Defense in Depth: 17 Keys 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*, 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 cited they had suffered damage to their corporate image following a breach.

Prevention is the most effective defense. By identifying malicious behavior before an attack takes place, these attacks can automatically be blocked. The first step is to deploy VMware Carbon Black next-generation endpoint security to detect and stop ransomware attacks.

Follow these 17 best practices recommended by our security experts

1. Implement an awareness and training program.
   - End users are key targets, so everyone in your organization should be aware of the threats and know how to prevent them.

2. Block ads.
   - Ransomware is often distributed through malicious ads served when visiting certain sites. Blocking ads can reduce that risk.

3. Configure firewalls.
   - This allows authorized users to access data, while blocking access to known malicious IP addresses.

4. 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.

5. Enable strong spam filters.
   - This is to prevent phishing emails from reaching end users. Also, authenticate inbound emails using technologies such as SPF and DKIM.

6. 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.

7. Back up data regularly.
   - Verify the integrity of those backups and test the restoration process to ensure it’s working.

8. Secure your offline backups.
   - Ensure backups are not connected permanently to the computers and networks they are backing up.

   - Expand beyond next-gen antivirus and into VMware Carbon Black® Cloud Audit and Remediation™.

10. Use application control on critical systems.
    - Define policy for non-approved programs and scripts to stop ransomware before it can access your critical assets.

11. Configure firewalls.
    - This allows authorized users to access data, while blocking access to known malicious IP addresses.

12. Scan and filter all incoming and outgoing emails.
    - Use content scanning and email filtering to detect threats before they reach end users.

13. Categorize data based on organizational value.
    - Implement physical and logical separations of environments and data to prevent accidental access.

14. Use the principle of least privilege to manage accounts.
    - Users should not be assigned administrative access unless absolutely needed.

15. Scan network artifacts.
    - Dynamically analyze file behaviors for threats using AI to detect malicious code.

16. Inspect east-west traffic (internal traffic).
    - This provides anomaly detection of certificates when traffic is encrypted.

17. Inspect north-south traffic.
    - Detect command and control (C&C) traffic by using threat intelligence to identify malicious IPs, domains and more.

For more information on how you can protect your business with VMware Carbon Black Cloud, visit [carbonblack.com/use-cases/ransomware-protection/](https://www.carbonblack.com/use-cases/ransomware-protection/)