Endpoint Detection and Response

Help Protect Your Business From Ransomware



COMCAST BUSINESS

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 a great solution for ransomware, what to look for, and how companies have used it to help fight against some of the biggest attacks, helping them to create a great customer experience that will help keep customers coming back and make new customers loyal.

WHAT YOU'LL LEARN:

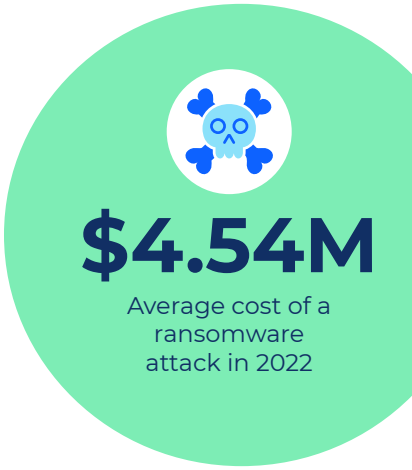
- **How to help protect against ransomware**
- **Key EDR features to look for**
- **How companies use EDR**



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.

According to a study by IBM, the average cost of a ransomware attack in 2022 cost $4.54 million, not including the cost of the ransom itself. 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.

Companies need to be prepared to both prevent ransomware and reactively handle it. The questions customers and partners ask 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 security?
- 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?

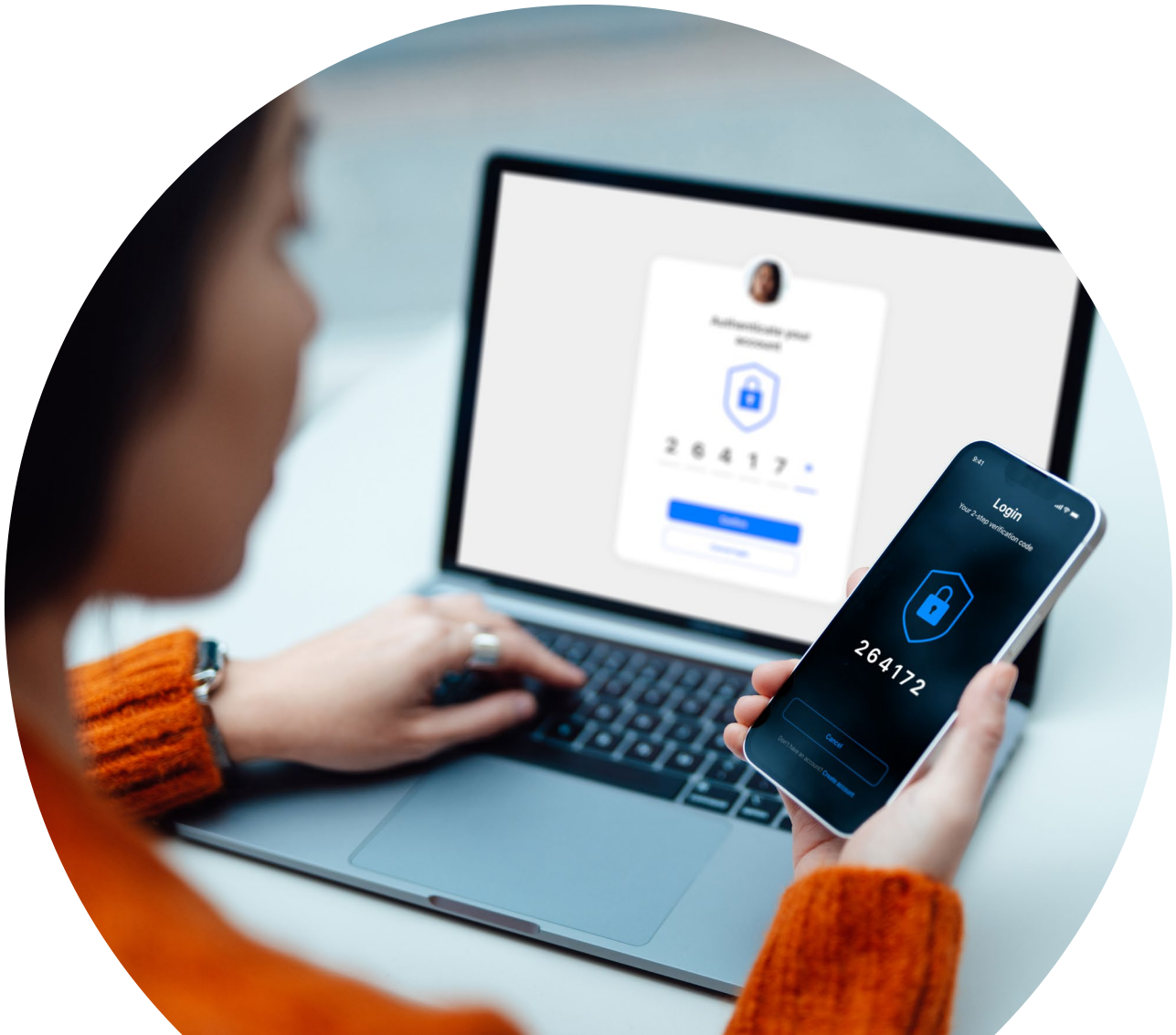
Ransomware is exploding because it is easier than ever for bad actors to start a lucrative business in it.

Ransomware: Why EDR is a Great Option

With bad actors now acting more strategically versus only opportunistically, there is a security solution that keeps up with the current ransomware evolution: advanced EDR combined with 24/7 SOC monitoring for incident response and remediation. A great way to help defend your company is to establish an EDR that takes your cyber security beyond standard signature-based antivirus and threat detection methods.

Time is not on your side when responding to an attack, which is why technology alone is not enough. According to a study from IBM, data breaches with lifecycles greater than 200 days costs on average $1.12 million higher than breaches with lifecycles shorter than 200 days.

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 secure endpoints around the clock.



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 security
- Automated remediation and roll back capabilities
- Real-time host quarantine
- USB port blocking
- 24/7 monitoring, detection, and response
- Optional integrated threat hunting and forensics

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

©2023 Comcast. All rights reserved. CB-EDR-E-Guide_SLS91677-D_7.23