A Guide to Endpoint Security

COMCAST BUSINESS

Hybrid work has become business as usual for many companies, which has altered the calculus for enterprise security.

In this new model, IT leaders aim to provide workers with the proper tools and network access while maintaining adequate security requirements. And when it comes to securing the new network edge, more companies are turning to cybersecurity services like Endpoint Detection and Response (EDR) solutions.

What is Endpoint Security?

Endpoint security is the practice of securing user devices like desktops, laptops, servers and network devices from cyber attacks, including:

- Ransomware
- Vulnerability Exploits
- Email Phishing
- Drive-by Downloads
- Watering Holes

This practice includes endpoint security technology — often endpoint agents that are installed on the device — as well as security analyst expertise and 24/7 monitoring and response capabilities to make effective use of that technology.

WHAT YOU'LL LEARN:

- ✓ **The importance of endpoint security**
- ✓ **How EDR helps protect endpoints**
- ✓ **Why Comcast Business EDR is unique**

Why is Endpoint Security Important?

Endpoint security is critical for any enterprise because endpoints are the common entry point for attackers into the enterprise network, where – once landed – they can pivot and go after the valuable information targets, such as file servers, applications, and databases, which are their real objectives.

Endpoints are initial targets for attackers because they are operated by end users, who in spite of best efforts with cybersecurity awareness training, are human and will make mistakes with their device and IT system security. These mistakes include succumbing to phishing and social engineering attacks, installing unauthorized and often malicious applications and browser plugins, and visiting malicious websites that take advantage of browser vulnerabilities.

Endpoints are also prone to application and operating system vulnerabilities that continue to impact endpoint risk postures on a never-ending cycle of software vulnerability scan and patch. This means that endpoints offer a large and relatively easy attack surface for cyber attackers to target. Think of hackers and other criminals as waging a war against cybersecurity defenses, and endpoints are considered where attackers can land and pivot to go after the high value data assets that are typically their end objective. Therefore, it’s critical to defend these endpoints to deny a entry for the attackers.

What is Endpoint Detection and Response (EDR)?

Endpoint detection and response is relatively new to the cybersecurity industry. The popularity of EDR has grown amongst CIOs and CISOs within the past few years because it can help solve the key challenges of securing a network endpoint — the quickly finding and thwarting potential threats.

Detecting and responding to threats are crucial components of the National Institute of Standards and Technology (NIST) Cybersecurity Framework. As per the NIST Framework, prevention controls are not sufficient on their own. EDR can implement much needed detection and response capabilities for endpoint devices. It does this by leveraging a deeply integrated security agent that acts as a gatekeeper between the operating system and any malicious applications or activities.

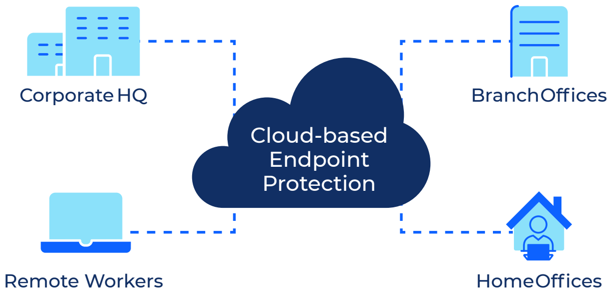
Identify	Protect	Detect	Respond	Recover
• Asset management • Business environment • Governance • Risk management strategy	• Access control • Awareness and training • Data security • Information protection and procedures • Maintenance • Protective technology	• Anomalies and events • Continuous security monitoring • Detection process	• Reponse planning • Communications • Analysis • Mitigation • Improvements	• Recovery planning • Process improvements • Communications

The EDR agent identifies, analyzes, and responds to operating system level activities that are indicative of malicious intent. Through either automated or analyst assessment, malicious activity can be blocked or otherwise mitigated before the attacker can compromise the device or user. Overall, it's a very effective endpoint defense strategy and technology because it does not rely on attack signatures or unique indicators of compromise, all of which can change quickly or be previously unseen.

However, EDR systems require sophisticated analyst skill and procedures to make the solution effective. Even with recent advances in artificial intelligence and machine learning, no 100% automated system can effectively determine which potential threats are real in the context of an enterprise network's daily operations. For that, a human cybersecurity analyst is needed but staffing that level of expert human capital on a 24/7 basis is often challenging for typical mid-sized enterprises to build in-house. In these situations, EDR is an appealing solution.

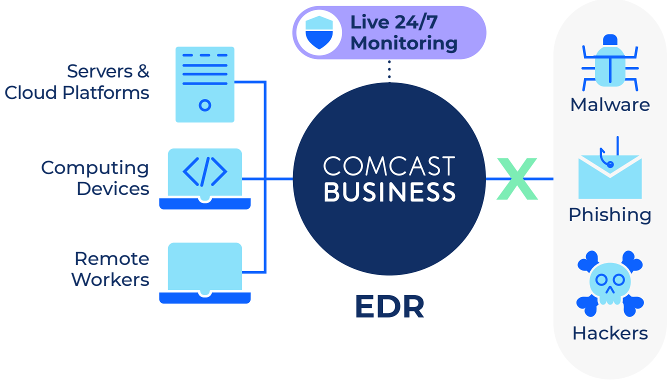
Why Choose Cloud-Based Endpoint Security?

Many security tools, including EDR, require a management server where EDR software agents report their activities and receive policy and command for endpoint security enforcement. Cloud-based endpoint security refers to the option where these management servers are hosted in the cloud (e.g. as a virtual machine in IaaS or a SaaS app), making deployment quicker and easier. With this approach, enterprises do not need to "stand up" their own management server before actually deploying agents.



What's Unique About Comcast Business Endpoint Detection & Response?

Comcast Business Endpoint Detection & Response (EDR) is a fully managed service delivering affordable turnkey ransomware, malware, and phishing security with industry-leading technology and proactive 24/7 security monitoring from highly-qualified security analysts. Our EDR solution empowers IT leaders with unified prevention, detection, and proactive response that scales with your business to cover network endpoints monitored by industry-certified analysts in security operations centers (SOCs) globally.



About Comcast Business

Comcast Business makes it simple for businesses of all sizes to deliver global secure networking solutions at scale, to help accelerate business impact and keep enterprises future-ready for what's next.

- The nation's largest converged IP broadband network
- Gigabit speeds that deliver lightning-fast bandwidth
- Physically diverse network from telcos
- Extensive on-premise and cloud-based options offering end-to-end secure network solutions