COMODO
Creating Trust Online®

WHITE PAPER

Endpoint Security and the Case For Automated Sandboxing

A World of Constant Threat

We live in a world of constant threat. Every hour of every day in every country around the globe hackers are working feverishly, attacking both large and mid-sized companies across every industry and region, writing malicious code to exploit your website and computer network.

Every computer, laptop, tablet and mobile phone connected to your network represents a vulnerable endpoint for viruses, worms, spyware, rootkits, trojan horses and other malicious software – all of it designed to either disrupt your operations or gain access to proprietary data and information.

"Every computer, laptop, tablet and mobile phone connected to your network represents a vulnerable endpoint that needs to be protected"

Yet despite the constant threat, a 2013 survey by *The Small Business Authority* with a portfolio of over 100,000 members reveals that the majority of business owners are unaware of their website's security with sixty percent not concerned about vulnerabilities. According to Barry Sloane the organization's President and CEO, "Despite the rise of cyber-attacks, there is an air of complacency with independent owners thinking it will not happen to them – even though organizations experiencing such an attack run the risk of decimation."

And it's not just small businesses that are under threat. In 2012, the social networking site LinkedIn was breached with more than six million customer passwords stolen then posted to an online hacker's forum for all to see. Similar incidents have occurred at the CBS music site Last.fm as well as the online dating site eHarmony. Global Payments, a leading payments processing firm, revealed that expenses associated with the theft of an estimated 1.4 million of its payment cards was $84.4 million.

A 2012 report places the average global cost for computer security breaches at all-time high of $136 per record. Examples of stolen information include payment transactions, employee records, social security numbers, financial data and proprietary research. Add to this the loss of reputation with customers, prospects and business partners and it's easy to see why endpoint security has no longer become an option but a front-line priority.

Mobile Security and the Rise of BYOD

International Data Corporation (IDC) estimates that about half the US population owns smartphones, with the number of users expected to reach 181.4 million in 2013 and climb to 222.4 million in the coming four years. Many of those phones are used by employees to connect to corporate networks. Most of those connections are unmanaged and unsecure. The phenomenon of using your personal smartphone for business purposes is known as *Bring Your Own Device* or more popularly, BYOD.

"The average mobile security incident costs over $100,000 with many running in excess of $500,000"

With so many employees accessing their corporate networks through endpoints such as smartphones and other mobile devices, it's no surprise that the majority of businesses had a mobile security incident in the past year. A report by Dimensional Research reveals that the average mobile security incident costs over $100,000 with many running in excess of $500,000.

The rising rate of incidents is due to the fact that mobile security continues to remain unmanaged. 67% of firms surveyed allow personal mobile devices to connect to their networks. 88% of those devices are used to access corporate email. And 53% of those devices have customer data stored on them.

Companies that allow their employees to utilize personal mobile devices say the number of devices connecting to corporate networks is growing. Most estimate they have more than five times as many personal mobile devices connecting to their corporate networks than they had two years ago. Nearly all report that they've experienced problems implementing BYOD policies with securing corporate information as their greatest challenge.

Zero-Day Attacks & the Vulnerability Window

A zero-day attack targets a previously unknown vulnerability in a computer application. Because it occurs on the first day of awareness, developers have had zero time to address the problem.

Malware writers are able to exploit zero-day vulnerabilities through several different attack vectors. Web browsers are often a primary target because of their widespread distribution and usage.

Attackers can also send e-mail attachments which exploit vulnerabilities in the application opening the attachment.

Vulnerabilities discovered by hackers will be kept secret for as long as possible and will circulate only through the ranks of hackers until the software or security companies become aware of the vulnerability or the attack targeting it.

"Given the nature of zero-day attacks, it's impossible for a blacklist to be up-to-date 100% of the time for 100% of the threats"

Antivirus systems use a file called a "blacklist" to prevent such attacks by determining which programs are safe to run. The problem is that a blacklist requires that a threat has already been identified, diagnosed and the antivirus system's blacklist file updated. Given the unidentified nature of a zero-day attack, it's impossible for a blacklist to be up-to-date 100% of the time for 100% of the threats.

What this means is that no protection can be complete unless it addresses the gray area where a program is not on a blacklist as a known threat but also not on a whitelist as confirmed safe.

The Case for Sandboxing

A sandbox enables you to safely run suspected programs in a virtual environment. By sandboxing a program, you prevent it from making any permanent changes to your files or system. If the program turns out to be malicious, no harm is done.

Sandboxing is a vehicle for coping with zero day attacks that take advantage of unknown security holes in web software such as Adobe Flash, Internet Explorer and Java. Security relying on blacklists cannot protect you against these threats because the threats have not yet been identified and diagnosed. A sandbox can.

Running suspicious applications in a sandbox provides protection that a blacklist cannot. If an exploit downloads malicious software while in a sandbox it will be isolated and unable to spread.

Not all Sandboxes are Created Equal

Sandboxes can be divided into two categories: standalone solutions and those integrated into a security system. A standalone sandbox requires that the user select the programs to run in the sandbox. This type of solution is popular with companies that want to segregate high risk software such as Internet browsers. But it does not address the problem of unknown threats.

Security systems that utilize sandboxes provide an additional layer of protection by incorporating antivirus scanning to spot potential threats then place them in the sandbox. Antivirus scanners deal with unknown threats by leveraging heuristics, a process that analyzes a program's behavior as well as similarities with known viruses. If a program is considered dangerous, it is segregated and run safely in the virtual sandbox.

Heuristics work well but still fall short of being able to guarantee 100% protection. Like a blacklist, they must first detect a threat in order to deal with it – and there will always be some percentage of threats that cannot be identified by a scanner.

Why "Default Deny" is the Only Guaranteed Solution

Comodo's Detection+ is the only antivirus solution that guarantees your computer will not be harmed by a virus. Detection+ is a Host-Based Intrusion Protection Solution (HIPS) that incorporates a "Default Deny" strategy to restrict the access of *all* unknown applications to important files, folders, settings and the Windows Registry.

Default Deny refuses *all* files permission to install or execute outside of its virtual sandbox except when specifically allowed by the user or when the file appears on Comodo's whitelist. The whitelist identifies binaries that are known to be safe, such as signed code.

The benefit of Default Deny is that it closes the hole that other antivirus systems leave open thereby eliminating the risk of unknown threats. Where other antivirus solutions are limited to protecting you against files they are able to definitively identify as dangerous, Comodo's Default Deny is the *only* strategy that protects you against *any* file not fully confirmed as safe. Default Deny authenticates every executable and process running on your computer and prevents them from taking actions that could compromise or harm your files

Equally important, Default Deny enables you to access and work with the files as they execute within the sandbox's virtual environment. The result is total guaranteed protection without the loss of time, money or productivity.

ABOUT COMODO

Comodo is a leading provider of trust-based, Internet security products for organizations of every size. Comodo's offerings range from SSL certificates and antivirus software to endpoint security, mobile device management and PCI compliance. Clients utilizing Comodo security products include Morgan Stanley, Comcast, Sears, Time Warner, and Merck among others. Comodo is headquartered in Clifton, New Jersey with additional offices in the UK, China, India, Ukraine, and Romania. To learn more, visit www.comodo.com