Guarding the Castle

The strategies and tools of cybercriminals and how to defeat them.

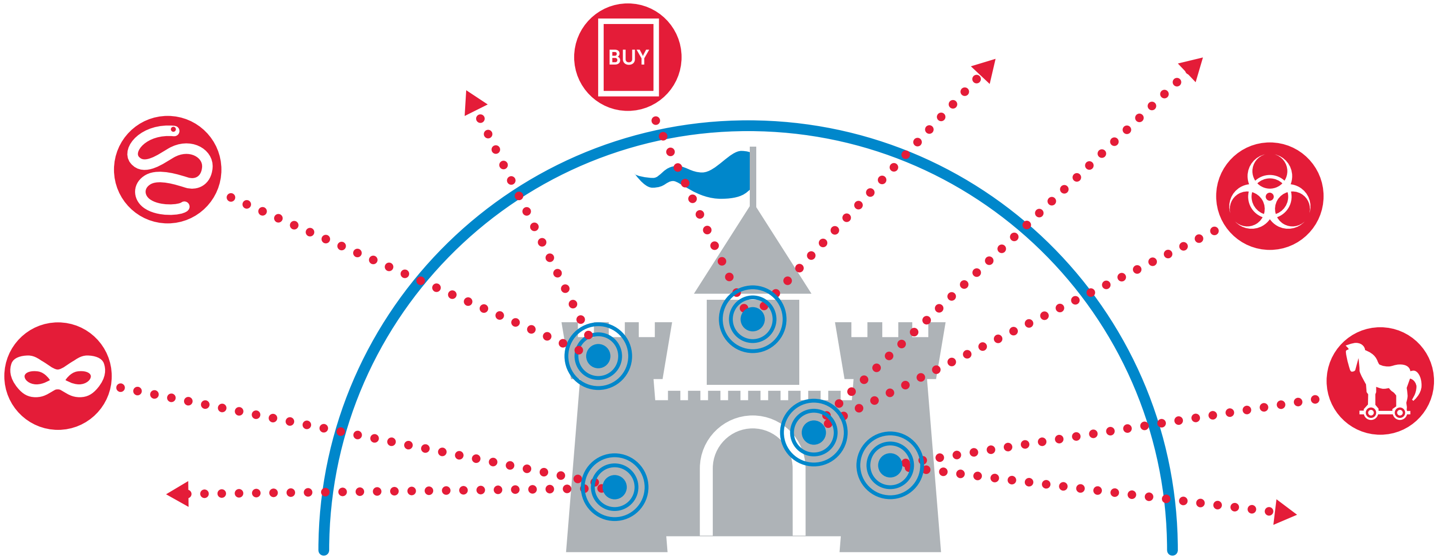


Table of contents

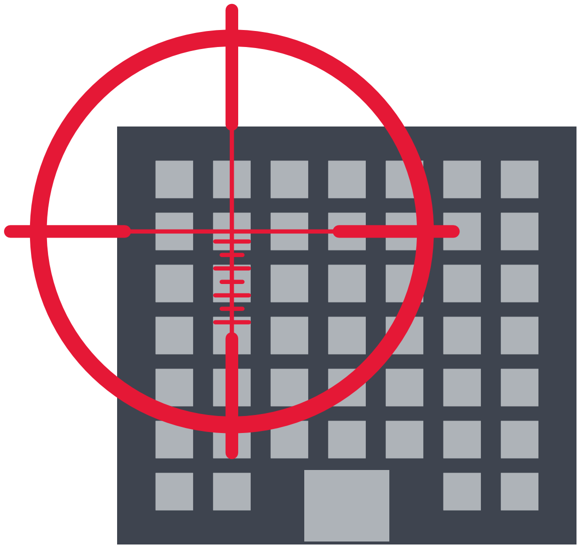
Introduction

Today's cybercriminals employ several complex techniques to avoid detection as they sneak quietly into corporate networks to steal intellectual property. Their threats are often encoded using multifarious complicated algorithms to evade detection by intrusion prevention systems. Once they have exploited a target, attackers will attempt to download and install malware onto the compromised system.

In many instances, the malware used is a newly evolved variant that traditional anti-virus solutions don't yet know about.

This ebook details the strategies and tools that cybercriminals use to infiltrate your network and how you can stop them.

You need to understand your enemies before you can defeat them.



Cyber attack strategy #1: Bombard networks with malware around the clock

Many next-generation firewall (NGFW) vendors offer some form of network-based, anti-malware technology as part of a multi-layered security approach. Most of these systems, however, are limited to just a few thousand malware (5,000-30,000) signatures that reside in the onboard system memory of the NGFW. The problem with this approach is that many of these systems receive new malware protection updates as infrequently as once per day, leaving networks vulnerable to ongoing, ever-evolving attacks.

Wednesday

P.M.

Friday

Sunday

Cybercriminals work 24/7 to exploit your weaknesses.

A.M.

Monday

Thursday

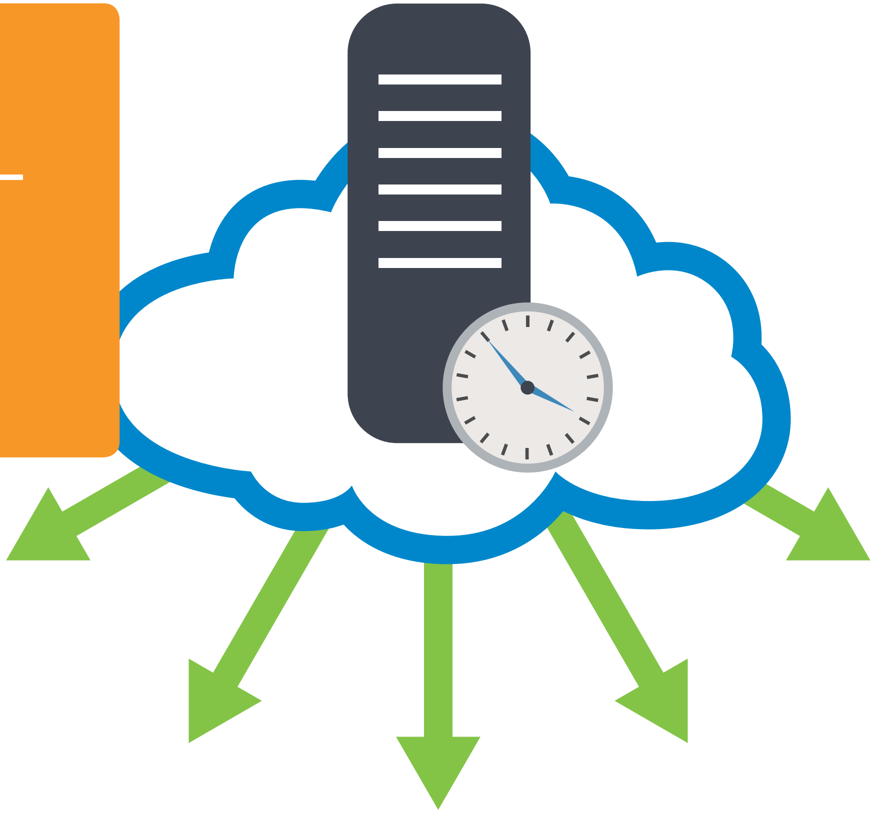
Tuesday

Saturday

Counterattack: Protect your network every minute of every day

With hundreds of new variants of malware developed every hour, organizations need up-to-the-minute, real-time protection against the latest threats. Dell™ SonicWALL™ firewalls have access to a continually updated (24 hours a day, seven days a week) cloud database with more than 14 million variants of malware. Combining proven, network-based malware protection with an enormous cloud database that is updated every few minutes enables Dell SonicWALL to provide organizations of any size with deep security protection against advanced modern threats.

Dell NGFWs leverage the power of the cloud for real-time countermeasures to the latest malware threats.



Cyber attack strategy #2: Infect networks with different forms of malware

Cybercriminals use different types of malware to attack networks. The five most typical types are: viruses, worms, Trojans, spyware and adware.

Computer viruses were originally spread through the sharing of infected floppy disks. As technology evolved, so too did the distribution method. Today, viruses are commonly spread through file sharing, web downloads and email attachments.

Computer worms have existed since the late 1980s but were not prevalent until networking infrastructures within organizations became common. Unlike computer viruses, worms can crawl through networks without any human interaction.

Trojans are designed specifically to extract sensitive data from the network; many types of Trojans will take control of the infected system, opening up a back door for an attacker to access later. Trojans are often used in the creation of botnets.

Spyware is not typically malicious in nature, but it is a major nuisance because it often infects web browsers, making them nearly inoperable. At times, spyware has been disguised as a legitimate application, providing the user with some benefit while secretly recording behavior and usage patterns.

Adware, as the name implies, is often used to spread advertisements that provide some type of financial benefit to the attacker. After becoming infected by adware, the victim becomes bombarded by pop-ups, toolbars and other types of advertisements when attempting to access the internet.

Cybercriminals use different types of malware to catch you off guard.

Counterattack: Ensure that your network is protected against all types of malware

Awareness is the first step in preventing a cyber attack. Once organizations are aware of the different types of methods that cybercriminals use to access and threaten networks, they can choose the right security strategy — one that can effectively block all forms of malware.

Dell SonicWALL firewalls safeguard organizations from viruses, worms, Trojans, spyware and adware by integrating malware protection within their patented, low-latency, single-pass Reassembly-Free Deep Packet Inspection engine. In addition, Dell SonicWALL NGFWs feature:

- **Network-based malware protection** to block attackers from downloading or transmitting malware to a compromised system.
- **CloudAssist malware protection** to safeguard networks around the clock from millions of new variants of malware as soon as they are discovered.
- **Intrusion prevention service (IPS)** to prevent attackers from exploiting network vulnerabilities.

Working in conjunction with the on-board and cloud-based malware protection of Dell SonicWALL firewalls, Dell SonicWALL Enforced Client Anti-Virus software provides a third layer of malware protection for desktops and laptops. When organizations pair the two solutions, they can be assured that all computers accessing the network are using the latest version of anti-virus and anti-spyware software.

Dell SonicWALL NGFWs offer multiple layers of protection against malware.

Cyber attack strategy #3: Find and compromise the weakest networks

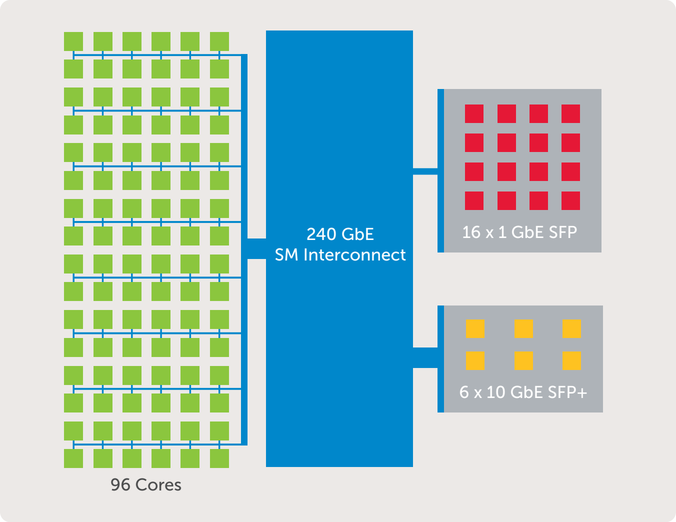
Although many firewall vendors claim to offer superior threat protection, few have been able to demonstrate the effectiveness of their solutions. Organizations that use inferior firewalls may believe their networks are protected, even though skilled criminals can sneak past the intrusion prevention system by using complicated algorithms to evade detection and compromise the system.

Because some firewalls offer protection at the expense of performance, organizations that use them may be tempted to turn off or limit their security measures in order to keep up with the demand of high network performance. This is an extremely risky practice that should be avoided.

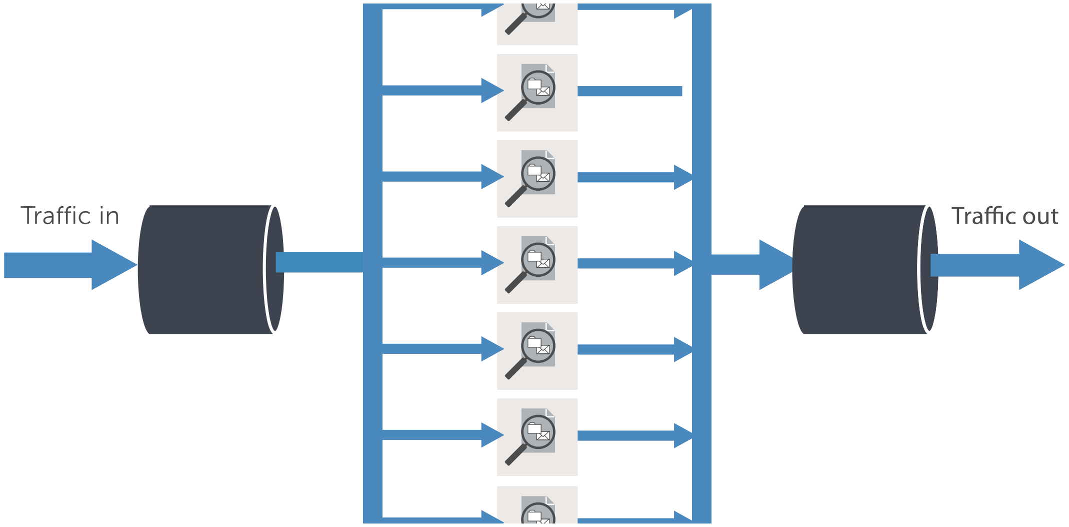
Cybercriminals often target their victims based on the network weaknesses they discover.

Counterattack: Choose a firewall that offers superior threat protection and high performance

Dell SonicWALL NGFWs have been independently tested and certified for network-based malware protection by ICSA Labs. In addition, they feature a multi-core hardware design and Reassembly-Free Deep Packet Inspection® engine to protect networks from internal and external attacks — without compromising performance.



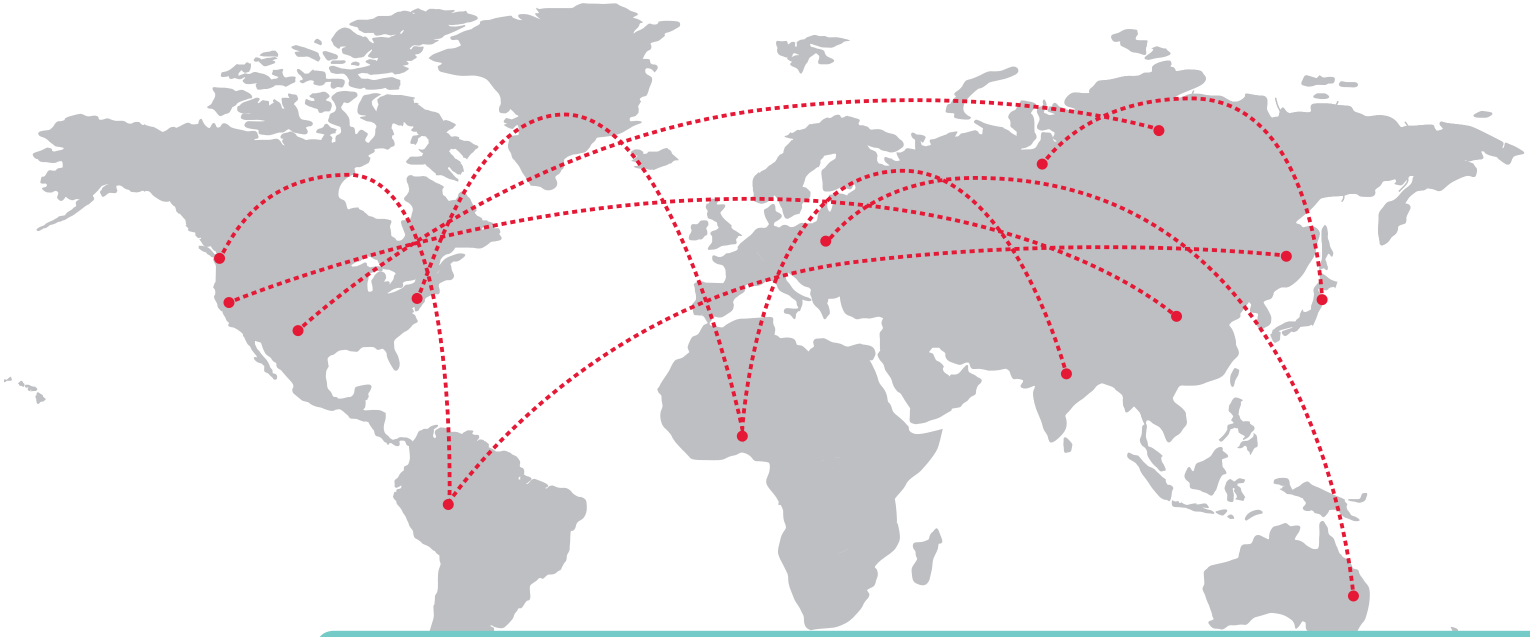
Multi-core hardware architecture for scalability and performance



Reassembly-free packet scanning without proxy or content size limitation

Cyber attack strategy #4: Morph frequently and attack globally

Many cybercriminals succeed by continually reinventing new malware and sharing it with their counterparts around the globe. This means that new threats are popping up every hour on all continents.



Dell leverages more than one million sensors around the world to provide up-to-the-minute threat protection.

Counterattack: Choose a firewall that offers protection against the latest global threats

The dedicated, in-house Dell SonicWALL Threats Research Team provides continuous communication, feedback and analysis on the nature and changing behavior of today's threats. With input from millions of shared touch points in the SonicWALL Global Response Intelligent Defense (GRID) network, the Threat Research Team processes this information in real time and proactively delivers countermeasures and dynamic updates to Dell SonicWALL NGFW appliances, so customers are continually protected against global threats as they emerge.

In addition, Dell SonicWALL NGFWs provide countermeasures against cyber attacks with the Malware Protection CloudAssist Service, a cloud database that continually adds new onboard signatures — more than 14 million to date. CloudAV is accessed by Dell SonicWALL NGFWs via a proprietary, lightweight protocol to further augment signature inspection and security.

Dell SonicWALL NGFWs also feature Geo-IP and botnet filtering capabilities, so organizations can block traffic from dangerous domains, or block connections coming to and from a particular geographic location, in order to reduce network exposure to known global threats.

To block the latest global threats, invest in a security solution with global reach.

How can I learn more?

- Download the whitepaper "Achieve Deeper Network Security"
- View the webinar "The need for a deeper level of security without compromise"
- Opt-in to receive Dell SonicWALL newsletters

For feedback on this ebook or other Dell SonicWALLebooks or white papers, please send an email to feedback@sonicwall.com.

For more information

Dell SonicWALL
2001 Logic Drive
San Jose, CA 95124

www.sonicwall.com
T +1 408.745.9600
F +1 408.745.9300

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.

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results.

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

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.