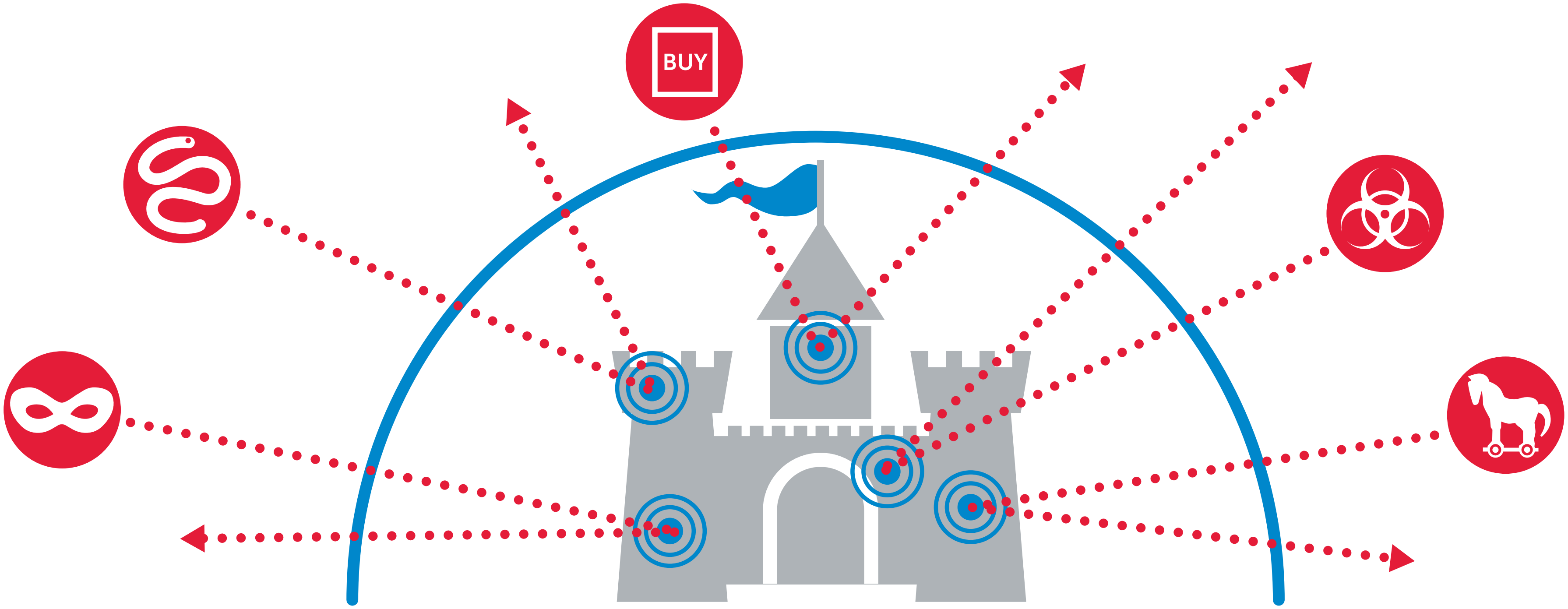
Types of cyber-attacks

And how to prevent them

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 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.



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 5,000-30,000 malware 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.

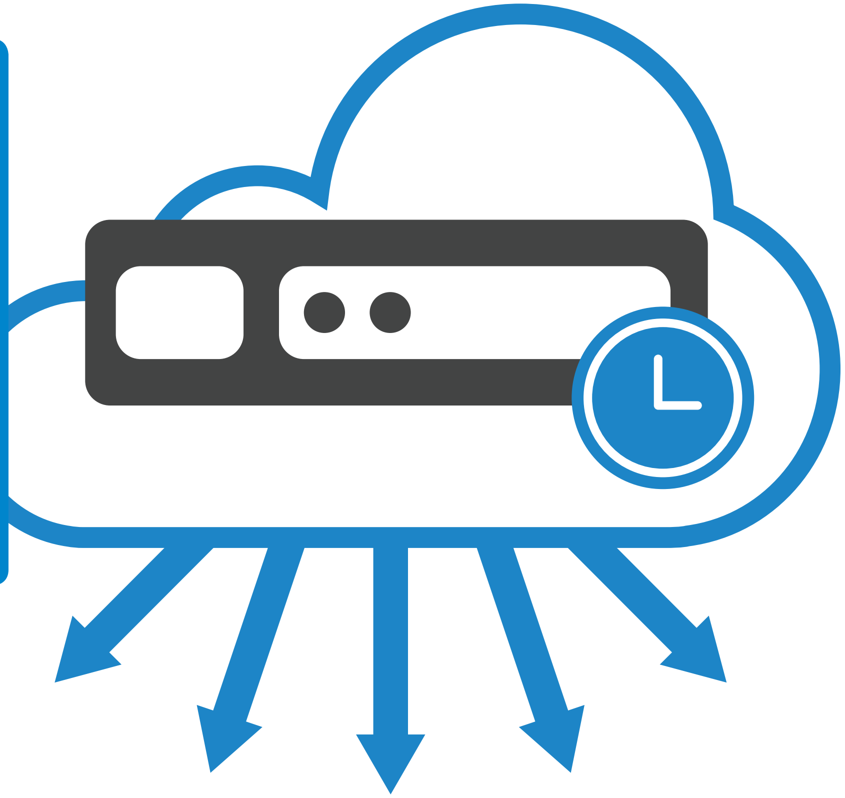
Cybercriminals work 24/7 to exploit your weaknesses.

Counterattack #1

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. An effective firewall needs to be continuously updated, 24 hours a day, 7 days a week. In addition, because the number of malware types and variants is so large, it exceeds the available memory of any firewall. Firewalls should use the cloud in order to provide the broadest view of malware and their variants and best identify them.

Insist on a firewall that leverages 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 #2

Ensure that your network is protected against all types of malware

All firewalls should safeguard organizations from viruses, worms, Trojans, spyware and adware. This is best accomplished by integrating these protections into a single-pass, low latency approach. Look for features that include:

- **Network-based malware protection** to block attackers from downloading or transmitting malware to a compromised system.
- **Continuous and timely updates** 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.

Making sure that everyone who has access to your network has current anti-virus protection software will provide an additional layer of network malware protection. When organizations pair an enforced PC anti-virus with network firewalls, they can reduce many of the tools cybercriminals have for compromising the network.

To stay ahead of threats, consider 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.

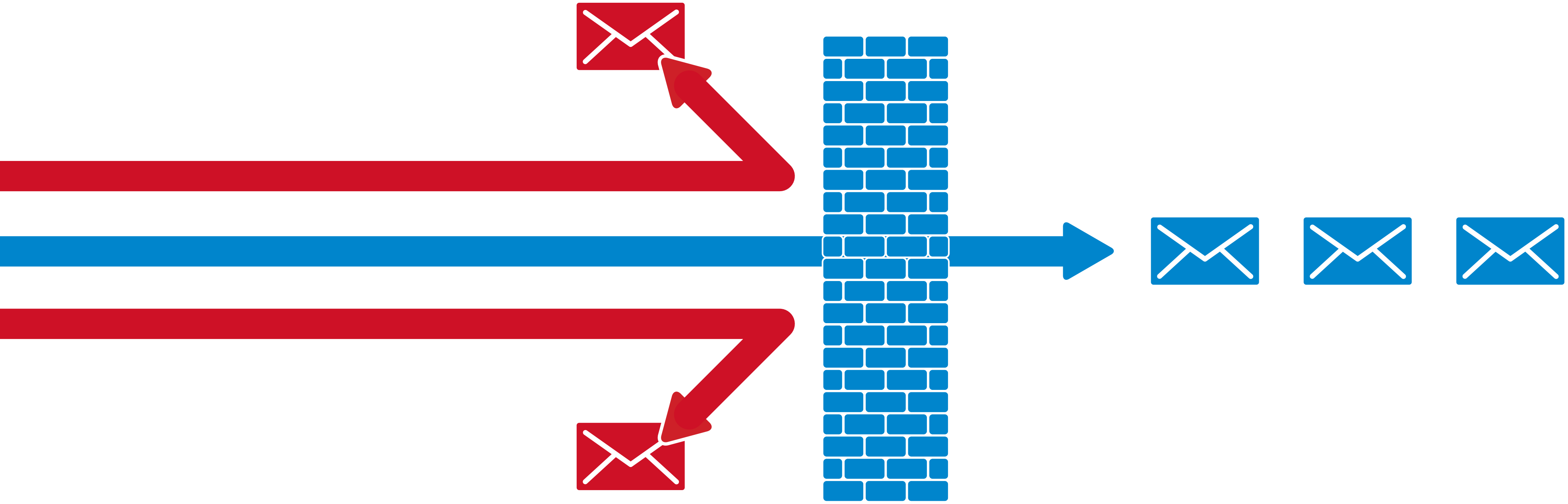
Because some firewalls offer protection at the expense of performance, organizations that use them may be tempted to turn off or limit their security measures in order to keep up with the demand of high network performance. This is an extremely risky practice that should be avoided.

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

Counterattack #3

Choose a firewall that offers superior threat protection and high performance

Look for a firewall that has been independently tested and certified for network-based malware protection by ICSA Labs. In addition, consider a multi-core design that can scan files of any size and type to respond to changing traffic flows. All firewalls need an engine that protects networks from both internal and external attacks — without compromising performance.



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. Many cyber-criminals use a “smash and grab” approach to attacks: get in, take what they can, and get out before anyone can raise the alarm. Then they repeat the attack elsewhere.

New threats are popping up every hour on all continents.

Counterattack #4

Choose a firewall that protects against global threats

Reacting quickly to threats is critical to protection. To most rapidly deploy countermeasures to emerging threats onto your firewall, look for a firewall provider that has its own rapid-response, in-house team of countermeasure experts. In addition, that team should extend its reach by collaborating with the broader security community.

No firewall appliance can hold all of the millions of malware types out there. Older, less-used threat signatures may get dropped from the local firewall, leaving you open to attack. A broad-spectrum solution prevents this by utilizing a globally comprehensive cloud-based malware catalogue to augment local firewall analysis.

Finally, suspicious activity can also be recognized through traffic coming from places you do not do business. While a simple firewall can identify and block by geography, a sophisticated firewall will add botnet filtering capabilities to reduce exposure to known global threats by blocking traffic from dangerous domains or blocking connections to and from a particular location.

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

Conclusion

Cyber-attacks are on the rise, but there are effective defenses. When you are ready to evaluate counter-attack solutions to fit your network environment, learn more by downloading our white paper, "Achieving Deeper Network Security."

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. www.dellsoftware.com.

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

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