

# 7 ways to protect your network against ransomware

Steps to prevent ransomware attacks and save your money



## The ransomware threat

Sometimes old becomes new again. Such is the case with ransomware attacks, which have become popular once more. First released in 1989, ransomware infects a system and “locks out” the user from accessing the device or files on it. Only when the victim agrees to pay a ransom, usually in the form of bitcoins, can the system be unlocked and accessed again.

The following e-book provides seven ways you can protect your network against ransomware attacks and avoid giving your money to cybercriminals.

Ransom amounts vary, but are often in the \$200-\$400 range.<sup>1</sup>

### 1. Educate your employees

User education and awareness are critical when it comes to defeating ransomware. Treat suspicious emails with caution. Look at the domain name that sent the email. Check for spelling mistakes, review the signature and the legitimacy of the request. Hover over links to check where they lead to.

### 2. Use a multi-layered approach to network security

Protection from ransomware and other forms of malware doesn't begin and end at the gateway. Extending security through the use of anti-virus, anti-spyware, intrusion prevention and other technologies on devices at the network perimeter is critical. Adopt a layered approach to stop ransomware by avoiding a single point of failure in your security architecture.





### 3. Back up your files regularly

Another safeguard against having to pay ransom is a robust backup and recovery strategy. Depending on how quickly the compromise is detected, how widely it has spread and the level of data loss that is acceptable, recovery from a backup could be a good option. However, this calls for a smarter backup strategy that is aligned to the criticality of your data and the needs of your business around recovery point objectives (RPO) and recovery time objectives (RTO).

Implement a layered security strategy for greater network protection.

### 4. Make sure your endpoints are protected

Since most users primarily interact with personal and corporate devices, the endpoints are particularly at risk if they are not managed or don't have the right anti-malware protection. Most anti-virus solutions are signature-based and prove ineffective if not updated regularly. The newer ransomware variants are uniquely hashed and thereby undetectable using signature-based techniques. Many users also turn off their virus scans so that it doesn't slow their system down.

## 5. Patch your systems and applications

Many attacks are based on known vulnerabilities in browsers including Internet Explorer, as well as in common apps and plug-ins. Therefore it's critical to apply updates and patches promptly and reliably. Choosing a solution that is able to automate patching and version upgrades in a heterogeneous device, OS and application environment will go a long way in addressing a range of cyber threats, including ransomware.

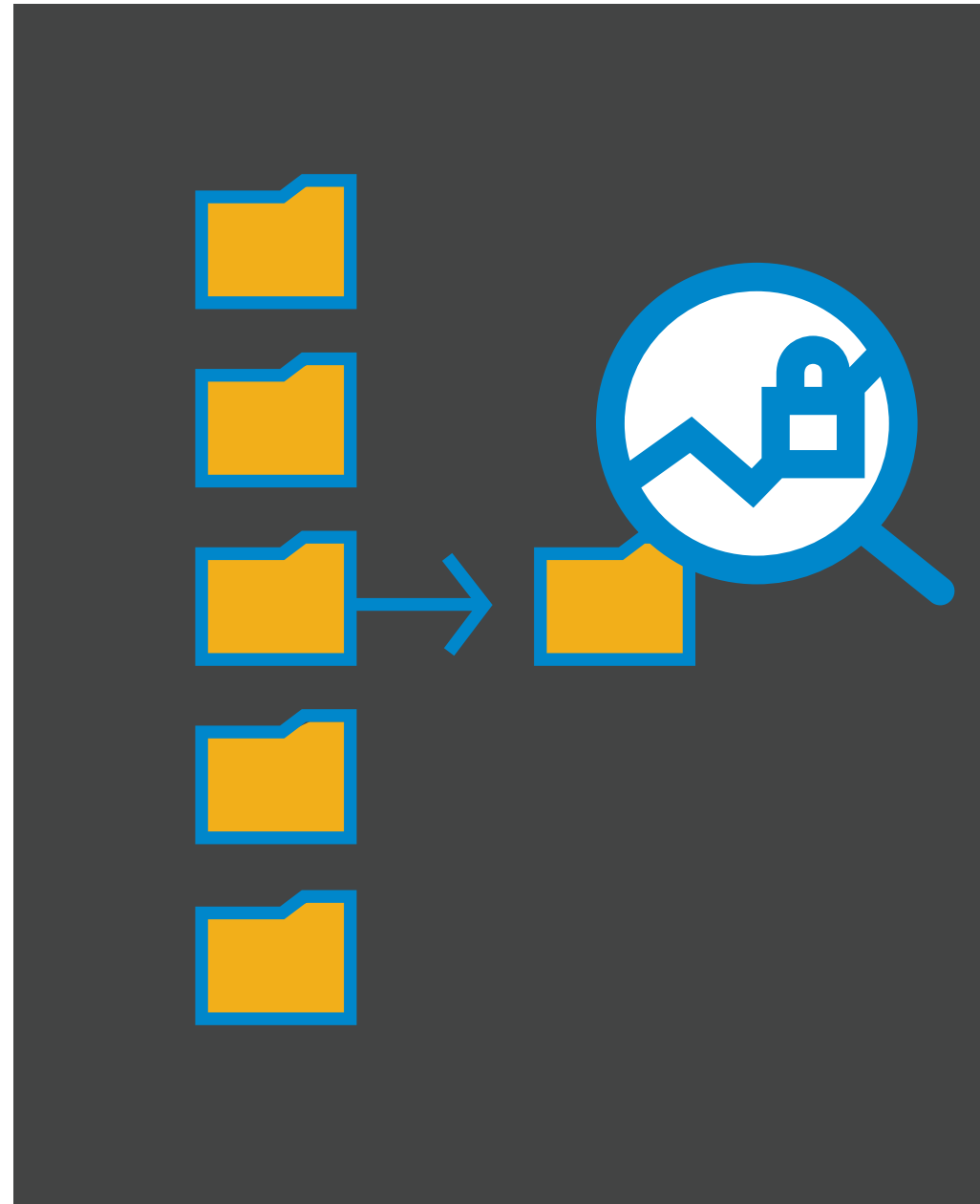
## 6. Segment your network to stop the spread

Most ransomware will try to spread from the endpoint to the server/storage where all the data and mission critical applications reside. Segmenting the network and keeping critical apps and devices isolated on a separate network or virtual LAN can limit the spread.

Segment your wireless LAN to separate internal from guest users for an additional level of security.

## 7. Quarantine and analyze suspicious files

Technologies such as sandboxing provide the ability to move suspicious files to quarantine for analysis before they can enter the network. The files are held at the gateway until a verdict is returned. If a file is found to be malicious you can prevent follow-on attacks by implementing protective measures such as policies that block associated IP addresses or domains, or deploying signatures to security appliances across the network.



## Conclusion

Ransomware attacks have become increasingly popular with cybercriminals. Make sure your network is protected. Dell Security can enhance protection across your organization by inspecting every packet and governing every identity. As a result, this protects your data wherever it goes, and shares intelligence to safeguard against a variety of threats, including ransomware.

Visit the [Dell SonicWALL Network Security Products](#) web page.

## References

[US Computer Emergency Readiness Team Alert \(TA16-091A\)](#)



## About Dell Security

Dell Security solutions help you create and maintain a strong security foundation with interconnected solutions that span the enterprise. From endpoints and users to networks, data and identity, Dell Security solutions mitigate risk and reduce complexity so you can drive your business forward. [www.dell.com/security](http://www.dell.com/security).

If you have any questions regarding your potential use of this material, contact:

### Dell

5455 Great America Parkway,  
Santa Clara, CA 95054  
[www.dell.com/security](http://www.dell.com/security)

Refer to our Web site for regional and international office information.

© 2016 Dell, Inc. ALL RIGHTS RESERVED. This document contains proprietary information protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose without the written permission of Dell, Inc. ("Dell").

Dell Security logo and products—as identified in this document—are trademarks or registered trademarks of Dell, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN DELL'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

