fireglass

THE CHALLENGES OF PROTECTING USERS

White Paper

It is often said the employees are an organization's most important asset, and as such the role of information technology is to make the end-user as productive as possible. However, employees and their devices are often the organization's soft underbelly from a security perspective. Organizations struggle to control all end-points and prevent potential harm. This creates startling conundrum: users require access to websites, emails and documents in order to be productive, but that same access is often the greatest security challenge an organization faces. End-users face the threat of malware infection and social engineering attacks such as Phishing, and existing solutions often fall short in protecting them.

Background: users and the threats they face

Despite becoming an area of board-level concern and strategic investment, Information security teams have been unable to stem the tide of data breaches and security incidents. This comes not because of lack of expertise or diligence, but rather because the tools organizations invest in all rely on **detection.** Tools such as Secure Web Gateways, Next Generation Firewalls, Network Sandboxes, and end-point protection solutions all rely on the ability to differentiate malicious content from legitimate content. But detection by its very nature is always **behind the curve** as attackers innovate and adapt. As security solutions evolve, advanced detection heuristics often come with the burden of **false-positives**, and because of their complexity often cannot be deployed in real-time and thus not able to stop damage before it's done. Because of these limitations teams are forced into a cycle of constant **updates and tuning**, and the layering of multiple overlapping solutions and escalating costs and operations.

Because of the inherent unreliability of detection, security conscious policies often restrict access to resources. This however lowers productivity by breaking legitimate traffic, and causes security to be a barrier to new functionality requirements and technologies. In addition, information security teams carry the additional need to deal with exceptions to the restriction policy which cause increasing management complexity in addition to operational overhead and lost productivity.

In addition to attacks, organizations attempt to prevent **negligent behavior** through **education** and **policies.** But it has been shown that education provides diminishing returns, and a significant segment of the population never internalizes these messages. In addition, users often attempt to skirt policy in the name of productivity: in order to get the job done.

The Fireglass Threat Isolation Platform

The Fireglass Threat Isolation Platform eliminates common attack vectors against web browsers and applications. Fireglass executes and renders all potentially malicious content within secure containers, and sends a safe visual feed to the end-user without altering user experience. While requiring no client installation,it is compatible with all browsers, devices, and operating systems. Normally an attacker can infect an end-user through malicious content on web-sites such as flash, Javascript, or code that exploits vulnerability in the browser. With Fireglass none of the original content is sent to the end-user, and all attacks end at the Fireglass platform itself.

This means that Fireglass can protect many forms of attack, including:

- **Drive-by infection attacks, malvertising, Water-holing, or other attacks targeting browser or application vulnerabilities**
- **Attacks on platforms such as Flash or Java**
- **Javascript or HTML attacks such as XSS, etc**
- **"Social Engineering" attacks such as Phishing**
- **Malicious exfiltration or command and control of already existing malware**

However, this protection comes with no change to user experience, no client installation and without the onerous cost of alerts, false positives, and undue restriction.

Unlike detection where everything is risky, with isolation you fear nothing.
This results in a solution that allows you to:

Secure your organization with a future proof solution by eliminating the surface area of attacks, ending the arms race between attackers and defenders

Enable users to engage in activities or to leverage technologies previously considered too risky

Simplify your IT environment by consolidating existing solutions, and reducing operational overhead of alert management, exception handling, and policy management.

In the remainder of this document we will explore these threats in greater detail and explore how the Fireglass Threat Isolation platform prevents them.

Protecting users from drive-by infection or malvertising

Drive-by infection is currently the largest vector for malware infection and delivery, accounting for 43% of all infections (Verizon 2014 data breach report). Furthermore 85% of malware are hosted on legitimate sites (Websense), or served through legitimate sites. This has recently come to public notice as a rash of malicious infection through ad syndication networks (malvertising) on popular news or content sites. In addition, attackers have started to target specific groups by compromising sites that they are likely to visit (commonly called a "watering-hole" attack). Currently the only defense against drive-by infection is keeping end-points patched and up-to-date with security updates, and search for blacklisted patterns of vulnerability. However, these solutions are often behind the curve and cannot detect previously unseen attacks. They also trap security teams in an endless scramble to keep software and signatures up-to-date.

The Fireglass solution

With Fireglass Threat Isolation Platform no active content (such as Adobe Flash, HTML, Javascript or any other plugin or content) ever reaches the end-point, and cannot compromise it.

Protecting users from malicious documents or downloads

Proactively downloaded and installed malware accounts for 38% (Verizon 2014 data breach report) of malware infections. There are multiple challenges involved with mitigating the risk of downloads without harming productivity: real-time scanning engines such as Anti-Viruses are mostly irrelevant today as 90% (Verizon) of malware is unique to each organization, and network sandboxes cannot stop infections in real time as they need to run the malware and wait for certain behavior (most advanced malware can also detect sandboxes). This causes these solutions to alert after the fact when users have already been breached and damage has already been done.

The Fireglass solution

Fireglass eliminates the potential surface area of attacks by not requiring download in order to view, edit and be productive with common file types: this is accomplished by integrating a full-featured viewer into the Threat Isolation platform , so that the content of files such as PDFs or Microsoft Office files are relayed to the end-point as a visual stream just like other active content originating in the Internet.

For files that do need to be downloaded Fireglass offers a great advantage: all downloads are fully downloaded to the Fireglass platform and can be scanned or modified before the download connection to the end-user's browser is initiated. This allows for Fireglass to integrate multiple possible solutions for downloads:

1. Sanitizing files such as PDF or Microsoft Office files by creating new "known good" files and importing text and images from the original document into the "known good" document and having that document sent to the end-user's browser.
2. Sending files to a sandbox for analysis and waiting for a response prior to sending the file to the end-user which can, in the meantime, view the content on Fireglass' platform.
3. Scanning the file with multiple detection engines using threat intelligence services.
4. Storing the files in a queue for manual review.

Any combination of approaches can be combined together or implemented separately

Protecting users from Phishing and other "social engineering" attacks

Phishing and social engineering are a significant and growing part of targeted attacks. Social engineering attacks are usually addressed through education and content filtering. However, compelling research that suggests that education has reached the limits of its efficacy with 23% of users opening phishing emails and 11% opening attachments. Likewise, because of their targeted nature and short life-span, reputation based controls are mostly ineffective, and textual filters cannot differentiate between targeted emails and legitimate business correspondence.

The Fireglass solution

The Fireglass security policy operates at the browser level, as such it can enforce controls on communications with web sites that are at the intersection of human behavior and the browser rendering. By employing Fireglass, organizations can prevent Phishing by enacting controls such as the following:

1. Prohibiting users from typing in password fields, when the site is not SSL protected (less than 1% of Phishing sites employ SSL) or not in a whitelist of allowed sites.
2. Checking user's typing against Active Directory or previously seen credentials and preventing submission of established credentials to external sites.
3. Applying regular expressions to users typing or copy/paste operations to preclude submission of information such as credit card numbers.

As such, the Fireglass approach neither relies on detection, nor on education to curb the efficacy of Phishing and other social engineering attacks.

Protecting the organization from existing malware on end-points

It is often impossible to completely prevent malware on organizational assets, as the infection may happen outside the network or control of the organization. In order to be effective malware needs to be able to retrieve information from the infected machine, and transfer it to an internet site (C&C), or provide a back-channel for the attacker into the organization. Current web security gateways let an average of 90% of this traffic (as it appears to be normal web-browsing) through and do not impede the effectiveness of the malware.

The Fireglass solution

The Fireglass Threat Isolation platform breaks the attempts of malware to communicate outside the organization, as it does not relay HTTP/HTTPS traffic, but rather accepts communication only in the form of user gestures (such as mouse movements and key clicks) performed by a human being. Any unauthorized program trying to communicate directly over HTTP/HTTPS will simply be blocked by Fireglass. In addition, automated transactions such as those that occur in the Man-in-the-middle or Man-in-the-browser attacks would fail as well. Indeed, even most forms of key-loggers and form-grabbers would fail to retrieve information as there is no HTTP communication with the application, including form submission.

Protecting users from malicious emails

Security of email applications is often considered more mature and effective than the "wild west" of web browsing. This is due to the more technologically limited elements of the medium as well as its less interactive nature. However, many challenges remain in handling of emails and it remains a significant vector for malicious activities. These activities can be roughly divided into 3 categories:

1. Malicious email attachments
2. Links to malicious sites hosting drive-by infection or malware downloads
3. Links to Phishing sites

When it comes to attachments or downloads, organizations have a trade-off between the productivity of allowing employees to communicate and receive files from the outside world, and the limited effectiveness of detection solutions for malware in popular document formats.

"spear-phishing" is sent in low volumes and is customized for its specific intended target. As such it is often impossible to differentiate it from the normal email correspondence of the intended victim.

The Fireglass solution

Fireglass protects users from malicious attachments by isolating the files behind the Fireglass platform. Fireglass replaces the attachment with a link to view or download the file through the Clientless Isolation Platform. Fireglass then replaces the attachment with a link to view or download the attachment through the Fireglass document isolation or download policies. Phishing links are addressed through normal browsing protection as described above.

Contact us

www.fire.glass +1-(650)-50-FGLAS (34527) contact@fire.glass

4 World Trade Center, New York, NY 10007