



MANAGED DATA DETECTION AND RESPONSE (MDDR)

24x7x365 protection for your most critical asset: *your data*.

CHALLENGE

Companies pay millions for threat detection products and services, yet when an incident occurs, they struggle to answer the most important question, "Was this a material data breach?" Data blindness is why organizations with advanced security stacks can fall victim to breaches from insider threats and attackers that bypass endpoint and network controls, targeting data at the source.

SOLUTION

Varonis Managed Data Detection and Response (MDDR) is the world's first managed service for monitoring and protecting critical data with a 24x7x365 SLA. MDDR combines Varonis' industry-leading threat detection technology with a world-class team of elite threat hunters, forensics analysts, and incident responders. Our team triages, investigates, and responds to every Varonis alert, so you don't have to.

KEY BENEFITS

Up and running **in hours**, not days or weeks

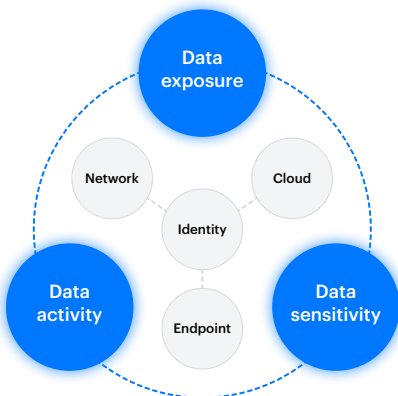
24x7 communication

Dedicated data security expert

Covers data in the **cloud and on-premises**

Data-Centric Telemetry

Unique, hard-to-get ingredients to uncover threats to data others miss.



AI-Powered Threat Detection

We understand normal and abnormal data access for each user and device.



AI / Machine Learning

Behavior-based threat models

Real-time alerts

Automated analysis & response

24x7x365 MDDR

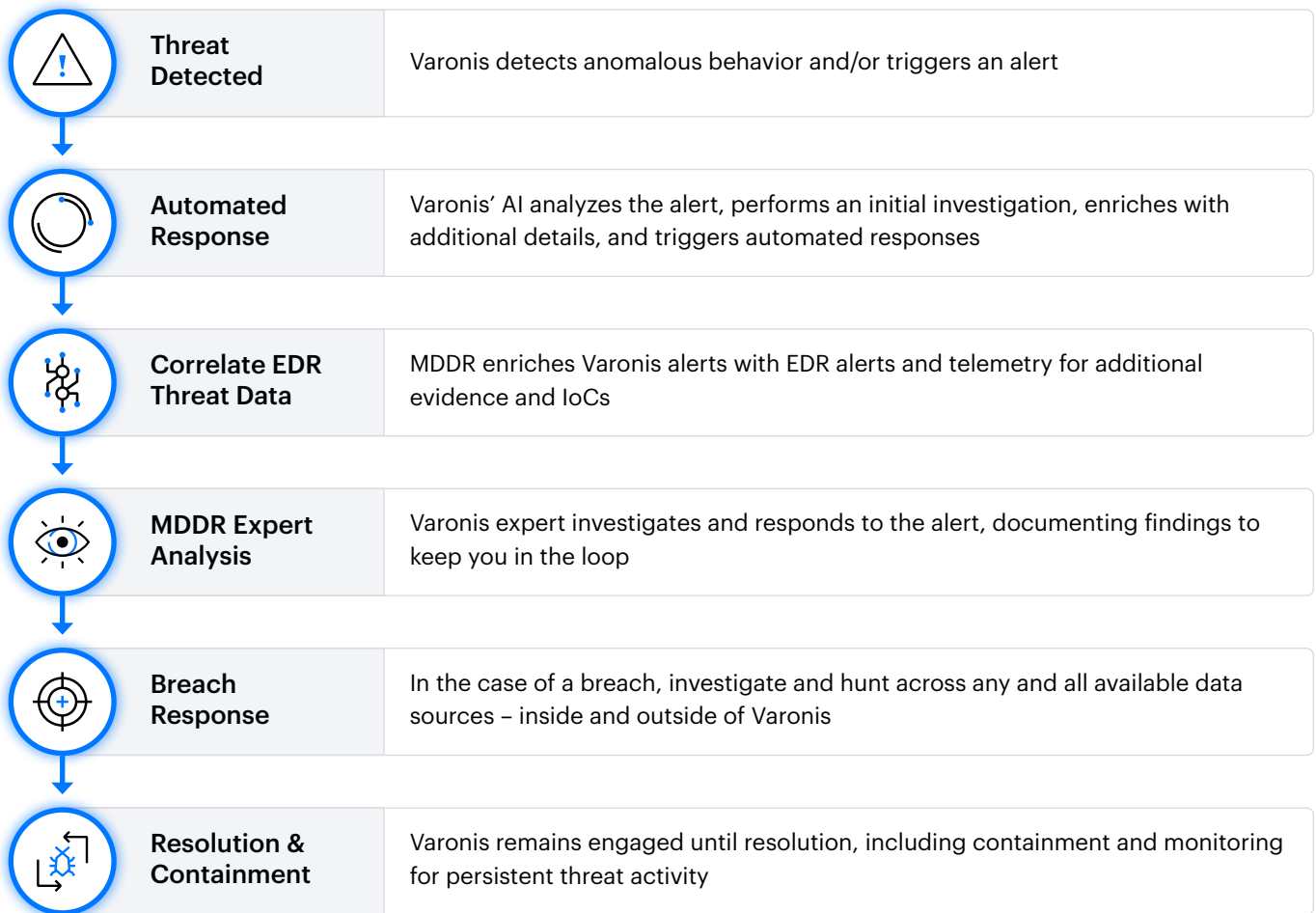
Our experts monitor and respond to alerts so you don't have to.

- ✓ Dedicated security expert
- ✓ Industry best SLA
- ✓ 24x7 communication
- ✓ Proactive hunting
- ✓ Incident response
- ✓ Threat intelligence
- ✓ Security posture assessments

Varonis Managed Data Detection & Response

Varonis MDDR combines world-class incident response, breach response, and threat intelligence. Our global team of elite cybersecurity experts solves the challenge of protecting sensitive data without the complexity and overhead of building your own 24x7x365 operation. We'll seamlessly integrate with your team and escalate incidents only when needed.

How MDDR works



“The investment we’ve made in Varonis has been immeasurable in finding and stopping cyberattacks. The Varonis team proactively reaches out to me with true incidents, rather than just surfacing more alerts for my team to manage.”

SCOTT MERCER

Director, Cybersecurity and Technical Services, KU Endowment

24x7x365 Incident Response

MDDR delivers 24x7x365 incident response and threat detection with AI-driven analytics and expert threat hunters, ensuring rapid containment, breach support, and unmatched visibility into data-centric threats – backed by the research of the Varonis Threat Lab.

Ransomware activity detected

- Abnormal behavior: Activity from new geolocation to the organization
- Abnormal behavior: An unusual amount of data was uploaded
- Kerberos delegation to a user identified

My Varonis security expert

"We've triggered a response and are investigating."

Industry-best SLA

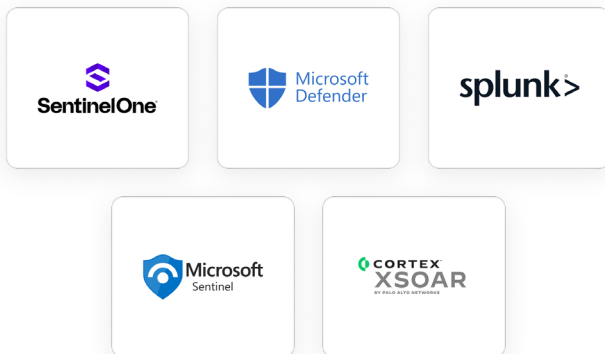
Varonis MDDR offers an industry-best 30-minute guarantee to investigate ransomware attacks and a 120-minute guarantee for all other alert investigations. MDDR also includes proactive threat hunting and regular security posture assessments to ensure your data security is always improving.

Agentic AI-enhanced response

MDDR is powered by Varonis' proprietary data insights and an AI analysis engine that automates investigations. Critical alerts are sent to Varonis' expert team for further investigation and mitigation.

Alert Received

- What is the **time frame**?
- Who is the **alerting account**?
- Where has the account **operated from**?
- What are the **impacted files**?



End-to-end threat detection

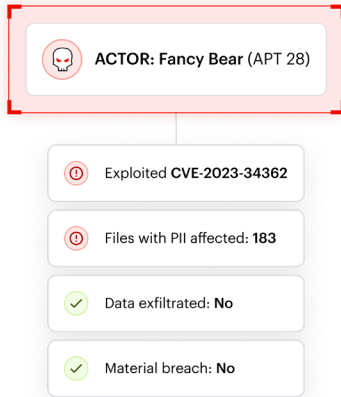
Integrate EDR with MDDR for faster investigations, earlier threat detection, and proactive responses, like endpoint quarantining. Varonis also integrates with leading SIEM and SOAR vendors to centralize alert management and automate remediation.

KEY FEATURES

- + 24x7x365 threat detection & incident response
- + Industry-best 30-minute SLA on ransomware
- + Agentic AI-enhanced threat response
- + Integrates with EDR, SIEM, and SOAR

World-Class Breach Response

In the event of a security incident or breach, Varonis' MDDR team provides hands-on response services, including the collection of critical evidence, subsequent analysis, and in-depth reporting to help your team contain and evict advanced threats. Our forensic team remains engaged until your business objectives are successfully met— no matter the depth or scope, offering a level of DFIR service comparable to high-cost retainer-based solutions

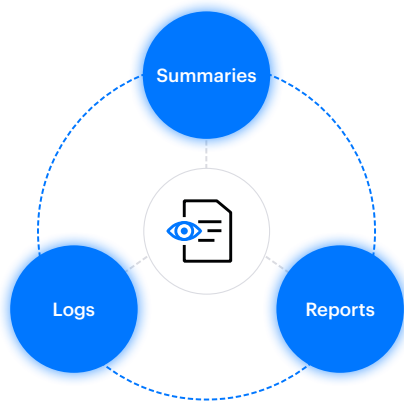
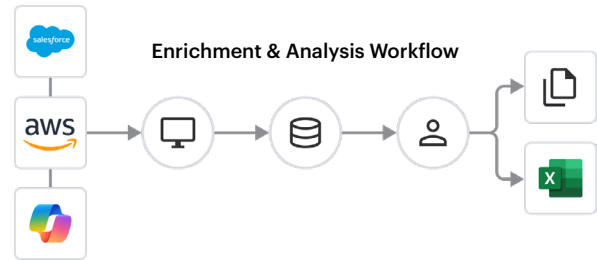


Comprehensive breach response

Varonis MDDR delivers comprehensive breach investigations to scope and identify compromised devices and users across cloud, SaaS, on-prem, and hybrid environments. Leveraging all available internal and external data sources, our team conducts deep threat hunts to eliminate blind spots and ensure complete visibility. No data source is outside of scope – inside or outside the Varonis platform.

Full spectrum of investigative tools

To aid investigations, Varonis MDDR leverages a full suite of tools, including EDR, SIEM, SOAR, and cloud platforms such as Microsoft 365, Azure, Google Cloud, Google Workspace, and AWS. Custom triage agents collect endpoint forensic data and logs from firewalls, DNS, DHCP, bespoke systems, and third-party applications, which are analyzed to guide threat response strategies.



Continuous reporting and communication

MDDR keeps stakeholders informed at every step of the investigation. Customers are given clear documentation, breach impact analysis, and proactive communication— ensuring transparency, accountability, and confidence throughout the entire breach response lifecycle.

KEY FEATURES

- + Dedicated team of security experts
- + No retainer or hourly fees
- + Remain engaged until objectives are met
- + Custom tools for evidence collection/analysis
- + No data source out of scope