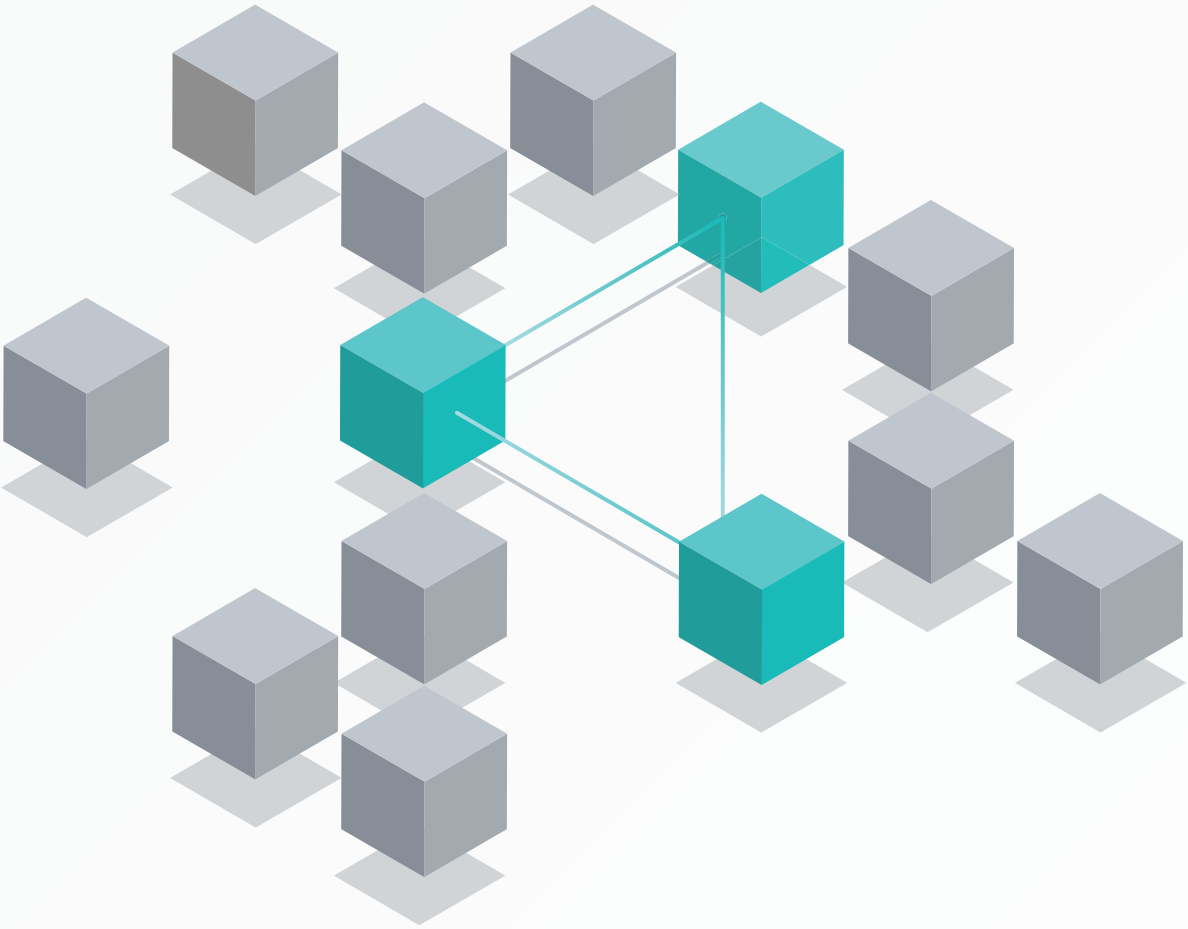
IBM Security QRadar EDR

AI-powered, automated endpoint security



IBM Security QRadar EDR offers a unique, forward-thinking approach to endpoint security.

The solution uses exceptional levels of intelligent automation, taking advantage of AI and machine learning, to help detect and remediate sophisticated known and unknown threats in near real-time. With deep visibility across endpoints, the solution combines expected features, such as MITRE ATT&CK mapping and attack visualizations, with dual-engine AI and automation to propel endpoint security into a zero trust world.

Why QRadar EDR?

1

Continuously learns as AI detects and responds autonomously in near real-time to new and unknown threats

2

Helps secure offline infrastructures, as well as on-premises and cloud environments

3

Maps threats against the MITRE ATT&CK framework and uses a behavioral tree for easy analysis and visualizations

4

Offers a bidirectional API that integrates with many popular security information and event management (SIEM) and security orchestration, automation and response (SOAR) tools

5

Provides heuristic, signature and behavioral techniques in its multilayered defense

6

Allows users to build custom detection strategies to address compliance or company-specific requirements without the need to reboot the endpoint

7

Simplifies and speeds response through guided or autonomous remediation

8

Offers automated, AI-powered threat detection and threat hunting including telemetry from indicators that can be customized for proprietary detection and granular search

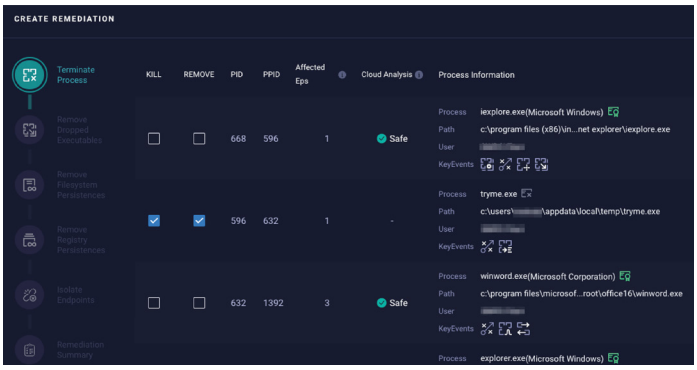
9

Makes remediation available with automated or single-click remote kill

10

Provides deep visibility with NanoOS, a unique hypervisor-based approach that works outside the operating system and is designed to be invisible to attackers and malware

QRadar EDR behavioral tree provides full alert and attack visibility.



QRadar EDR remediation automation simplifies incident remediation with clickthrough options.

Autonomous AI-powered endpoint detection and response (EDR)

- Uses continuous self-learning AI and machine learning to build an evolving baseline that protects endpoints from threats without requiring daily updates
- Future-proofs your organization with autonomous prevention of ransomware, fileless and in-memory attacks, both online and offline
- Supercharges gaps left by traditional security antivirus (AV) solutions with enhanced detection, visibility and control

High threat resolution

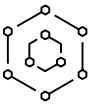
- Increases your understanding of threats in your environment mapped against tactics and techniques in the MITRE ATT&CK framework
- Helps reduce investigation time from minutes to seconds with threat intelligence and analysis scoring
- Uses prevalence monitoring to remove the guesswork needed to understand the impact and spread of infected artifacts across your organization

Complete hunt and response features

- Provides a user-friendly threat hunting platform with preconfigured hunt parameters that don't require database query knowledge
- Offers complete remediation guidance and clickthrough response automation to help you contain any situation within seconds

Compliance monitoring

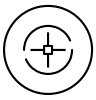
- Delivers full visibility into user behavior and application usage to enhance your organization's compliance policies and enforce standards
- Allows users to build custom detection strategies to address compliance or company-specific requirements using DeStra (Detection Strategy) scripting, without the need to reboot the endpoint
- Enables users to activate updates across the organization without endpoint intervention or downtime



Enterprise automation

– Helps you quickly implement new automations and functionality into your existing workflows using QRadar EDR API and integrations

– Integrates with SIEM and SOAR tools



Managed detection and response (MDR)

– Provides 24x7 monitoring, tracking and resolution of critical alerts while keeping you informed

– Helps you identify and track even the most sophisticated actors and run advanced threat hunting campaigns using both AI and our team's deep experience in intelligence and analysis

– Contains and remediates threats as soon as they're detected, minimizing your business risk and reducing damages and interruption of services

Deployment in any environment

– Provides options for cloud and on-premises infrastructures and works in offline environments with no need for daily signature updates

– Installs in seconds without complex integrations, becomes operational within minutes and coexists seamlessly with existing AV software with zero conflicts

– Leaves no impact on the endpoint during deployment, daily operations and even after responding to a live incident

For more information, visit:
To learn more about QRadar EDR, please contact your IBM representative or IBM Business Partner, or visit ibm.com/products/qradar-edr

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
May 2023