BLUE COAT®

Network
+ Security
+ Cloud

SECURITY INSIGHTS BRIEF

ENSURING BUSINESS CONTINUITY WITH A MULTI-LAYERED AV DEFENSE

Protection and Empowerment in Today's Evolving Threat Landscape

There is no question that security attacks targeting your organization will continue to grow and evolve. The question is, how can you respond to malware and other risks without unnecessarily constraining your workforce? How can you get beyond the fear and anxiety that leads to excessive prohibition, prevention, blocking, and excluding – so that you can use security technology to both protect and empower people?

The answer is with a multi-layered defense – one that uses advanced security technologies and sophisticated operational practices in combination to cover the full spectrum of threat vectors. This solution brief explores the growing importance of multi-layered defense in today's fast-changing web environment, and key considerations in implementing an effective multi-layered defense strategy.

Overcoming the Obstacles of Securing the Web

The web remains the primary source of malware distribution, but it is difficult for organizations to secure the web because of its ever-changing nature and massive scale. Highly motivated malware authors need just the tiniest security hole to exploit for financial and competitive gain.

Attackers have a broad variety of methods that they can use in any combination to exploit vulnerabilities. The increased mobility of an organization's data, combined with bring your own device (BYOD) initiatives, are creating ample opportunities for cybercriminals.

The productivity advantages achieved by BYOD are tempered by the fact it introduces new platforms (e.g. iOS and Android) that need to be secured, but over which the organization has little control. Moreover, cloud and social media apps make it extremely difficult for organizations to keep up with all the potential vectors of attack.

For instance, Sophos, a leading AV vendor, found that[1]:

- **250,000** new executable files are added every day – a **300%** increase over four years! (Executables are often used to infect a network.)
- **20 – 30,000** new malicious URLs are seen each day – a new one every two seconds!
- **80%** of malicious URLs are actually legitimate sites that have been compromised, which means it's important to stay on top of all changes that take place on every site.

The Growing Need for Multi-Layered Defense

Since computers and networks can be infected from a variety of attack points, the days of single-point detection belong to the past. The rise of new, dynamic web threats and APTs demands a multi-layered security architecture that maximizes coverage to ensure best-in-class enterprise security.

Organizations must deploy combinations of security mechanisms to maximize their attack coverage. That means not only using multiple security technologies in multiple layers of the environment, but also deploying good operational practices, such as applying updates and patches in a timely manner and demanding that suppliers provide fast fixes to vulnerabilities.

From an anti-virus (AV) perspective, your multi-layer defense should include coverage at the desktop, server and network levels. Industry standards such as PCI (Payment Card Industry) have strict requirements around what AV protection must be put in place in specific verticals. And quite often end-customers want assurances you are doing all you can to prevent a security breach. As a result, a multi-layered approach makes sense from a security perspective and a business perspective, helping you mitigate risks to your organization and your brand.

Equally important, it is beneficial to take advantage of the security products of more than one AV vendor. This will ensure that, in the event of a new virus outbreak, you will have the best chance of receiving the earliest signature from one of your vendors.

[1] "Security Threat Report 2013: New Platforms, Changing Threats," Sophos, 2013.

Network
+ Security
+ Cloud

Desktop AV: A Good First Step

Desktop AV solutions address threats that originate from an infected desktop. They can help protect attacks that originate “inside” the network; for instance, when a user with an infected USB thumb drive plugs it in and uploads the malware to their computer. Organizations may also use desktop AV solutions from multiple vendors to maximize their attack coverage.

However, relying only on desktop AV provides a false sense of security. Users can tamper and disable desktop AV settings; they may not regularly update their software to protect against the latest threats. In addition, with the advent of BYOD, many of the mobile devices being used to access an organization’s resources are completely vulnerable – few AV solutions are available for iOS and Android devices, and even fewer users install these security apps on their devices. As a result, organizations need to apply multiple layers of anti-malware defense to optimize their coverage to include the wide variety of possible infection methods.

AV at the Internet Gateway: A Must

The Internet gateway is the entry point through which all Internet traffic passes, from all types of end-points: PCs, laptops, tablets and smartphones. By adding network-based AV protection, your organization can complement the security on the desktop and mitigate the risk of attacks, with a single point of control that users cannot disable or tamper with. Catching viruses as close to the security perimeter and as far away from the desktop as possible further reduces the risk of infected data reaching end users.

Not All Network-Based AV is the Same

An Internet gateway solution reduces your threat exposure in several ways. One is by limiting a user’s surfing activity to websites relevant to their work, or restricting access to categories (pornography, gambling, etc.) that are breeding grounds for malware (sometimes this is referred to as Web filtering or URL filtering). The Internet gateway should also protect you from trusted sites that may be hijacked to silently spread malware to unsuspecting visitors. Finally, it should protect your Internet resources from abuse as a result of the exchange of illegal content or bandwidth-sapping streaming media.

Some organizations deploy AV as part of their firewall/unified threat management (UTM) solution, which often doesn’t provide the additional layer of security needed to protect against today’s threats. This is because UTM-like solutions often sacrifice security for the sake of performance. When AV is turned on, it can drastically reduce device performance, so the AV detection is often configured for selective scanning, rather than thorough analysis.

Minimum Requirements of Network-Based AV

For effective protection, organizations need an in-line network-based AV solution that scales to support high-speed traffic scanning. It should also offer flexible deployment options and support AV engine choices. Additionally, it should deliver:

- **Productivity and reputation filtering** to establish acceptable user policies, limit threat exposure from notoriously malicious site categories, and filter out sites with bad reputations regardless of category.
- **Proxy filtering** to prevent users from bypassing web filtering and putting themselves and the organization at serious risk.
- **Real-time malware filtering** to catch malware as it’s downloaded from hijacked trusted sites.
- **HTTPS filtering** secures an increasingly important vector that evades most web filtering solutions.
- **Content-based filtering** to reduce the threat surface area from file types associated with malware and control bandwidth consumption.
- **Protection everywhere**, so even users outside the corporate network are fully protected, wherever they go.

Multi-Layered Security is Your Best Defense – and Your Biggest Opportunity

The combination of desktop and Internet gateway AV protection provides an aggressive, highly effective means of preventing infection. It helps organizations increase the certainty that malware will be stopped, mitigating the overall risk to your organization. More than that, a multi-layered defense will enable you to overcome overprotectiveness toward users – and embrace rather than impede BYOD and other initiatives that empower your workforce and your business.

To learn more how Blue Coat can help you add network-based AV protection to your network, visit us at www.bluecoat.com/products/content-analysis-system.

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000