COMCAST BUSINESS | MASERGY

WHAT YOU'LL LEARN

- How to protect against ransomware
- Key EDR features to look for
- How companies use EDR to fight and win

E-GUIDE

EDR: The single best protection against ransomware

No matter how much you educate employees on cybersecurity risks and trust them to protect their devices and endpoints, ransomware attack methods are continuously evolving, and endpoint deficiencies are often the primary reason organizations fall victim to ransomware attacks. Here we explore why advanced Endpoint Detection and Response (EDR) is the best medicine for ransomware, what to look for, and how companies have used it to fight and win against some of the biggest attacks over the past two years.

Ransomware: Costing companies the ultimate price

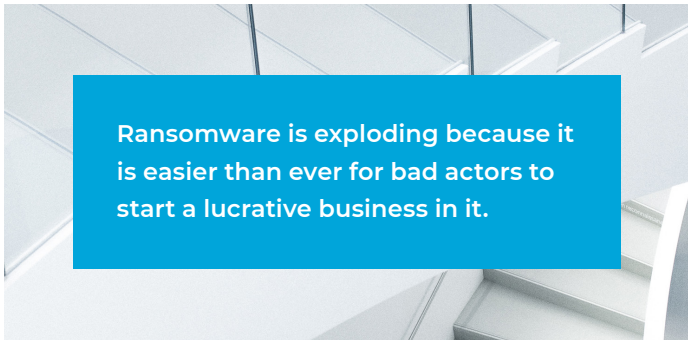
Ransomware at its most basic level is a form of malware that encrypts files on both user endpoints and servers, making them inaccessible until they are decrypted. Attackers aren't always looking for your specific data, but simply the ability to disrupt your business operations. They know that it's often easier and cheaper for IT leaders and their companies to pay the ransom in order to restore day-to-day operations than try to recover from the attack on their own.

Ransomware attacks on business have been incrementally increasing by at least 148% year over year and even more when you look at specific industries. This is a serious and rising threat to all businesses of all shapes and sizes, including both public and private companies. Ransomware is exploding, because it is easier than ever for bad actors to start a lucrative business in it. For example, ransomware-as-a-service tools offer upgraded infrastructures that are more scalable and simple to use, increasing the ability to target victims.

Most attacks are strategic in nature, with the vast majority of them occurring on the weekends and/or overnight using a "logic bomb" to do the most damage. Logic bombs harvest company data on the network and lock users out of the entire environment. With no one able to access the corporate network, an attack can easily take a company offline for 5 to 10 days and cost millions of dollars in lost productivity and damages. Insurance doesn't help in these scenarios either, making bankruptcy another plausible result.

Companies are ill prepared to both prevent ransomware and reactively handle it. The questions Masergy receives from our partners and customers, reveal just how difficult ransomware challenges can be:

- We were hit with a ransomware attack. What can I do about it?
- How can we be more proactive with ransomware protection?
- We know we need to protect our endpoints, but we can't see what is really happening on them. Can you help?
- We have an endpoint product, but we continue to get hit with malware and ransomware. Is there a better option?



Ransomware: Why EDR is the single best protection

With bad actors now acting more strategically versus only opportunistically, there is only one security solution that makes a successful ransomware attack virtually impossible and keeps up with the current ransomware evolution: advanced EDR combined with 24/7 SOC monitoring for incident response and remediation. The best way a company can defend themselves is to establish an EDR that takes your cyber security beyond standard signature-based antivirus and threat detection methods–which have little to no chance in helping you fight against the sophisticated ransomware attacks today.

Time is not on your side when responding to an attack, which is why technology alone is not enough. EDR tools must be paired with 24/7 security monitoring and response services in order to stop these compromises in their tracks. Certified security analysts working in the SOC are needed to watch over and protect endpoints while everyone is sleeping.

Ransomware attacks on business have been increasing yearly by at least

148%

Advanced EDR: How to identify the best solutions

It's important to note that not all EDR solutions are created equal. The most effective EDR tools are ones that get visibility into both local and remote endpoints and server assets while including advanced algorithms to detect and contain ransomware which also have the ability to mitigate an attack once it has occurred.

Key features of an advanced EDR solution

- AI or machine learning to detect previously unknown "zero-day" attacks
- Fileless attack protection
- Automated remediation and roll back capabilities
- Real-time host quarantine
- USB port blocking
- 24/7 MDR monitoring services
- Integrated threat hunting and forensics

Ransomware success stories

Organizations using advanced EDR solutions were not susceptible to the recent Solar Winds supply chain attack (Sunburst). More recently, organizations using advanced EDR tools were able to mitigate and stop the proliferation of the zero day ProxyLogon attack (Halfnium) against Microsoft Exchange Server, an attack that impacted over 100,000 servers worldwide. That attack was weaponized by multiple ransomware operations and used to encrypt servers inside company networks.

As ransomware surges, EDR is proving to be the single best protection against attacks.

- **SUNBURST** - The supply chain attack on IT management software SolarWinds that compromised tens of thousands of large government and business organizations
- **HAFNIUM ProxyLogon** - The zero-day exploit that encrypted information on over 100,000 Microsoft Exchange email servers worldwide
- **DarkSide** - The ransomware attack that shut off the Colonial Pipeline, critical infrastructure delivering 45% of the US east coast's gasoline and jet fuel

About Masergy

Masergy is the software-defined network and cloud platform for the digital enterprise. Recognized as the pioneer in software-defined networking, Masergy enables unrivaled application performance across the network and the cloud with Managed SD-WAN, UCaaS, CCaaS, and Managed Security solutions. Industry-leading SLAs coupled with an unparalleled customer experience enable global enterprises to achieve business outcomes with certainty.