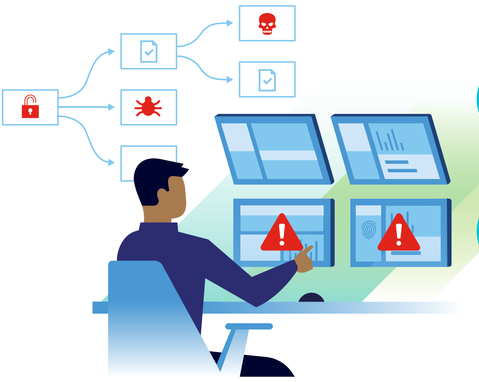
vmware NSX Security

17 Best Practices to Protect Against Ransomware

Ransomware attacks can be extremely destructive to a business and its ability to function. According to a study published in *Health Services Research*,[1] ransomware adds an extra 2.7 minutes to response times for heart attacks, leading to an additional 36 deaths per 10,000 heart attacks each year. Recovery efforts from ransomware attacks can also damage an organization's finances and reputation.

Seventy percent of surveyed respondents in the VMware Carbon Black *Global Incident Response Threat Report*[2] cited they had suffered damage to their corporate image following a breach.

Cybercriminals increasingly evolve their attack tools and strategies by developing ransomware variants that slip by legacy malware protection.



2.7 minutes
added response times for heart attacks

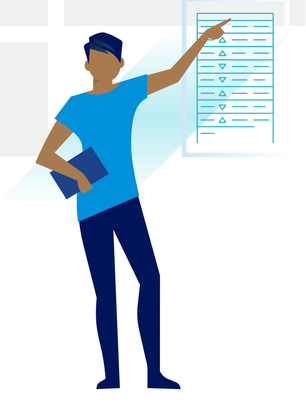
70%
suffered damage to their corporate image

Prevention is the most effective defense.

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

Follow these 17 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.**
   This is to 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 internal as well as perimeter firewalls.**
   This allows authorized users and workloads to access data, while blocking access to known malicious IP addresses.
6. **Logically separate networks.**
   This 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 traffic (internal traffic).**
   This provides anomaly detection of certificates when traffic is encrypted.
8. **Inspect north-south traffic.**
   Detect command and control (C&C) traffic by using threat intelligence to identify malicious IPs, 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.**
    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.**



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

References:
1. Health Services Research. "Data Breach Remediation Efforts and Their Implications for Hospital Quality." Sung J. Choi, M. Eric Johnson, Christoph U. Lehmann. September 10, 2019.
2. VMware Carbon Black. "Global Incident Response Threat Report." Tom Kellermann, Greg Foss. October 2020.

vmware

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com

Copyright ©2021 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.