Making Sense of EDR

and the Cyber-Insurance Connection

LeapFROG®

Making Sense of EDR
and the Cyber-Insurance Connection

Hackers keep finding more advanced ways to infiltrate your company, so your company needs to keep up.

EDR, or Endpoint Detection and Response, is an advanced cybersecurity tool that meets today's cybercriminals where they are. By continually monitoring your most likely attack surfaces — your endpoints — you can thwart attacks and reduce recovery costs, which protects your company and makes you more attractive to cyber insurance providers.

Why does EDR protect you better than what you're using right now?

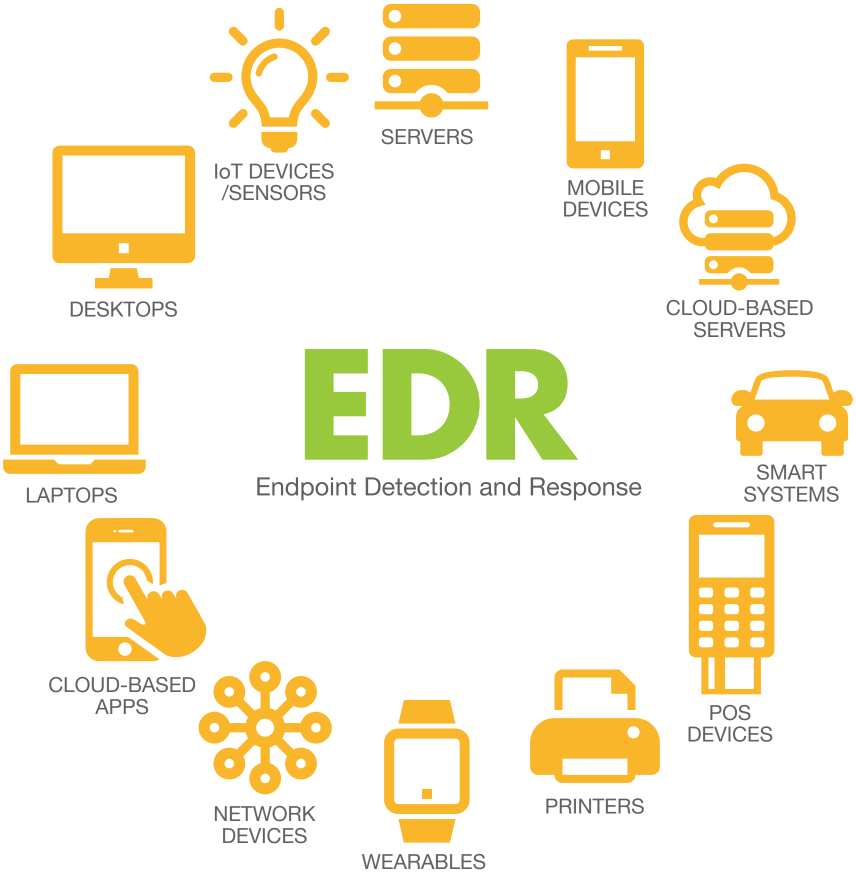
Your endpoints are the easiest targets for hackers. Endpoints include all of the desktops, laptops, mobile phones, tablets, servers, and virtual environments connected to your network — any one of them can be your weakest link.

EDR continually monitors all of the endpoints connected to your network. It combines artificial intelligence (AI), next-gen antivirus, and other technologies into a single integrated solution with a hub that provides exceptional visibility. The tool collects, correlates, and analyzes all endpoint data to quickly detect and mitigate both previously known threats and new, unknown threats.

Detecting and responding to endpoint threats is especially important in today's environment — hackers are relying less on malware and viruses. Instead, they're infiltrating legitimate business applications used on endpoints. Even best-in-class traditional security tools can't detect those kinds of threats.

EDR lets your company stay on top of modern threats by recognizing threat patterns in real time and then taking action.

By continually monitoring your most likely attack surfaces — your endpoints — you can thwart attacks and reduce recovery costs, which protects your company and makes you more attractive to cyber insurance providers.



What's different about today's threat environment?

Hackers are showing no signs of letting up. The pandemic pushed cybercrime into overdrive, with the prime drivers being remote working and fast-turnaround digital transformations.

For the past two years, risk management has taken a back seat to actions that keep businesses running. Now it's time to catch up.

- Nearly half of businesses reported a breach in the past year
- SMBs are attacked as frequently as larger companies
- Ransomware attacks, payouts, and recovery costs continue to rise
- Downtime from an attack can cost 50x a ransom demand
- It takes an average of 197 days to identify a breach
- It costs about 4x more to recover from a breach than to contain it
- Companies with immature cybersecurity spend 2.5x more to recover

For the past two years, risk management has taken a back seat to actions that keep businesses running. Now it's time to catch up.

What's more, cybercriminals are getting bolder and adding new tactics.

Cybercriminals are attacking supply chains to magnify their impact, using deep-fake video and audio scams, and threatening ransomware victims with "name and shame" schemes that involve stolen data.

Nation-states have moved beyond targeting critical infrastructure to focusing the majority of their efforts outside the government sector, and now hackers are supporting their side in international conflicts by trying to disrupt rival economies with cyber warfare that includes targeting the private sector.

All of these trends increase your risk and need for cyber insurance. But companies like yours aren't the only ones facing higher risks.

Why are cyber insurance companies charging twice as much for half the coverage?

Greater cyber risk means insurance providers are pickier about who they insure, charge higher premiums to cover the increased risk, and limit what and how much they'll cover.

Over the past year, many companies have found it harder to get or renew cyber insurance policies without updating their systems first. Insurers and reinsurers have reevaluated their appetite for risk and now require tighter security controls.

The most recent data from MarshMcLennan show cyber insurance premiums increased by an average of 174% per million in coverage over the previous year. Coverage options have also been slashed. Today, getting more than $10 million in coverage can be difficult regardless of the premium.

Part of the reason for the changes is due to the age of the industry — cyber insurance is relatively new and had been priced too low initially. As it turned out, providers didn't have enough money from cyber policyholders to cover multiple major simultaneous incidents. Even with reinsurance, providers' risk is increasing substantially, according to Harvard Business Review.

Cybercriminals are doing their research and attacking companies they know have cyber insurance policies and for what amount of coverage. This leaves providers vulnerable to systematic, strategic attacks on their policyholders.

Part of the reason for the changes is due to the age of the industry — cyber insurance is relatively new and had been priced too low initially.

What can you do to get a cyber insurance policy at the best premium with the most coverage?

Everything you do to assume more responsibility for protecting your own IT environment will improve your ability to qualify for cyber insurance and get an affordable policy that meets your needs.

You can think of security management in two distinct buckets.

First, you need to do the basics to protect and defend your environment. These activities will help you meet the minimum requirements to qualify:

- Secure what's most important and use ransomware-resistant backups
- Implement Multi-Factor Authentication/MFA to keep out unauthorized users
- Make sure your systems and technologies are always up to date
- Encrypt your data and devices so they're unreadable to others
- Secure email and mandate Security Awareness Training
- Implement EDR to monitor all endpoints and mitigate threats
- Simplify protection with Unified Threat Management/UTM

Infrastructure first! To benefit from EDR or any advanced technology, you need the infrastructure to run it. The key is to build the strong foundation you need before you want to implement new technologies. By planning ahead, you'll be ready to leverage innovations that help you grow, prosper, and stay secure.

Next, add greater security by monitoring for threats and taking steps to contain them. These activities further reduce your risk to help you get better rates and coverage:

- Use proven security standards, such as NIST or ISO
- Minimize exposure with network segmentation and firewall policy-based boundaries
- Make the best use of your available security by enabling the latest security controls
- Reduce points of compromise with vulnerability scans and vulnerability-free technology
- Improve your ability to spot and respond to events by consolidating visibility
- Classify all data based on their sensitivity level
- Limit third-party vendor risk and leverage third-party security expertise
- Put processes and plans in writing and practice them for emergencies

Finally, consider hiring an external security firm to try to penetrate your network before insurance-provider experts test for themselves.

Get more details on **Why EDR?** and **Can You Qualify for Cyber Insurance?**

Infrastructure first! To qualify for cyber insurance, your infrastructure needs to support the activities that protect your IT environment. The best plan is to build a strong foundation in anticipation of new technologies, processes, and opportunities — including advanced security tools. Your infrastructure will be ready to support your business continuity and growth.

Leapfrog requires our clients to run EDR

Leapfrog Services is confident in the ability of EDR to reduce our clients' risk exposure and improve their ability to get good cyber insurance because we see it in action every day. As an MSP and MSSP responsible for thousands of endpoints, our security team confirms that EDR stops threats before they can do much (or any) damage and that companies can recover much more quickly when they leverage EDR's capabilities.

While EDR is just one piece of your security management strategy, it's become table stakes for a secure IT environment.

The more cyber risk your company can manage through a proactive security program, the more attractive you are as a cyber insurance client. EDR is part of that equation.

It's important to note that having EDR onboard is the first step in three levels of detection and response. XDR, or Extended Detection and Response, improves threat visibility and mitigation further by expanding the information sources to more than just endpoints. And with MDR, or Managed Detection and Response, a security team actively evaluates and responds to detected events and continually fine-tunes your system for accuracy.

Leapfrog provides all detection and response management levels, and we are developing additional materials to help you make sense of these technologies and services.

Data Sources: The Hiscox Cyber Readiness Report 2022, Sophos State of Ransomware 2021, Microsoft Digital Defense Report FY21, FBI Cyber Division, IBM Data Breach Report 2021

Everything you do to assume more responsibility for protecting your own IT environment will improve your ability to qualify for cyber insurance and get an affordable policy that meets your needs.

Leapfrog is an outsourced MSP and MSSP that designs, builds, and manages secure IT environments that are easy to use.

Since 1998, we've been partnering with organizations to solve business problems by solving IT problems. We manage IT in more than 350 locations for organizations across all industries, partner with all of the leading technology providers, and are SSAE 18 SOC 2 and PCI compliant.

*To deliver high-performing IT services that are holistic, scalable, and aligned with your business needs, we use a proven methodology to optimize and improve your IT systematically. First, we **assess** your current IT to understand your business and challenges, then we **deploy** updated solutions and proactively **manage** and **enhance** your IT environment.*

Leapfrog is proud to have partnered with many of the same clients for decades, and the majority of our new clients come from referrals. Leapfrog clients over the past ten years:

96%
say they will continue to partner with Leapfrog for the next 12 months

97%
say Leapfrog is more effective than their in-house IT staff

96%
are happy with our after-hours support

97%
have confidence in Leapfrog security

If you're ready to take your IT to the next level, Leapfrog is ready to help. Please call 866-260-9478 or contact us at sales@leapfrogservices.com.

Our managed IT services include:

Security Management
Cloud Management
Infrastructure Management
Application Management
IT Support Center