Endpoint Detection & Response

Scalable, turnkey device security for mid-to-large enterprises

Endpoints remain the most common attack surface for ransomware and other malware attacks. Users continue to make critical mistakes with web, email, and other applications, resulting in security compromises.

Application and operating system vulnerabilities continue to proliferate endpoint devices and are challenging to identify and patch. Remote and mobile workers increase this risk as they are not behind corporate next-generation firewalls (NGFWs). This risk is greatly increased when organizations lack broader security controls and best practices as part of an in-depth defense strategy.

Endpoint security (anti-virus) remains critical as part of a first line of defense, but commonly fails because it cannot detect innovative or previously unseen attacks, and may lack real-time response capabilities to actively contain or mitigate ongoing attacks. Without it, compromised endpoints can become “beachheads” for the attacker to pivot and target high-value assets like file servers, databases and applications.

Endpoint Detection and Response (EDR) technology, with its integrated operating system level agent, can be highly effective at:

- Detecting, visualizing and contextualizing advanced Tactics, Techniques and Procedures (“TTPs”) attackers are using on the endpoint.
- Helping understand what is happening on the endpoint, including attacker progression and objectives, as well as root cause analysis.
- Intervening the attacker’s “Cyber Kill Chain” by leveraging the EDR agent’s integrated controls to mitigate attacker activity and determine root-cause.

However, EDR is an intensely interactive tool designed for highly skilled security analysts that understand how to leverage the technology to achieve optimal security outcomes. **Most enterprises simply do not have the security expertise and 24/7 resources to make an EDR deployment effective**. With Comcast Business EDR, we make it easy and affordable to help protect your enterprise with cybersecurity professionals working 24/7 for you in our security operations centers (SOCs).

50%

Reduction

in serious incidents for organizations using EDR

Source: Nemertes

1. Gartner, Endpoint Detection & Response; Architecture, Implementation and Operations Practices.

COMCAST BUSINESS

Fully Managed EDR Service Delivers Cost-Effective Ransomware and Advanced Malware Mitigation for Resource Constrained Enterprises

Comcast Business EDR is a **turnkey fully managed** service that enables security- and resource-constrained organizations to deploy an **effective EDR**. Our cloud-based EDR solution deploys quickly with **fast time-to-value while liberating in-house IT teams** to help improve productivity. Plus, our expert EDR analysts strive to align directly with your organization to understand and prioritize business and risk management objectives, while our 24/7 SOC quickly triages endpoint incidents and responds effectively with mitigation to help reduce business disruption and improve outcomes. Additionally, we provide customized Threat Intelligence services for improved effectiveness across different industry vertical threat landscapes. Optional Threat Hunting services are available for organizations with demanding risk posture objectives.

Confidently support your IT-driven business objectives with effective ransomware mitigation in place

Features & Benefits

Every effective EDR program depends on an optimal balance of security expertise, mature security processes and cost-effective technology. Comcast Business is an ideal partner for mid-to-large enterprises to deliver EDR due to our security expertise and effective processes at scale, along with our strong partnerships with leading technology providers. Plus, strong synergies of managed EDR integrations with our SD-WAN solutions can provide enhanced mitigative actions including firewall blocking.

Solutions to help liberate your IT teams

Our cloud-deployed EDR service can be up and running quickly. Plus, our SOC assists with recommended EDR agent deployment practices through common desktop management tools and provides ongoing administration.

Expert security support

Our EDR SOC analysts work with you to understand your business objectives and how those align with your risk prioritization. We strive to offer white glove security support as well as calls with our SOC to:

- Review and update business priorities.
- Track SOC performance and adjust processes and playbooks as needed.
- Update customer on latest threat intelligence and threat actor trends for any pre-emptive mitigation.

Effective mitigation and rapid incident response

Our advanced EDR technology platform identifies suspicious endpoint behavior which is then promptly assessed and triaged by our EDR analysts 24/7. Decisive action can be taken on your behalf, with escalations to your team on a need-to-do basis (as per customer-specific incident response plan). All incident and response actions will be documented and logged as per your organization's requirements.

Threat Hunting Services for proactive defense

We offer optional Threat Hunting Services for enterprises that need a proactive defensive posture against advanced attacks. Our Threat Hunting EDR analysts coordinate with Threat Intelligence analysts for effective search and destroy missions on early detected attacks. Plus, our analysts offer post-hunting consultations with your team to provide recommended configuration changes for additional infrastructure hardening.

COMCAST BUSINESS

Product Features	Business Benefits
Storyline feature with instant visibility	Helps provide a view of the business' threat life cycle in the customers IT environment
One-click remediation and rollback	Helps provide quicker mitigation to help return to normal operating posture
Provides machine speed threat detection powered by AI	Comprehensive and resilient threat detection to help maximize EDR service effectiveness
Extended data retention	Helps enable compliance requirements and retrospective Threat Hunting to help improve risk posture
Automatic blind-spot coverage	Help increase visibility for faster incident response

Comprehensive, integrated SD-WAN and Managed Security Services

Integrating EDR with SD-WAN enhances the overall cybersecurity posture of an organization. It strengthens the organization's cybersecurity defenses, helps respond rapidly to threats, and creates a more resilient and efficient network infrastructure.

Enhanced Threat Detection and Response

Combining EDR and SD-WAN allows for real-time monitoring and analysis of endpoint and network activities. By correlating data from endpoints and the network, security teams gain greater visibility into potential threats and can respond more quickly and accurately to security incidents.

Improved Incident Investigation

EDR and SD-WAN integration provides a deeper view of security incidents, allowing security analysts to investigate incidents more efficiently. With contextual information from both EDR and SD-WAN, analysts can understand the full scope of an incident, including its impact on endpoints and the network.

Proactive Threat Hunting

The combination of EDR and SD-WAN data empowers security teams to conduct proactive threat hunting. By analyzing endpoint and network behavior, they can identify potential threats before they escalate, reducing the likelihood of successful attacks.

Cybersecurity Framework

Endpoint Protection

Identify:

- Operating System and application vulnerabilities
- Endpoint misconfigurations

Protect:

- Remote traffic with strong authentication and encryption
- Prevent/control split tunneling
- Against advanced malware
- Against risky and malicious website and application traffic
- Unauthorized data transfer on Removable Media

Managed Endpoint Detection & Response

Detect:

- Endpoint security protection failures
- Unknown or suspicious processes and other attacker endpoint malicious activities

Respond:

- Mitigate suspicious endpoint processes and activities
- Quarantine infected endpoints for remediation

Recover:

- File roll-back to recover corrupted/encrypted files
- Expert 24/7 EDR analyst support for incident response and mitigation

Our EDR Offerings

Explore our two offerings that can help protect your business from malware.

	OPTIONS	
Capabilities	EDR Standard	EDR Advanced
Guided Install	●	●
24/7 SOC	●	●
Automated Response	●	●
0-day Data Retention	●	●
Advanced Features		
Custom Detection Rules		●
Threat Hunting		●
Extended Data Retention		●
Extended Data Retention Longer Duration (30, 90, 180 and 365 Days)		●

COMCAST BUSINESS

Supported Platforms and Features

Platforms that integrate with our EDR solutions to help secure your endpoint devices.

	OPTIONS	
Platforms	EDR Standard	EDR Advanced
Windows		
Windows Server Core: 2022, 2019, 2016, 2012	●	●
Windows Server: 2022, 2019, 2016, 2012 R2, 2012, 2008 R2 SP1	●	●
Windows Storage Server: 2016, 2012 R2, 2012	●	●
Windows: 11, 10, 8.1, 8, 7 SP1+ / 10 IoT Enterprise	●	●
Windows “Legacy”: XP SP3+, 2003, 2008	●	●
Windows Server 2003 SP2 or later, or R2 SP2 or later	●	●
Windows Embedded POSReady 2009	●	●
Mac OS		
macOS Ventura	●	●
macOS Monterey	●	●
macOS Big Sur	●	●
Linux		
Ubuntu 14.04, 16.04, 18.04, 19.04, 19.10, 20.04, 22.04	●	●
RHEL 6.4+, 7.0-7.9, 8.0-8.7, 9.0, 9.1	●	●
CentOS 6.4+, 7.0-7.9, 8.0-8.4	●	●
Oracle 6.9, 6.10, 7.0-7.9, 8.0-8.7, 9.0	●	●
Amazon Linux 2, AMI 2018, AMI 2017	●	●
SUSE Linux Enterprise Server 12.x, 15.x	●	●
Fedora 25-30, 31 (kernel 5.5+) 32-36	●	●
Debian 8, 9, 10, 11	●	●

COMCAST BUSINESS