

Enables informed decision-making with attack visualization storyboards

New AI-Powered Threat Detection

Empowers staff and helps safeguard business continuity with advanced continuous learning AI capabilities and a user-friendly interface

Industry-leading Alert Management

Automates alert management to reduce analyst fatigue and focus on threats that matter

Why IBM Security QRadar EDR?

100%

Visibility

Achieved 100% visibility across all evaluated stages of the MITRE ATT&CK framework.

100%

Detection

Achieved 100% of its detections without change configurations in MITRE ATT&CK Evaluations.

90%

Reduced false alert

AI-powered alert management system helps to ease analyst workloads.

Feature and benefits

AI-powered threat detection and insights

Key features

- Pre-execution prevention
- NanoOS and dual AI engines
- Attach visibility
- Threat hunting
- Ransomware prevention
- Behavioral detection
- API access
- Cyber assistant
- Custom playbook

Benefit

- AI-powered endpoint detection
- Complete hunt and response features
- High threat resolution
- Compliance monitoring
- Enterprise automation
- Deployment in any environment
- Managed detection and response (MDR)

Why it's better

Gain deeper visibility on your endpoints

Get a clear line of sight

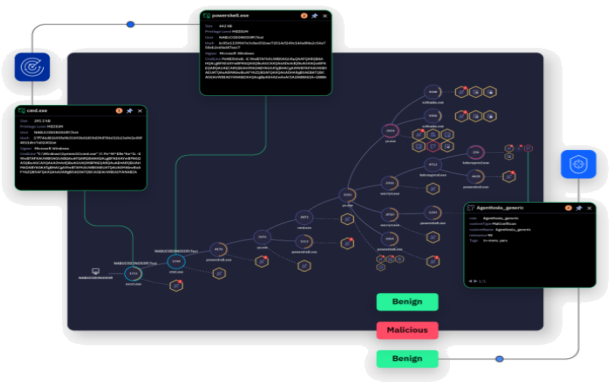
NanoOS technology provides deep visibility into the processes and applications running on endpoints.

Automate your response

AI detects and responds autonomously in near real time to previously unseen threats.

Move from reactive to proactive

Get ahead of attackers with easy-to-create detection and response use cases that return results in seconds, leaving dormant threats with no room to hide.



Requirements

- Server: Hardware requirements will based on the number of endpoint management.Please refer to system requirements
- Agent: Endpoint systems are supported on Linux, macOS, and Windows. Please refer to agent system requirements for supported versions.
- Note: For IBM Qradar EDR specifications and hardware/software support guidelines. Please refer to IBM Qradar EDR official website