Light Point Security

Browsing the web has never been safer

Why Web-Based Malware Is the Most Serious Threat to Your Business

Learn how your employees' web browsing activity exposes your business to exceptional risk, and why your traditional security software is no longer capable of protecting you from it.

INTRODUCTION

Web browsers are an indispensable source of information for today's workforce, as well as a large portion of the population as a whole. However, 85% of all malicious software (or "malware") is spread through web browsers. Even more alarming, 94% of fully undetectable malware is delivered via web browsing. The results of these infections can range from annoyances like adware to the complete collapse of a business.

Beyond their prevalence and high costs, these never-ending attacks have created a situation that CISOs and IT leaders must come to grips with. That is, their traditional, detection-based security products offer no protection against these new and unrecognized attacks. Therefore, a different approach is urgently needed.

This white paper examines the current state of web-based malware and the ineffectiveness of current solutions used by businesses today. It also proposes an alternative solution to the problem of ransomware and other web-based malware.

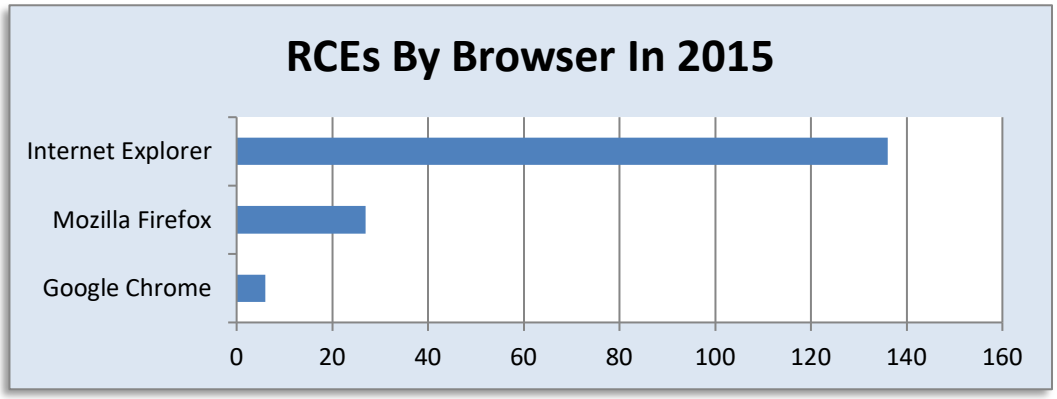
THE PROBLEM OF WEB-BASED MALWARE

Modern web browsers are incredibly complex pieces of software that are able to decode and execute HTML, JavaScript, CSS, a myriad of audio and video formats, and even perform peer-to-peer video conferencing, with more and more advanced technologies on the way. These features require millions and millions of lines of code. And most of these lines of code are used to perform the most dangerous action a computer program can perform: receiving and executing instructions from an untrusted source.

VULNERABILITIES AND EXPLOITS

When the web browser code contains a flaw in the way it decodes, validates or executes these untrusted instructions, it is known as a "vulnerability". When an attacker writes a set of instructions to take advantage of a vulnerability, it is called an "exploit". Not all vulnerabilities are equal; some are more serious than others. One vulnerability may be classified as leading to a Denial of Service (DoS) in its worst case. For example, if you visit a website that exploits this vulnerability, your browser may freeze and become unusable.

The most severe type of vulnerability is classified as a Remote Code Execution (RCE). An RCE allows an attacker to run whatever they want on a victim's computer. Exploitation of this type of vulnerability means an attacker can gain full control of the victim's computer. Then the attacker can steal any information this



computer can access like passwords, credit card details, sensitive documents, or anything else that has value. The attacker can also destroy information the computer has access to. The attacker can even use the computer to perform illegal activities like distributing illegal files, or to launch attacks against other computers.

It is important to note that just visiting a site that hosts an RCE exploit can lead to an infection. The user does not have to agree to any downloads or interact with the page at all. Just viewing the page is enough.

How common are web browser vulnerabilities? According to the Symantec 2015 Internet Security Threat Report, there were a total of 639 new vulnerabilities for the top 5 web browsers in 2014. In addition, there were another 345 vulnerabilities for the 5 most common web browser plugins like Adobe Flash, Adobe Reader, and Oracle Java.

In just the first 10 months of 2015, there were a total of 169 RCE vulnerabilities for the top three web browsers (Internet Explorer, Firefox, and Chrome). This is an average of one RCE vulnerability every 1.8 days.

THE ZERO-DAY THREAT

When a vulnerability is identified in a software product, it is up to the vendor of the product to fix the problem by creating a "patch" and then sending it out to all users of the product. If there is an exploit that exists for a vulnerability before the patch has been released, it is known as a "zero-day attack." This means users of the software have no defense against it.

There were 24 total zero-days in 2014, which is an all-time high. The top four most exploited of those vulnerabilities were either web browser or browser plugin-based, and three of those four led to complete system compromise. For the top five most exploited zero-days of 2014, it took an average of 59 days for the vendor to publish a patch.

COMMON ATTACK METHODS

Once the attackers have their exploit code, their attention turns to finding ways to get victims to load that code into their browser. They use a range of tactics to infect as many users as possible, and many of the techniques only require the user to browse to a malicious site. The following are some of the most commonly used methods to infect unsuspecting users with malware.

COMPROMISED LEGITIMATE WEBSITES

Instead of creating a brand new website and then trying to generate inbound traffic, attackers can simply take over a legitimate website that is already trusted and has existing traffic to cause it to start attacking all its visitors. How likely is this to work? According to the Symantec 2015 Internet Security Threat Report, 20% of all websites they scanned contained critical vulnerabilities which could allow an attacker to insert browser exploits into the site.

NBC.com, which has over 4 million unique visitors monthly, was hacked in February 2013 and started attacking the computers of anyone who browsed to the site. The malware infecting visitors was only detected by three of 46 anti-virus programs at the time.

WATERING HOLE

A "watering hole" is a specialized type of a compromised legitimate website where attackers target a specific group, and then identify websites frequented by that group. By infecting one or more of these websites, they can infect someone in their target group, and the infection spreads from there.

In February 2013, Facebook, Apple, Twitter and Microsoft were all infected by malware from a watering hole attack targeted at mobile app developers despite having up-to-date anti-virus. The attack used a Java plugin zero-day to exploit employees from these major companies visiting the same work-related developer website.

MALVERTISING

Another approach is known as malicious advertising (or "malvertising"). In this approach, an attacker utilizes web advertisement space from a legitimate advertising network. Attackers craft advertisements to either attack the web browser as soon as it is displayed or cause the browser to automatically redirect the user to another site which hosts the attack. Users do not need to click on the ad to be attacked.

The advantage of this method is that a single malicious ad can appear on hundreds of sites around the web, even extremely large, well-known sites. In September 2014, Cisco reported a single malvertising campaign was successful in landing malicious ads on Amazon, Yahoo, YouTube and 71 other reputable sites. This attack had amazing reach considering that Yahoo alone gets nearly 7 billion visits a month. As soon as the ad was displayed, the browser was automatically redirected to a dedicated attack site.

The threat of malvertising is only going to get worse. The infection rate from malvertising increased 325% from 2014 to 2015.

PHISHING

Another method of attack is phishing campaigns via email malware. For email malware, attackers have two choices. They can include a malicious attachment in the email and try to convince the recipient to download and execute it, or they can include a link to a malicious website and try to convince the recipient to click on it to visit the site. In November 2014, 41% of all email malware included a link versus an attachment.

IMPACT OF INFECTION

After a data breach, businesses are on the hook to pay to investigate the breach, provide credit monitoring services to its customers, increase call center staffing, and pay legal and professional services. According to the Ponemon Institute 2015 Cost of Data Breach Study, the average cost of a data breach is $3.79 million worldwide and $6.5 million for US companies specifically. However, enterprises in heavily regulated industries such as healthcare, pharmaceutical and financial services have substantially higher costs. These costs don't even include the immeasurable damages like public humiliation and the loss of trade secrets.

Malware infections affect everyone, but small to medium sized businesses suffer the most. 60% of all targeted attacks are directed towards small to medium sized businesses. And because small businesses are not as equipped to handle the unexpected burden of a data breach like larger companies are, 60% of SMBs that are breached go out of business within 6 months.

EFFECTS OF MALWARE

Once malware gets a foothold into your network, the attackers have many options on what to do next. The effect can range from mild annoyances to a complete collapse of your business. This section highlights two of the most common repercussions to a business after malware breaches their defenses.

RANSOMWARE

Ransomware is a problem that's all too familiar to many CISOs and IT leaders. It's a special type of malware designed to extort money from its victims. Ransomware is not new, but a few years ago, a new breed of ransomware that encrypts its victims' files started circulating on the internet. The crypto-ransomware began generating significant income for the attackers, so in 2015 they invested more energy into distributing it relentlessly. The crypto-ransomware angle has been successful because the ransom amount isn't prohibitively expensive, and because the use of public key cryptography means there is no other way to recover the files. If a business is infected with crypto-ransomware and they do not have backups of their files, their only options are to either pay the ransom or lose their business data forever.

> *Cyber criminals to collect $1 billion in ransomware payments in 2016.*

There were 729,000 ransomware attacks per month in 2014. The total damages caused by ransomware in 2014 were $8.8 million. However, in 2015 the damages inflicted by just one ransomware variant (CryptoWall v3) was a staggering $325 million. And according to the FBI, cyber criminals are on pace to collect $1 billion from ransomware payments in 2016.

DATA THEFT

One of the most common repercussions for a business infected with malware is data theft. Targeted malware can be used to steal intellectual property and trade secrets, tax records, legal documents, private communications, source code and anything else of value to a business. While any of these can be immeasurably destructive in the wrong hands, the most publicized type of data breaches are those in which large amounts of sensitive customer information are stolen. Customer information like Social Security numbers and credit card data can be stolen en masse by malware, which the attackers then sell on the black market.

The worldwide average financial cost for lost or stolen customer information is $154 per record. For companies in the US specifically, that cost is $217 per record.

TRADITIONAL DEFENSES

There are many products on the market to combat the threat of web-based malware. This section is a survey of the most common types, along with a discussion of the biggest weakness of each approach.

ANTI-VIRUS

The most widely used type of product to protect computers from malware is anti-virus (AV). AV works by comparing files against a large database of known malware signatures. The weakness of AV is that if a piece of malware is unknown, AV will not detect it. Malware authors employ simple techniques to automatically rearrange the contents of malicious files, so each new copy has a new signature. Because of this, AV vendors have seen an explosion of new malware variants for which they must find, study, and produce signatures. Symantec reports identifying 317 million new malware variants in 2014, up from 252 million the year before.

There is always a delay from the time that each new variant is created before a specific AV product detects it. A study in 2014 by Lastline Labs showed that two months after a variant was created, one third of AV products still failed to detect it. Even after 365 days, no single AV product detected all malware variants in the test.

While AV is great at finding and removing known malware, it is simply not reliable enough to be used as the only protection against malware.

WEB CONTENT FILTERS

Another solution commonly seen is web content filters. A web content filter is usually an appliance like a proxy or a firewall that all web browser traffic is routed through. Every time a user browses to a website, the content filter will make a decision about whether that navigation should be allowed. The vendor of the content filter must continually update the appliance with a list of known malicious websites so that users can be protected from them.

Web content filters suffer the same weakness as AV. Their list of known malicious sites will always trail behind as new sites are created. McAfee reports identifying 59 million new malicious URLs in just the first half of 2015. Even worse, legitimate, trustworthy sites are regularly exploited to start attacking visitors. These sites may also

display malicious ads sporadically. This makes it impossible for a web content filter to have a 100% accurate database of malicious websites.

Because of this weakness, enterprises will often configure the content filter to block much more than just known malicious websites, and instead choose a small set of websites that their users may visit. This leads to employees being frustrated by being blocked from accessing sites they need to visit, and it still does not solve the problem of exploited trusted websites or malvertising.

MALWARE ANALYSIS CONTAINERS

Yet another solution to this problem is to use virtual machines or sandboxing software to analyze a file or website to determine if it is malicious or not. These types of products will intercept files or website requests, and open them in a virtual machine or sandbox. The virtual environment is monitored for things like file system changes and new processes that would indicate that something malicious has happened. If this is detected, the file or website is classified as malicious and access is blocked. If after a set time limit (on the order of several minutes) no malicious activity is seen, the file/website is classified as safe, and access is granted.

There are a couple of weaknesses to this approach. First, malware can be written to detect if it is executing in a virtual environment. If it detects this, it simply lies dormant. As a result, these products would see no malicious activity, and mark the file as safe - passing it on to the user, where it would become active and infect them. In 2013, 18% of malware could detect if it was running inside a VMWare virtual machine, but by the beginning of 2014, that number had jumped to 28%.

A second weakness to the sandboxing approach is based on the time limit. In a computing theory known as “The Halting Problem”, it was proven that it is impossible to create a general algorithm to determine if a program will ever finish running. This means these products can’t know how long they should watch a suspect file before they can safely say whether it will ever do anything malicious. Because of this, they set a reasonable time limit to wait, such as four minutes. Malware can simply use a longer dormancy period before performing malicious actions, and they will have a very high likelihood of being cleared by the security product.

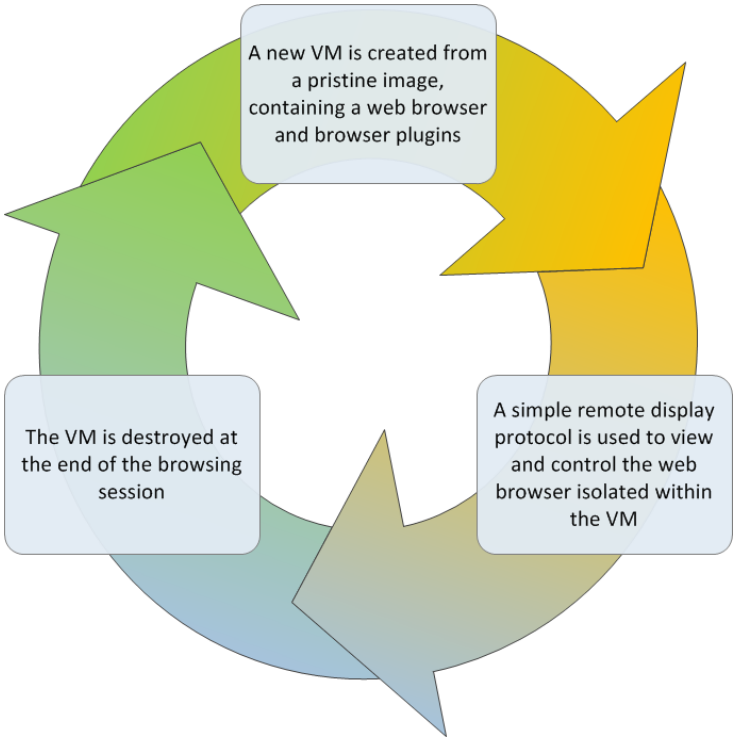
DEFEAT RANSOMWARE AND OTHER WEB-BASED MALWARE WITH ISOLATION-BASED SECURITY

The core weakness of existing solutions is that they are based on detection. A detection-based security product is only as strong as its detection algorithm. When attackers employ techniques to evade detection, they will defeat your security. As mentioned before, they can do this by simply mass producing hundreds of millions of new malware variants and tens of millions of new malicious websites a year.

Because of the shortcomings in detection-based security, we must move away from detection to a better solution - isolation. Isolation-based security is based on the premise that if dangerous tasks (like web browsing) happen in a separate, disposable environment that contains nothing of value, the inevitable malware infections will not have the ability to cause any damage.

An ideal solution to the problem of web-based malware would follow this process:

1. **Creation:** A full featured web browser and its plugins are loaded into a virtual machine (VM).
2. **Usage:** A limited but efficient remote display protocol is used to view and control this web browser from the user's computer.
3. **Cleanup:** When the user finishes their browsing session, the entire VM is destroyed, including all files and processes. This is critical to fully eliminate any possible infections that may have happened within the VM. This must happen after every session, and must not depend on a detection algorithm deciding if the VM has been infected or not.
4. **Rebuild:** After a VM has been destroyed, it can be replaced with a fresh, new VM created from a pristine, read-only image.



BENEFITS OF THIS APPROACH

There are several reasons why this approach is an ideal solution to the web-based malware problem.

ALL WEBSITES CAN BE VIEWED SAFELY

Any website can be viewed safely. Because safe websites and malicious websites are treated in exactly the same manner, it is no longer necessary to care if a site is malicious or not. In either case, no website content gets delivered to your computers.

INFECTIONS CLEANED AUTOMATICALLY WITHOUT DETECTION

Any potential malware infections that happen as a result of web browsing are cleaned automatically, without the need for detection. When the VM is destroyed, malware infections are removed as well. If the VM is always destroyed after the browsing session is complete, your security is not dependent on the accuracy of a detection algorithm. Malware infections are short-lived, and always contained within a disposable environment that holds nothing of value.

TRUSTED CONTENT MEANS NO CHANCE OF INFECTION

Untrusted and dangerous datatypes are converted to trusted, safe datatypes. Web browser traffic is dangerous because it is created by untrusted third parties, and the format is so powerful. Common web content like JavaScript, Flash and Java are entire programming languages, which gives attackers enormous power and a large attack surface.

The remote display protocol takes only the raw visual output from the browser, and passes that along to the user. With this method, the user's computer only has to parse a simple datatype that is produced by a trusted remote display server.

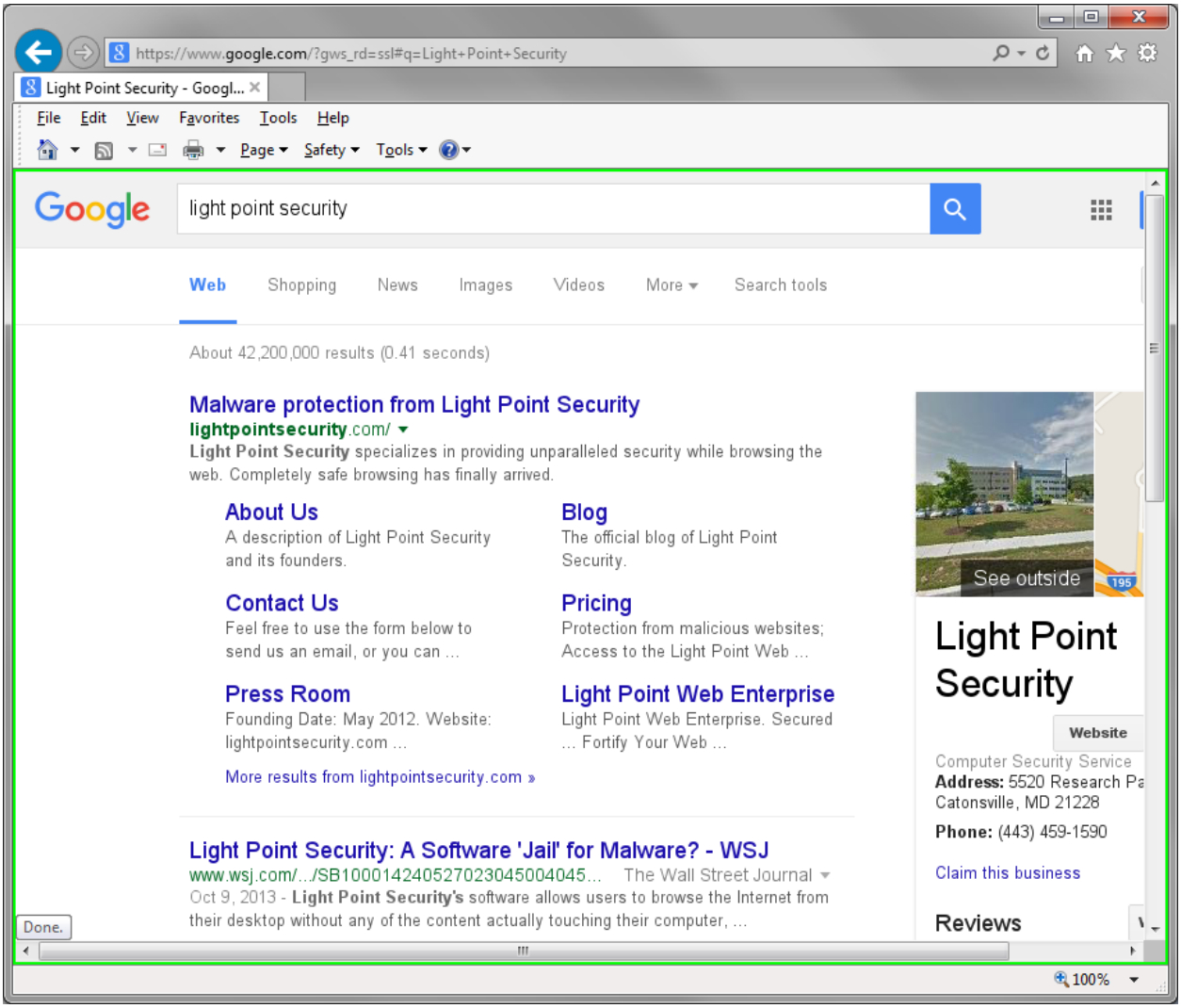
INTRODUCING LIGHT POINT WEB – AN IDEAL SOLUTION FOR ENTERPRISES

The Light Point Web Full Isolation Platform™ was designed by former National Security Agency (NSA) cybersecurity experts to meet these objectives in a user-friendly way. After decades of real world, hands on experience protecting national security systems at the highest level from cyber attacks, the founders of Light Point Security applied what they learned at the NSA to build a forward-looking, proactive solution to preventing malware attacks based on the idea of "what would it take to stop us?"

> *"We had problems with our staff introducing malware into our corporate network through the use of their personal email. Light Point Web allows us to very easily isolate our corporate network from these risky websites, while still making these sites available to our staff in a very user friendly way."*
>
> *Chief Information Officer*
> *Large specialty hospital*

SEAMLESS INTEGRATION

The Light Point Web Full Isolation Platform integrates seamlessly into standard web browsers such as Internet Explorer, Firefox, Chrome and Safari, so users do not need any training, nor do they need to change their behavior to use it. With Light Point Web's full featured browsing, users can continue to click links, enter URLs, go back and forward, copy/paste, and perform all other browser activities with their existing browser just like they always have. Light Point Web also delivers excellent performance, so even videos play smoothly.



Internet Explorer using Light Point Web to view google.com

UNMATCHED SECURITY WITH FULL ISOLATION

Light Point Web uses remote servers to host the virtual machines so user computers are totally isolated from any threats encountered by web browsing. By employing full isolation, Light Point Web offers the highest level of security possible.

The data sent to the client computer contains no web content like HTML, JavaScript, or Flash. Only raw graphical commands are sent to the employee's computer, such as "draw a red rectangle" or "draw a blue line". These commands are composited by the client software to produce an image that looks exactly like the real website. As the contents of the website change due to scripts or user interaction, the server sends more graphical operations to the client to keep the composite image up to date.

These screen updates happen so fast that they are unnoticeable to the user, all while using minimal network bandwidth.

UNMATCHED PERFORMANCE WITH SIMPLE BUT HIGHLY EFFICIENT NETWORK PROTOCOL

Light Point Web's remote server design also provides excellent performance by reducing the resource load on endpoint computers. Virtual machines require high amounts of physical resources. Light Point Web removes this burden from the user's computer and centralizes this load on server hardware, where such requirements can be shared across many users.

The protocol between the employee's computer and the virtual machine is extremely efficient. This allows videos and web page animations to appear crisp and smooth. The websites respond to users' mouse movements, clicks and key strokes just like if the websites were running on their local computers.

RANSOMWARE PREVENTION

Light Point Web prevents ransomware from infiltrating your corporate network through malicious websites, malicious browser-based downloads, and malicious links in email clients.

Additionally, the Light Point Web Full Isolation Platform provides protection from ransomware introduced through other means, such as an attachment in an email client, or even a USB stick. Before ransomware starts encrypting files, it contacts a command and control server in order to request a public key to use to encrypt your files. Organizations that use Light Point Web can combat this. Firewall rules can, and should, be set up to block all network traffic from the endpoint computers to the internet. The endpoints only need to access the Light Point Web server, and only the Light Point Web server needs to access the internet.

This setup will block ransomware from reaching their command and control servers, while allowing employees to browse the web. The Light Point Web server is not a web proxy, so malware is not able to use it to communicate outside of your network.

DATA LOSS PREVENTION TO STOP DATA LEAKAGE

In addition to preventing malware from getting into your corporate network, Light Point Web also prevents PII and other sensitive information from being leaked out of your network.

Light Point Web's upload policy lets administrators specify which users may upload which types of files to which websites. Furthermore, Light Point Web logs all file uploads for compliance monitoring and auditing.

Additionally, Light Point Web offers a copy/paste policy. This lets administrators control which users are permitted to copy and/or paste to which websites. By blocking paste operations and file uploads, it becomes infeasible for an employee to accidentally or intentionally exfiltrate large amounts of sensitive data.

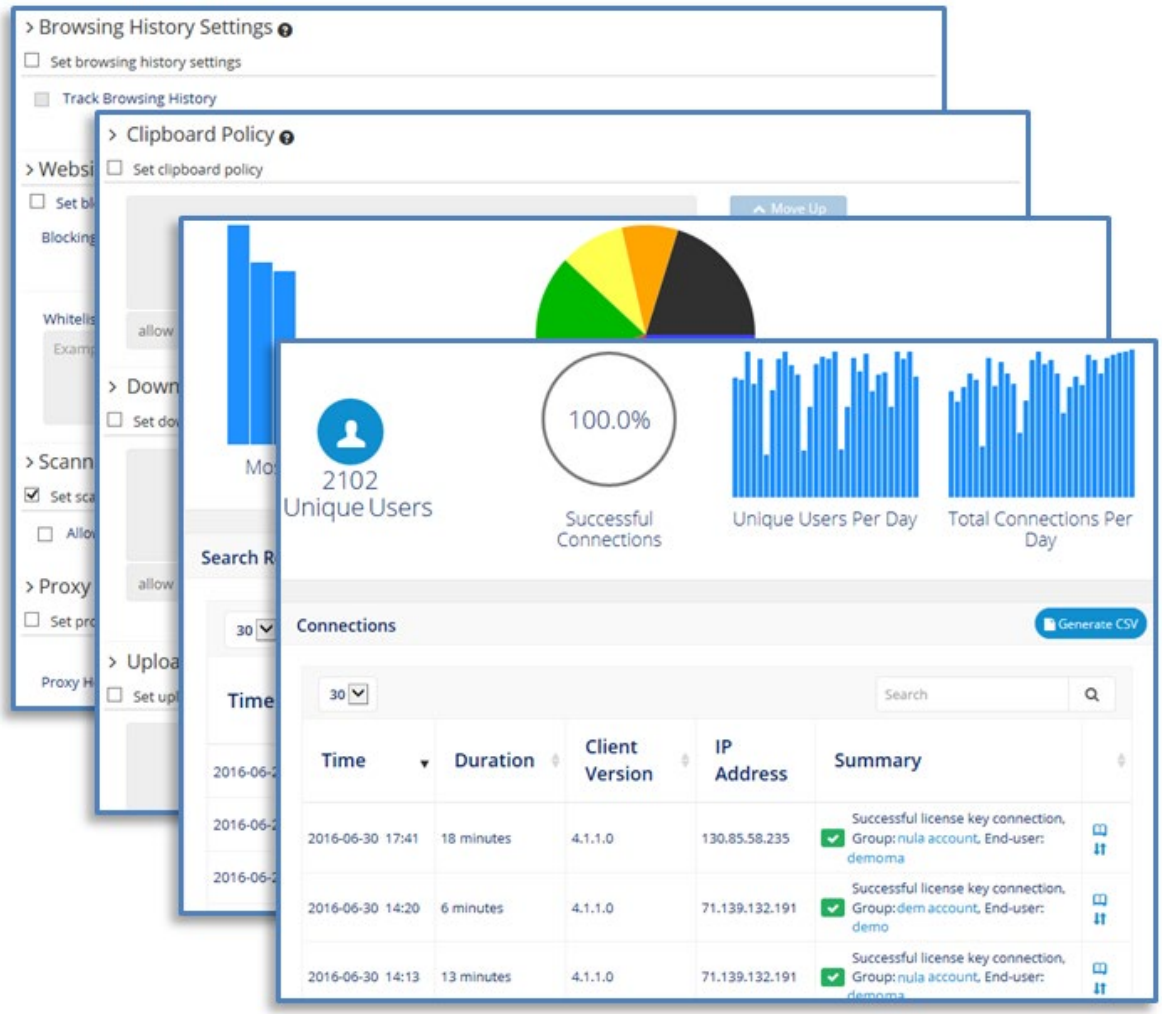
It is important to mention the flexibility of the policies in the Light Point Web Full Isolation Platform. They are not all or nothing controls. With Light Point Web, uploads, downloads, copies, and pastes can be allowed for certain users, certain file types, or for trusted sites, while blocking these operations everywhere else. This strikes the perfect balance between usability and security.

AUTOMATIC AND INVISIBLE CLEANUP

After a user finishes a Light Point Web browsing session, the VM they were using is automatically destroyed. All files such as cache files and any potential malware infections are destroyed with it. The VM is then rebuilt using a pristine image, so it can be used for the next browsing session. This happens invisibly with no interaction required by users or administrators.

POWERFUL USER BEHAVIOR ANALYTICS AND REPORTING FOR INSIDER THREAT DETECTION

The Light Point Web Full Isolation Platform provides powerful data analytics into user behavior and enterprise-grade policy management. Easily manage everything your employees do online and audit all online user activity with Light Point Web's insightful reports to prevent insider threats, discover unproductive employees and ensure compliance monitoring. See websites employees visit and how much time they spend on them, view a full audit trail of all downloaded and uploaded files, get details about all blocked malicious downloads, and much more.



AN ELEGANT SOLUTION TO A DIFFICULT PROBLEM

The end result of this combination is a security product that solves the difficult problem of web-based malware in an elegant way. Users of the software continue to use their standard web browser, but web content no longer reaches their computers. Web-based malware is trapped in an environment away from anything of value, and is destroyed automatically with no need for detection.

CONCLUSION

The problem of web-based malware is large and growing. Furthermore, traditional, detection-based solutions to this problem are becoming less effective with each passing day. However, a new isolation-based approach to avoid the weaknesses of these traditional solutions exists.

The Light Point Web Full Isolation Platform implements this new approach. Through the adoption of the isolation-based strategy, Light Point Web allows employees to visit any website safely, with no need for malware detection.

To learn how the Light Point Web Full Isolation Platform can protect you, contact Light Point Security:

Web: http://lightpointsecurity.com
Email: sales@lightpointsecurity.com
Phone: +1-443-459-1590

To join the conversation, follow Light Point Security:

Twitter: http://twitter.com/LightPointSec
LinkedIn: http://www.linkedin.com/company/light-point-security-llc

Sources:

1. Symantec Internet Security Threat Report, April 2015
2. www.cvedetails.com
3. McAfee Labs Threats Report, August 2015
4. labs.lastline.com/lastline-labs-av-isnt-dead-it-just-cant-keep-up
5. www.compete.com
6. money.cnn.com/2013/02/22/technology/security/nbc-com-hacked-malware
7. www.reuters.com/article/2013/02/20/us-apple-hackers-idUSBRE91I10920130220
8. blogs.cisco.com/security/talos/kyle-and-stan
9. Ponemon Institute 2015 Cost of Data Breach Study
10. Palo Alto Networks "Modern Malware Review Report"
11. Sophos Labs "The Four Rules of Complete Web Protection"
12. Cyber Threat Alliance "Lucrative Ransomware Attacks: Analysis of the Cryptowall Version 3 Threat"
13. National Cyber Security Alliance. "America's Small Businesses Must Take Online Security More Seriously."
14. Cyphort – "The Rise of Malvertising"