vmware

# 20 Best Practices to Enforce a Zero Trust Ransomware Defense

Ransomware attacks are extremely destructive to business continuity, producing downtime, leading to financial losses, and jeopardizing ongoing institutional trust. The average downtime after a ransomware attack is roughly 30 days, and 96 percent of victims do not regain access to all their data even after payment is made.[1]

How likely is it that your business will be targeted by a ransomware attack?

According to VMware's 2022 Modern Bank Heists report, 63 percent of respondents experienced some form of a destructive attack—a 17 percent increase year over year from 2021.[2] The reality is that ransomware is a threat your business can't afford to underestimate. Half measures and legacy strategies aren't enough. You need a holistic approach that combines contextual visibility, preventative measures, and recovery safeguards.

**277 Days**
Average dwell time (time to identify and contain a data breach)[3]

**30 Days**
Average downtime after a ransomware attack, but could be much longer[1]

## Prevention is the most effective defense

By identifying malicious behavior before an attack takes place, these attacks can automatically be blocked.

## Follow these 20 best practices recommended by our security experts

1. **Implement an awareness and training program.**
   End users are top targets, so everyone in your organization needs to be aware of the threat of ransomware and how it's delivered.
2. **Scan and filter all incoming and outgoing emails.**
   Use content scanning and email filtering to detect threats before they reach end users.
3. **Enable strong spam filters.**
   Spam filters can help prevent phishing emails from reaching end users.
4. **Block ads.**
   Ransomware is often distributed through malicious ads served when visiting certain sites. Blocking ads can reduce that risk.
5. **Configure firewalls.**
   Internal and perimeter firewalls allow authorized users and workloads to access data while blocking access to known malicious IP addresses.
6. **Logically separate networks.**
   Separating networks helps prevent the spread of malware. If every user and server is on the same network, the most recent variants can spread.
7. **Inspect east-west (internal) traffic.**
   Inspecting internal traffic enables anomaly detection of certificates when traffic is encrypted.
8. **Inspect north-south traffic.**
   Detect command and control traffic by using threat intelligence to identify malicious IP addresses, domains and more.
9. **Scan network artifacts.**
   Dynamically analyze file behaviors for threats by using AI to detect malicious code.
10. **Categorize data based on organizational value.**
    Implement physical and logical separation of networks and data for different organizational units.
11. **Use the principle of least privilege to manage accounts.**
    Users should not be assigned administrative access unless absolutely needed.
12. **Use application control on critical systems.**
    Implement a default-deny policy for non-approved programs and scripts to stop ransomware before it can access your critical assets.
13. **Patch operating systems, software and firmware on devices.**
    Consider using a centralized patch management system.
14. **Establish vulnerability discovery and remediation processes.**
15. **Back up data regularly.**
    Verify the integrity of those backups and test the restoration process to ensure it's working.
16. **Secure your offline backups.**
    Ensure backups are not connected permanently to the computers and networks they are backing up.
17. **Conduct an annual penetration test and vulnerability assessment.**
18. **Create a response plan.**
    Build a ransomware recovery incident response plan and test it frequently.
19. **Tap into behavioral analysis.**
    Leverage tools that provide behavioral analysis of powered-on workloads to contain and eradicate fileless strains of ransomware at recovery.
20. **Conduct safety tests.**
    Provision an isolated recovery environment to safely test and iterate workloads, so you can protect them in the event of a successful ransomware attack.

Secure your multi-cloud network with the strongest defense against ransomware. Start now by visiting vmware.com/solutions/ransomware-protection.

1. Sophos. "The State of Ransomware 2022." April 2022.
2. VMware. "Modern Bank Heists 5.0." April 2022.
3. IBM Security. "Cost of a Data Breach Report 2022." July 2022.