

7 WAYS TO PROTECT AGAINST RANSOMWARE ATTACKS



Cybercriminals are also getting bolder. Their frequency, sophistication, and reach are steadily increasing.

2,690
Organizations victimized by ransomware in 2021



\$600M
Ransomware payment by victims



22
Days average downtime due to ransomware attacks

518%
YoY increase in ransomware attacks, 2020-21



\$570K
Average ransom paid by mid-sized organizations



83%
Ransomware victims paid the ransom

The Top Ransomware Attack Vectors



Remote Desktop Protocol

Software Vulnerabilities

Phishing Emails

Fake Software



Recent advisories from the U.S. Cybersecurity & Infrastructure Security Agency (CISA), the FBI, and National Security Agency urge all organizations—even individuals—to take steps to protect themselves.

It's essential that all businesses, regardless of size, remain vigilant.



Here are 7 ways that enterprises large and small can protect themselves from ransomware.



1 Build a multi-layered defense

Implement and regularly update your cyber defenses, including email filters, antivirus software, and firewalls to protect your entire IT environment.



3 Strictly control who has access to what

Follow the Zero Trust model of least privileged access when provisioning users on critical systems storing sensitive data. Just what they need to do their jobs. Regularly review and update privileges, as necessary.



5 Implement multi-factor authentication

Something you know. Something you have. Something you are. MFA mitigates the risks associated with leaked user IDs and passwords.



7 Stay current with system updates & patches

It's easy for updates to critical software and firmware to slip through the cracks. Vulnerable applications and OSs are the attack vectors of most ransomware. Protect your enterprise by patching regularly.



2 Back up critical systems

Minimize the risk of losing critical data and ensure business continuity and disaster recovery in the event of an attack.



4 Consider advanced protection technologies

Advanced detection, monitoring, and response solutions can help your organization identify potential risks and remediate vulnerabilities before they become exploited.



6 Conduct cybersecurity awareness training

Advanced detection, monitoring, and response solutions can help your organization identify potential risks and remediate vulnerabilities before they become exploited.

90%

Ransomware infections via email



Ready to be ransomware aware?
Download the Ransomware Playbook now.