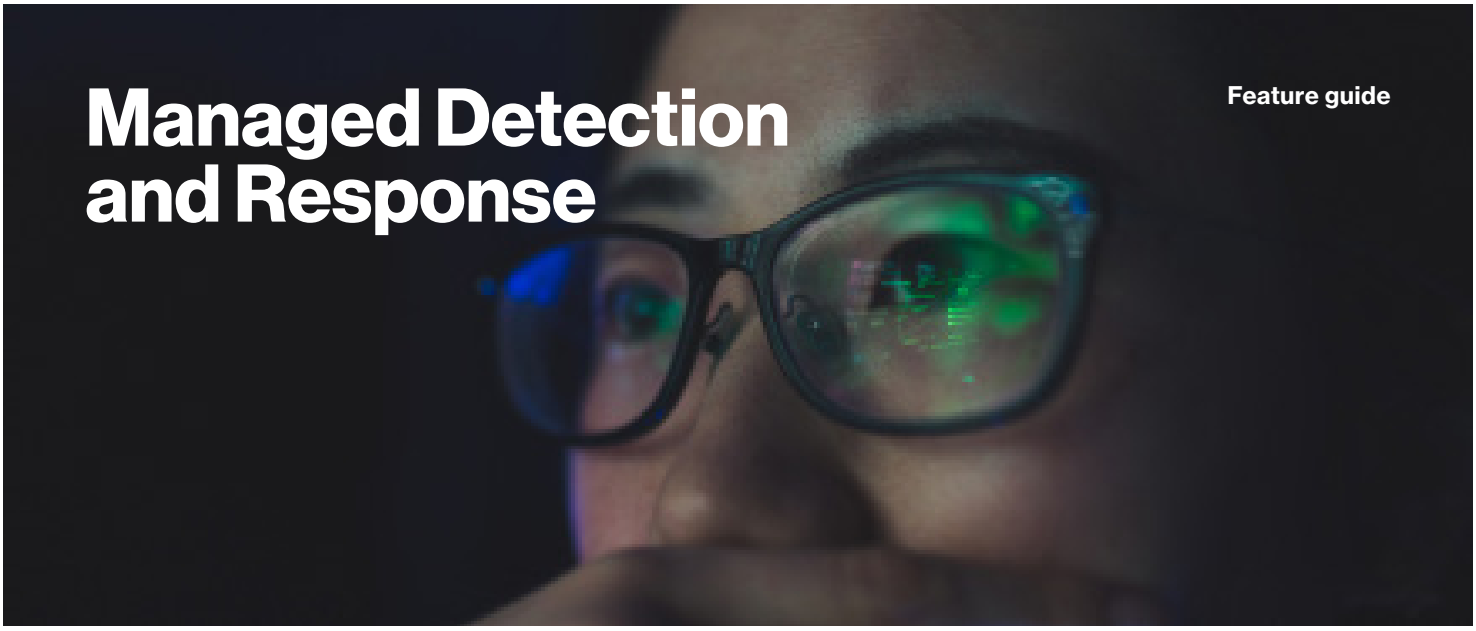
Managed Detection and Response

Feature guide



Verizon Managed Detection and Response (MDR) is a managed security solution that combines Verizon's people, process and technology in one solution. It's continually tuned to your unique requirements, reduces the need to hire and retain security talent, and enables more rapid detection and response, 24/7.

What does Managed Detection and Response include?

Detection and response capabilities

- Continuous (24/7/365) alert monitoring by expert Security Operations Center (SOC) analysts.
- Full incident validation.
- Containment and disruption (using your endpoint detection and response [EDR] tools).
- Remote incident response transition to your incident response team.
- Analysts and platform that can support market-leading EDR tools.
- Support for custom playbooks.

Threat hunting and threat intelligence

- Manual, monthly threat hunting to find malicious or potentially harmful activity in your IT environment.
- Market-leading threat intelligence powered by Verizon Threat Research Advisory Center (VTRAC) and third-party providers, including Recorded Future.
- Basic dark web monitoring and alerts.
- Custom threat modeling.

Service delivery

- Designated Client Security Engineer (CSE) and named Security Services Advisor (SSA) to enable routine fine-tuning and management of the MDR service components, day-to-day service delivery and management reporting.
- CSE-led discussions about specific alerts and reports, guidance on the impact of threat hunt findings and next steps for remediation.
- Dedicated access (fixed number of hours based on your package) to CSE for understanding and making use of other Verizon security products. This can help you improve your organization's security posture and provides you with guidance on the decision process when considering new security tools.
- Support behind the scenes during board or executive briefings, with reporting.
- Additional CSE time (can be purchased in five-hour blocks).
- Additional SSA time (can be purchased in five-hour blocks).

All the above requests and deliverables will be addressed by the CSE within your allocated time, which will be defined by the package and tier you purchase.

verizon

Implementation and setup

- Setup, implementation requirements gathering and deployment project plan.
- Technology setup, configuration and deployment assistance.
- Named SSA as your team's point of contact for implementation and setup.

Telemetry

- Advanced threat detections via cloud-based security information and event management (SIEM) engine to identify attackers and their tactics, techniques and procedures (TTPs).
- Proactive human-powered threat hunting services that can help find breaches that threat detection technology alone cannot identify.
- User and Entity Behavioral Analytic (UEBA) detections to identify anomalous user activity based on market-leading analytics engine.
- Support for Verizon Network Detection and Response (NDR; sold separately) to analyze and detect incidents based on full-packet capture.*
- Support for Acalvio® ShadowPlex® deception technology (sold separately) to detect attackers earlier in the attack chain and detect lateral movement.*
- Support for endpoint detections from market-leading EDR tools (sold separately), including data intake, alerting on incidents and manual response using the EDR's built-in capabilities.**

Reporting

- Monthly findings reports with tailored remediation guidance and recommendations.
- Monthly threat intel summary reports.
- Threat-hunting reports.
- State-of-the-art reporting from market-leading SIEM tool.
- Quarterly service reviews.

Technology

- Cloud-delivered SIEM (up to subscription levels).
- Customer portal protected by two-factor. authentication.
- Self-service centralized log management and search (30 days hot, 90 days warm, 365 days cold storage).
- During the first 90 days, logs can be searched and exported from the customer portal based on search queries. (Export limit of 10,000 records downloaded at one time).
- Offline or inactive data collected by Verizon MDR can be accessed upon request for up to 365 calendar days on a rolling basis.
- Cold-store data can be retrieved within seven days of a request through the customer portal or via CSE and is limited to two requests of up to 10 terabytes of data per year.
- DIY automated endpoint and user containment response actions are flexible.

verizon

* Full integrations planned for 1H 2022.
**Full integration planned for Q4 2021.

What is not included in Verizon Managed Detection and Response?

The following technologies require a separate license from Verizon:

- EDR licenses (if required)
- Deception licenses (if required)
- NDR licenses (if required)

Does Verizon provide a product demo?

Yes. The Verizon Solutions Architect team can be engaged to provide a product demo.

Is there a demo portal the customer can access to experience the technology?

Yes. The Verizon Solutions Architect team can be engaged to provide you with access to a demo portal for your use on demand.

Where will the CSEs, SSAs and SOC teams be located?

We aim to provide an SSA or a CSE in your local region, but the CSE may be globally located. SOC teams that provide triage, investigation and response are located globally and are not in-region, operating under a 24/7, follow-the-sun model.

Learn more:

For additional information or to ask a question, schedule time with a Verizon Solutions Architect by contacting your Verizon Business Account Manager.

verizon