

RANSOMWARE PREVENTION IS POSSIBLE

Effective ransomware protection starts with a Zero Trust mindset and a prevent-first strategy. With the most expensive and feared malware threats—double, triple, quadruple extortion strategies—occurring, shielding your organization from ransomware requires a proper defense posture, reduced exposure, and stopping threat actors at the start.

THE IMPACT OF RANSOMWARE

RANSOMWARE IS A SERIOUS THREAT TO ORGANIZATIONS AND PROVED TO BE A GROWING MENACE IN 2021:

\$1.85 MILLION

WAS THE AVERAGE COST OF A RANSOMWARE BREACH IN 2021¹

21 DAYS

WAS THE AVERAGE DOWNTIME FOR ORGANIZATIONS²

14 OUT OF 16

CRITICAL INFRASTRUCTURE SECTORS WERE TARGETED IN 2021³

32% OF THE TIME

C-LEVEL EMPLOYEES LEFT AFTER A SUCCESSFUL RANSOMWARE ATTACK⁴

80% OF ORGANIZATIONS

WERE HIT BY A SECOND, REPEAT ATTACK⁵

RANSOMWARE EVOLUTION TIMELINE

1989

First known ransomware attack

Traditional ransomware attack: encrypt data → extort for money → decryption key provided if ransom paid

WannaCry and Not-Petya caused global security crisis

• WannaCry attack included 150 countries⁶
• NotPetya caused about \$10 billion in damages worldwide⁷

2017

2019

First known double-extortion attack

935% increase in the number of companies that have had their data exposed on a data leak site during the study period⁸

First known triple-extortion attack

Ransomware's 93% surge was mainly fueled by triple extortion⁹

2020

2021

First known quadruple-extortion attack

• These types of attacks are not as frequent
• The average payment surged 171%, to more than \$312K¹⁰

TRENDING RANSOMWARE

According to BlackBerry® threat research, the top ransomware threats faced by organizations over the past year are:



REVIL

Typically spread through:

- Phishing attacks
- Known software vulnerabilities
- Brute force attacks on remote desktop protocol (RDP)



DARKSIDE

- Uses double-extortion tactics
- Targets Windows® and Linux® systems



CONTI

- Targets organizations in manufacturing, healthcare, and insurance industries worldwide
- Highly customizable, making it useful against a wide variety of targets



AVADDON

- First appeared in 2020
- Uses double and triple extortion



RAGNAR LOCKER

- Operated by threat actors who claim their attacks are a service for their victims¹¹
- Uses double extortion and hosts a 'Wall of Shame' where victims are listed



HIVE

- Notable for using the relatively new Go programming language
- Employs double extortion

TIPS TO HELP PREVENT RANSOMWARE ATTACKS

1

Keep software updated

Exploiting known vulnerabilities is a key component of many ransomware campaigns. Keeping devices updated deprives threat actors of a major advantage.

2

Track and manage

Implement a system to track vulnerabilities across networks, devices, and services because most enterprise environments are constantly changing.

3

Adopt strong password policies and multi-factor authentication (MFA)

Compromised and shared credentials are a massive vulnerability.

4

Reduce the attack surface

Follow the principle of least privilege access. Remove unnecessary devices and software from the environment. Where possible, reduce network connections and access.¹²

5

Protect data

Create strong data recovery (including testing recovery) and backup policies.

6

Follow good security practices

Train employees, use MFA, and implement strong passwords.

BE RANSOMWARE PREPARED.

Organizations looking for solutions that take ransomware protection to the next level should consider managed extended detection and response (XDR) platforms and artificial intelligence (AI). The **Cylance® Endpoint Security** offers organizations AI-empowered protection and a **Zero Trust** framework that can protect any device, anywhere, from ransomware.

For more information on preventing and remediating ransomware, [see our helpful guide](#) →