Managed Detection & Response (MDR)

Powered by Rapid7

Comprehensive, managed security solution that helps safeguard data and businesses from evolving cyber threats.

Solving Cybersecurity Challenges

Today's threats can happen anywhere across your IT stack, including applications and databases, email and endpoints, cloud and server infrastructure, identity, users, and the network.

In fact, over **90% of data breaches like ransomware start with initial access via phishing or stolen credentials**[1]**.** Once landed, adversaries can move laterally inside your network to exploit vulnerabilities and compromise systems.

That's why it's important to monitor the entire IT environment around the clock with a managed detection and response solution like Comcast Business MDR that can detect malicious behavior across IT assets and users.

Many companies not only need to defend themselves against data breach but must also comply with cybersecurity regulations, meet cyber insurance requirements, and provide security auditors with detailed reports.

According to Gartner®, by 2026, organizations prioritizing their security investments based on a continuous threat exposure management program will realize a two-thirds reduction in breaches.[2]

Today's cyber threats can be relentless:

It's important to monitor, detect, and respond around the clock.

Comcast Business MDR solves the challenge of cybersecurity detection and response.

1. Comcast Cybersecurity Threat Report
2. Gartner, Top Trends in Cybersecurity for 2024, By Richard Addiscott, Jeremy D'Hoinne et al., 2 January 2024. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

COMCAST BUSINESS

Solution Overview

Coupled with a suite of monitoring, response, and threat hunting services by our trained Security Operations Center (SOC) analysts, Comcast Business MDR makes it easy and affordable to use an industry-leading Extended Detection and Response (XDR) cloud platform for threat detection, security orchestration, reporting, and vulnerability management.

With advanced security telemetry, global threat intelligence, and 24x7x365 remote SOC services, Comcast Business MDR helps detect and disrupt cyber threats and vulnerabilities.

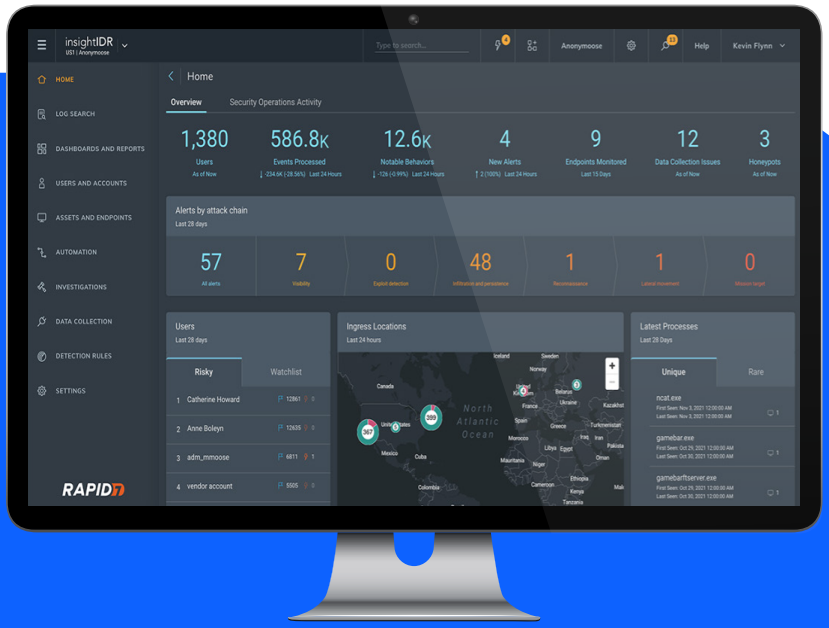

Figure 1: Platform Home Overview

Our solution helps your security and IT teams extend their capabilities across a spectrum of critical cybersecurity responsibilities, enabling them to focus on core business priorities. Comcast Business MDR provides an end-to-end service with the insights and technology to help protect against advanced threats, while our SOC works collaboratively with you as we respond to threats on your behalf.

Out of the Box Security Framework Reports to help satisfy compliance requirements, such as Payment Card Industry Data Security Standard (PCI DSS).

Trained MDR analysts monitor and triage critical detections across your IT environment.

A web console provides full visibility of MDR investigations, evidence, and reports.

COMCAST BUSINESS

MDR Services

With Comcast Business MDR, you get 24x7 threat monitoring, detection, response, and support from the Comcast Business Security Operations Center. Our commercial SOC is staffed by trained and certified security analysts who collaborate with you using the MDR platform and features.

A dedicated cybersecurity Customer Project Manager (CPM) will guide you through a short installation and deployment. If you want to review MDR security performance reports and recommendations, a Customer Service Manager (CSM) will meet with you monthly or quarterly.

You can request that our SOC respond proactively to contain or disrupt critical security threats when detected in your systems. Other MDR services include custom detection rules, custom Security Orchestration, Automation, and Response (SOAR) automations, threat hunting, threat intelligence advisories, and periodic rule tuning to reduce false positive detections.

How is Comcast MDR Different?

Unlike managed security solutions that simply provide alerts to companies, Comcast Business MDR actively responds across applications, endpoints, cloud, identity, network, and user behavior using a cloud Security Information and Event Management (SIEM) tool, dashboards and reporting, a threat investigation console, curated detection rules, and fully managed 24x7 SOC services.

With Comcast Business MDR, you benefit from:

- Affordable tiered pricing based on endpoint assets, not storage or log ingest volume.
- Integration with other Comcast cyber solutions, including managed UTM firewalls, Endpoint Detection & Response (EDR), and Secure Remote Access VPN services for automated, fast, and seamless active threat response.
- Enhanced custom detections and automated SOC response using Comcast Business Threat Intelligence, as well as customized automation designed to fit your business needs.
- Comcast Business-managed User and Entity Behavior Analytics (UEBA) Detections powered by Rapid7 machine learning.
- Managed custom and user behavior notifications to help reduce false positives and alert fatigue.

MDR Services:

- 24x7x365 Support
- Monitoring, Investigation and Response
- Notifications
- Installation Project Manager
- Customer Service Manager
- Optional Dedicated SOC Team
- Security Review and Collaboration
- Threat Hunting
- Threat Intelligence Advisories
- Custom Detection Rules
- Custom Automations
- Custom Log Ingest
- Tuning and Exclusions

Some services may incur add-on charges depending on the MDR version ordered.

COMCAST BUSINESS

XDR Platform

Comcast Business has partnered with Rapid7 to use their Insight platform for detection and response (InsightIDR), security orchestration and automation (InsightConnect), and vulnerability management (InsightVM).

Rapid7's InsightIDR is your security center for incident detection and response, authentication monitoring, and endpoint visibility. Together, these form Extended Detection and Response (XDR). InsightIDR identifies unauthorized access from external and internal threats and highlights suspicious activity, so you don't have to weed through thousands of data streams.

XDR accelerates more comprehensive threat detection and response. This cloud-native, scalable cybersecurity SIEM can unify and transform multiple cyber data telemetry sources.

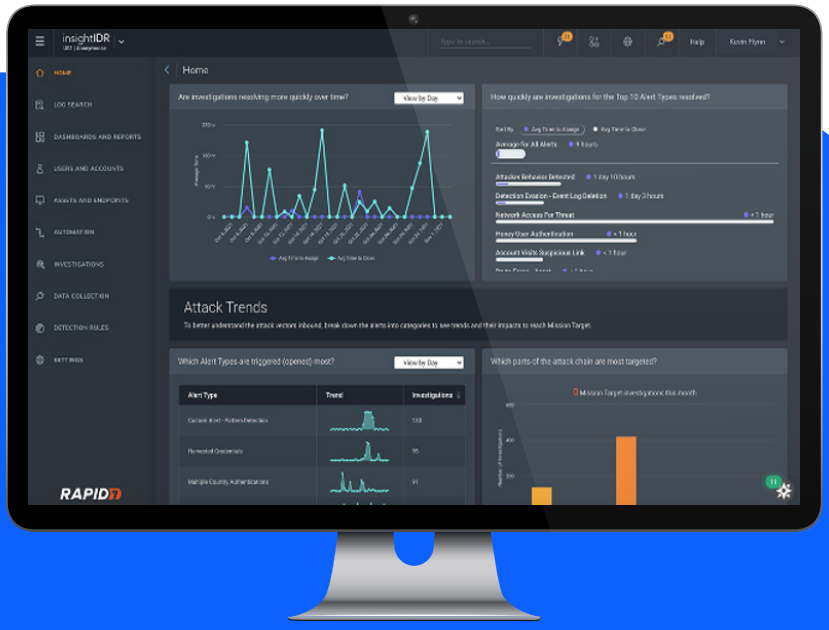

Figure 2: Attack Trends and Service KPIs

Email alerts, ticketing, and Slack integration give you timely notification of critical investigations.

Pre-built dashboards and scheduled reports.

"By year-end 2028, XDR will be deployed in 30% of end-user organizations to reduce the number of security vendors they have in place, up from less than 5% today." [3]

3. Gartner, Market Guide for Extended Detection and Response, By Thomas Lintemuth, Peter Firstbrook, Ayelet Heyman, Craig Lawson, Jeremy D'Hoinne, 17 August 2023

COMCAST BUSINESS

Feature Details

Dashboards and Reporting	Access pre-built dashboards and reports out-of-the-box or create your own custom ones to best suit your organization's needs.
SIEM, Log Management and Search	Analyze the complex data and find insights faster with a cloud-native data lake, diverse log collection capabilities, custom log parsing, and flexible search and reporting.
Investigation Console and Notifications	View your aggregated alert data in an investigations console to quickly search your active investigations and gather the context you need to effectively prioritize, sort, and respond to alerts.
Endpoint Detection & Response (EDR)	Identify and prioritize risk with endpoint detections powered by the critical data collected via the Insight Agent from endpoints across your environment.
File Integrity Monitoring (FIM)	Collect File Integrity Monitoring events with the Insight Agent so InsightIDR can attribute users to file modification activity. You can then create alerts based on certain file log events to notify you when one of your users modifies a critical file or folder.
Network Traffic Monitoring and IDS	Monitor for malicious activity and policy violations on your network with an Intrusion Detection System (IDS) device and packet-based traffic monitoring.
Curated Threat Detections Library	Leverage curated threat detections managed by Comcast Business and Rapid7's threat intelligence teams. Comcast Business MDR offers you wide threat coverage across your environment by capitalizing on our open-source community engagement, spanning known and unknown threats, and utilizing advanced attack surface mapping and proprietary machine learning.
Attacker Behavior Analytics (ABA)	Hunt for unique attacker behavior with ABA detection rules. With our ever-growing detection library, you'll be covered against even the newest of threats.
User and Entity Behavior Analytics (UEBA)	Identify compromised credentials, lateral movement, and other malicious behaviors with User Behavior Analytics detections.
Deception Technology	Deploy deception technology in the form of honeypots, honey files, honey users, and honey credentials to learn how attackers are accessing your systems.
Enhanced Endpoint Telemetry	Unlock comprehensive attack details, proactively hunt for threats, and tailor custom alerts to align your specific security policies and standards with Enhanced Endpoint Telemetry.
Enhanced Network Traffic Analysis	Access raw network flow data and rich metadata collected by the Insight Network Sensor with Enhanced Network Traffic Analysis. This metadata includes IP addresses, ports, content-based application recognition, and metadata attributed to specific users and devices.
SOAR Automation	Respond quickly and confidently with automated out-of-the-box workflows, including endpoint containment, Insight Agent containment, and more. Enable custom orchestration with a full-featured SOAR.

COMCAST BUSINESS

Vulnerability Management

Security vulnerabilities allow attackers to compromise hardware or software and then access confidential information.

Vulnerability Management is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them. This, implemented alongside other security tactics, is vital for organizations to prioritize possible threats and to minimize their "attack surface."

Vulnerability scanning needs to be performed continuously to keep up with new systems being added to networks, changes that are made to systems, and the discovery of new vulnerabilities over time.

- **Discover and prioritize active vulnerabilities**
  Gain visibility into your IT assets. Continually assess and prioritize critical vulnerabilities for remediation.
- **Assist with remediation with tracking and collaboration**
  Help IT better understand risks. Assist with remediation with automation and track progress with dashboards and reports.
- **Access to dashboards and reporting to help stay compliant**
  Our pre-built dashboards and custom reports help you access the data required to navigate the complexities of regulatory requirements.
- **Leverage expert research and community insights**
  Use intelligence from Rapid7 Labs to identify Internet-facing assets and better prioritize vulnerabilities.

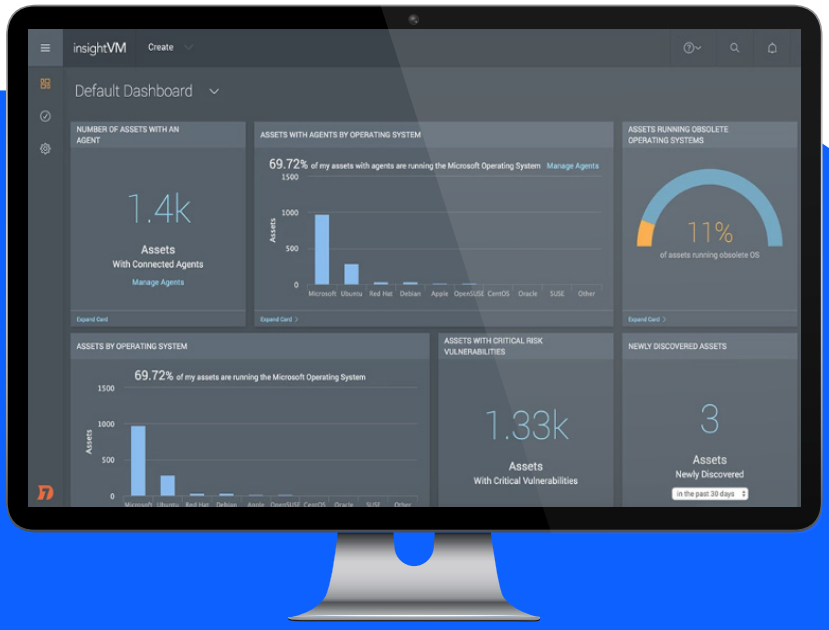

Figure 3: Integrated Vulnerability Management

"By 2025, 60% of organizations will be actively using remote threat disruption and containment capabilities delivered directly by MDR providers, up from 30% today."[4]

Over 250,000 new application and infrastructure vulnerabilities are discovered yearly.[5]

InsightVM from Rapid7 includes a library of vulnerability research, Nexpose and Metasploit exploit and attacker behavior knowledge, Internet-wide scanning data, exposure analytics, and real-time reporting.

4. Gartner, Market Guide for Extended Detection and Response, By Thomas Lintemuth, Peter Firstbrook, Ayelet Heyman, Craig Lawson, Jeremy D'Hoinne, 17 August 2023.
5. NIST National Vulnerability Database

COMCAST BUSINESS

Vulnerability Features

Integrated Endpoint Agent and Network Scans	The same Rapid7 Insight Agent used for MDR detection also automatically collects vulnerability data from your endpoints, even those from remote workers and assets that cannot be actively scanned, or that rarely join the corporate network.
Live Dashboards	Most vulnerability scanning dashboards are static: a snapshot of a particular time. InsightVM Live Dashboards are real-time and interactive by nature. You can easily create custom cards and full dashboards for anyone – from system admins to CISOs – and query each card with simple language to track progress of your security program.
Active Risk Score	CVSS-based risk scores can result in thousands of "critical" vulnerabilities, making it very difficult for security teams to prioritize vulnerabilities with the most efficient risk reduction. With Active Risk, security teams can prioritize vulnerabilities on a 1-1000 scale indicating those that are actively being exploited in the wild or the likelihood of an attacker exploiting the vulnerability in a real attack.
IT-Integrated Remediation Projects	With Remediation Projects, security teams can assign and track remediation duties in real-time, providing continuous visibility into how issues are being remediated. Take it one step further by integrating InsightVM directly with IT ticketing systems to fold remediation seamlessly into daily workload.

Cloud Detection & Response

Monitoring and detecting threats in dynamic cloud environments is challenging. Raw cloud logs lack sufficient context to properly investigate and triage cloud security events, and there is a lack of coordinated tools and resources. It's critical to have visibility into cloud infrastructure misconfiguration since these lead to many data breaches today.

There are three key categories of logs to consider when investigating cloud-related alerts:

1. Behavior across activity and access logs.
2. Network flow, DNS, firewall, and load balancer logs.
3. Resource-specific server, storage, database, and serverless compute.

Comcast Business MDR can address these needs.

COMCAST BUSINESS

How it Works

Many organizations today have diverse IT environments, including cloud and SaaS infrastructure. Your MDR solution needs to contain and disrupt threats wherever they may land across the full IT stack. Companies deploy endpoint agents and a log collector that forwards telemetry from multiple security data sources to a security data lake.

Data ingest can include applications, endpoints, cloud infrastructure, custom data sources, identity, network, and users. The cloud platform then normalizes security data formatting, enriches it with threat intelligence, and uses machine learning and thousands of detection rules to correlate and identify threats.

Security Detection & Response

Comcast Business MDR takes a comprehensive, holistic approach to security detection and response. Curated detection rules, global threat intelligence, and machine learning create a powerful detection engine. Optional components include a network sensor, deception honeypots, and vulnerability management. The platform delivers integrated visibility and analytics to correlate and contextualize security threats.

©2024 Comcast. CB-MDR-Solution-Product-Brief_6.24

COMCAST BUSINESS