Secure your endpoints with the automated, intelligent power of AI

Challenges

Organizations must detect and mitigate threats before they become a problem

IT infrastructures continue to expand in scale, complexity and diversity, which poses an unprecedented challenge for security analysts. Endpoints are especially vulnerable. With increasingly sophisticated cyber attacks showing up daily, it's crucial to gain visibility into the vast environment of endpoints before security threats gain entry and begin to impact the organization. Traditional signature-based security software is no longer capable of mitigating these sophisticated new attacks. As a result, security analysts are overwhelmed with alerts and spend an inordinate amount of time separating false alarms from the real issues. They need a layer of automated protection to not only filter out the false positives but also detect new threats as they emerge.

The IBM Security QRadar EDR Solution

Protect your endpoints with the power of automation and AI

IBM Security QRadar EDR on AWS was developed by cyber security experts and security analysts as a continually improving platform that can automate and simplify threat detection and remediation. This new approach to endpoint security uses AI and Machine Learning (ML) to respond to known and unknown security threats in near real time. This is accomplished without detection by attackers by monitoring from outside the endpoint's operating system. Security analysts benefit from autonomous threat responses, high-fidelity actionable alerts and fewer false positives. IBM Security QRadar EDR on AWS delivers ever-evolving endpoint security for the present and future zero trust world.

Benefits

IBM Security QRadar EDR on AWS leverages intelligent automation and AI to help automatically find and manage security threats, while remaining invisible to adversaries.

Respond to threats in near real time

Utilize the power of AI and automation running directly on the endpoint to detect and block new and unknown ransomware variants.

Undetectable by design

Get deep visibility into the operating system from the outside, with live hypervisor-based monitoring while remaining invisible to malware.

Customizable threat hunting

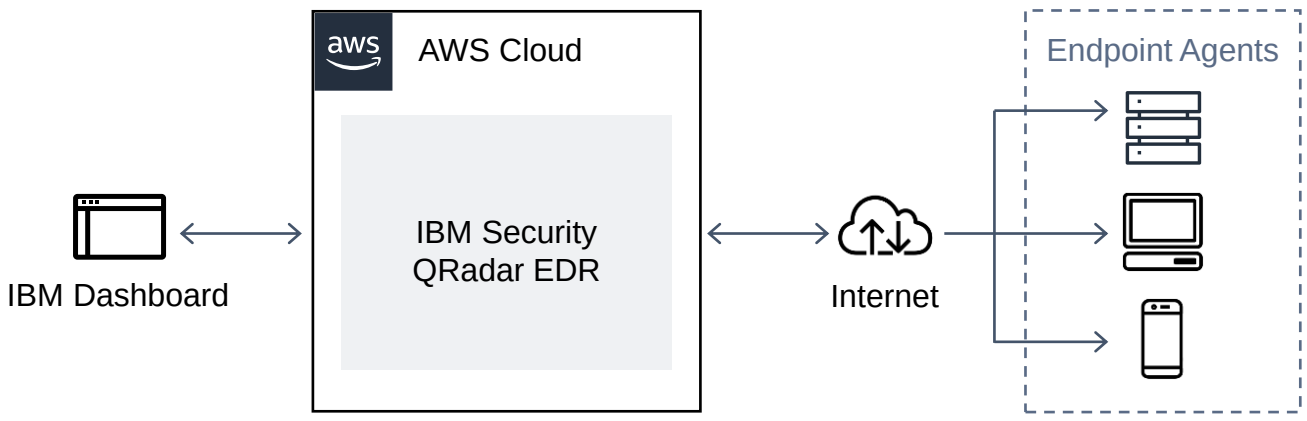
Design custom detection strategies that meet unique company-specific requirements while endpoints across the organization are updated quickly without interruption.

AI-powered learning and improvement

Reduce false positive with AI-powered threat detection that utilizes fully customizable telemetry for granular search and proprietary detection.

Contact IBM

IBM Security QRadar EDR on AWS



Case Study: Critical infrastructure operator

Challenges

A water management critical infrastructure operator was targeted by a ransomware attacker and assumed to be a contractor. After obtaining initial access, attackers managed to traverse the network and attempt to exfiltrate sensitive internal data about the facility.

Solution

IBM Security QRadar EDR on AWS was deployed on all servers and endpoints, allowing NanoOS to get full visibility over the attackers' movements. An alert was raised with the security team, who then activated the eradication plan and remediation module. The segment was cleaned up in seconds.

Results

A threat hunting session identified every machine that was accessed and obtained all the attackers' tools. All credentials were immediately reset for all users, and a new security policy was propagated across the entire infrastructure. There was no loss of data or interruption of services.

Features

Undetectable by Design

Gain deep visibility into the applications and processes running on an endpoint with NanoOS, which exists outside of the operating system and is designed to remain invisible to aggressors.

Customized Threat Hunting

Employ customized detection strategies designed to address your unique company-specific requirements.

Reduce False Positives

The AI-powered Cyber Assistant is a one-shot learning system that can reduce false positives by more than 90%.

Visit AWS Marketplace or IBM.com to purchase.

Get started with IBM Security solutions on AWS

Contact IBM

aws PARTNER Premier Tier Services

- L1 MSSP Services Competency
- Security Services Competency
- Security Software Competency