COMCAST BUSINESS | MASERGY

Endpoint detection & response

How to compare technologies and services

With hybrid work and IoT, endpoint security today is anything but optional. And while security service providers offer endpoint detection and response (EDR) services, it can be difficult to compare solutions. Here are some primary ways to separate leaders from laggards.

Why endpoint security?

56%
of employees use personal devices for work

150%
growth rate in ransomware attacks

Sources: TechRepublic and TechJury.net

Endpoint security technology checklist

Standard antivirus technologies have no chance in helping you fight against today's sophisticated ransomware threats — advanced endpoint protection technology is required.

Must-have features

- [ ] Cloud-enabled technology compatible with a full range of enterprise devices and IoT
- [ ] Machine learning analytics to detect malware, ransomware, and "zero-day" attacks
- [ ] Fileless attack protections to find memory-resident attacks
- [ ] USB port blocking functionality to ensure USB devices are used appropriately
- [ ] Real-time host quarantine features to stop threats in their tracks
- [ ] Management servers hosted in the cloud, thereby accelerating your deployment
- [ ] Automated remediation and roll-back capabilities to help accelerate threat response

BEWARE!

Endpoint security should NOT rely on attack signatures or unique indicators of compromise, because these can change quickly.

BE PREPARED!

It's not uncommon to find a ransomware attack immediately after installation.

Comparing endpoint detection & response services

Most companies struggle to staff 24/7 security operations, requiring a fully managed service.

Key questions to ask your EDR provider

1. Do you own and operate your own SOC? If so, where? Is it 24/7 service?
2. What is your process for addressing and resolving threats, and how is it customizable?
3. How are machine learning, SOAR automation, and intelligence subscriptions integrated?
4. What is your process for assessing, prioritizing, and communicating risks?
5. What industry-leading frameworks guide proactive security improvements?
6. Can you also help with network security, cloud security, and user identity management?

People + process = 90% of success

Technology is not enough. Gartner says an effective security program is:

60%
process

30%
expertise

10%
technology

Source: Gartner "Market Guide for Managed Security Services"

A guide to endpoint security

GET THE GUIDE

COMCAST BUSINESS | MASERGY