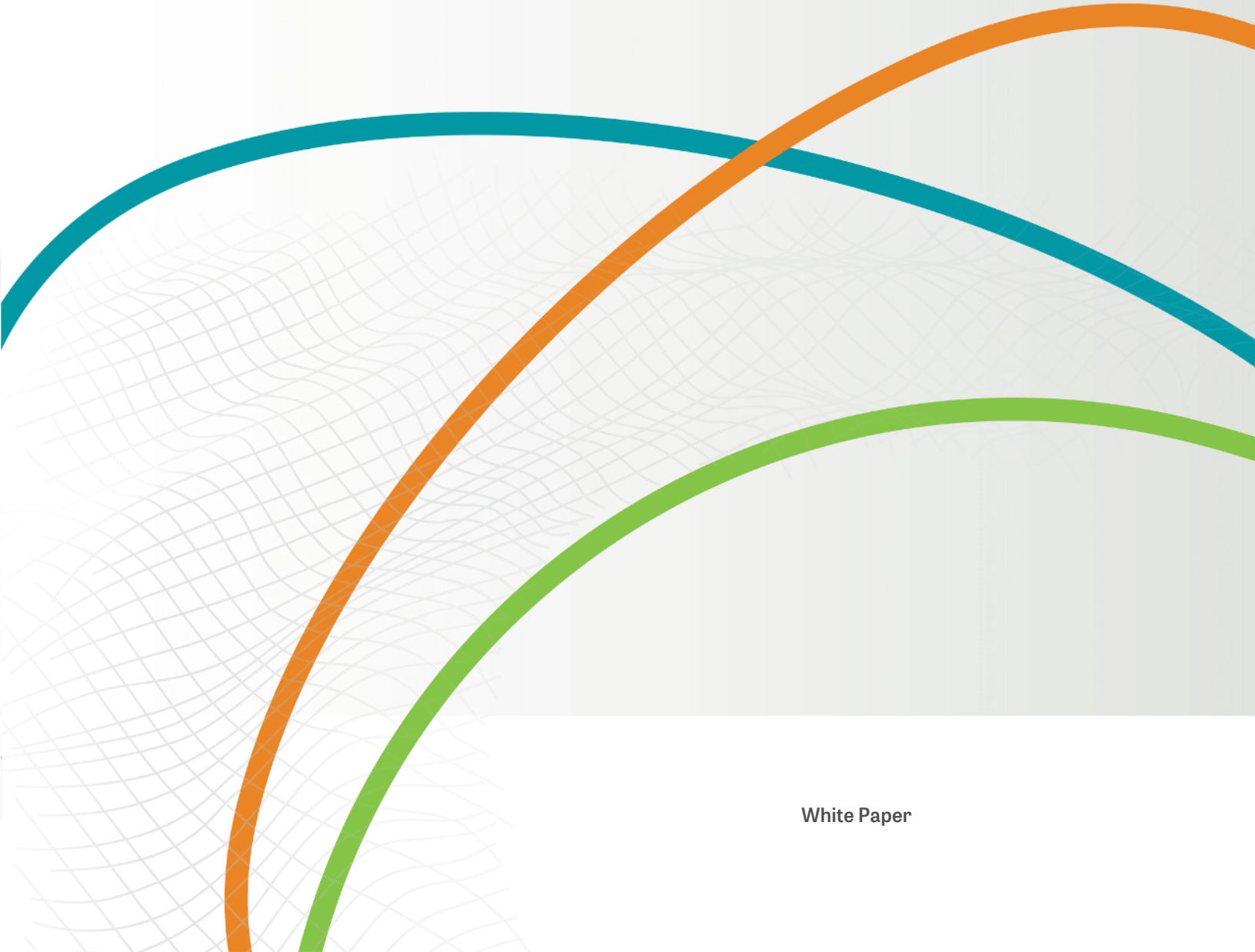
Fight Malware, Malfeasance, and Malingering with F5

F5 Secure Web Gateway Services give organizations control and visibility to secure their users' Internet usage. The solution helps protect against malware and data loss, ensure compliance, and improve productivity.



White Paper

Introduction

Every year brings an even more extreme set of threats to the enterprise than the last. Spam email used to be the number one headache. Now it's been replaced with malware, spear phishing, and the infamous spin-off of the two, the advanced persistent threat (APT).

Employee Internet usage is also changing in ways that challenge traditional enterprise security. Workers are often connected minute by minute, and the traffic is increasingly encrypted. This is great for privacy but not so good for visibility. After all, organizations still need to protect the business and make sure their employees comply with usage policies and appropriate standards.

If not managed effectively, all of these issues have the potential to be very costly for the organization. Whether it's a direct financial impact from data loss or the liability or loss of employee productivity due to inappropriate use of the Internet, failure in outbound security can be expensive.

The good news is that enterprises have a range of mitigation options, from integrated intrusion detection systems and intrusion protection systems (IDS/IPS) to next-generation firewalls (NGFW). The question, then, is which solution offers the organization the greatest protection and control over its web security without adding complexity or unnecessary costs.

F5 Secure Web Gateway Services provide both the broadest and the deepest coverage available to enterprises today. It's a comprehensive solution that ensures organizations gain the visibility and control they need to prevent asset loss, maintain compliance, and increase employee productivity.

Protecting and Managing the Changing Workforce

Organizations are seeking greater control over their outbound security infrastructure as they face growing security challenges. They need to prevent data loss and ensure compliance. They're responsible for enforcing HR and IT policies that protect the business and promote employee productivity. And they need to do all of it without increasing cost or complexity.

These issues have always existed, but they present new challenges as the next generation of employees (the Millennials) brings a different scope of Internet usage into the workplace. Previously, employees used the Internet on an ad hoc basic. Now, some workers are minute-to-minute connected. Vine. Social media. Tweeting. The dichotomy that many Millennials love to share their lives on social media, yet also defend Internet privacy, is more than just an academic observation.

The push for increased confidentiality and the use of SSL everywhere has made it more difficult for enterprises to monitor Internet usage. Encryption renders traditional solutions blind. An organization can load an IPS policy onto its firewall, but it can't see what's in the SSL traffic. Just as Internet usage in the workplace is exploding, web security solutions are losing the visibility they need to help the organization protect against malware, data loss, and inappropriate use.

Guest network access is another rising trend that businesses face. People simply expect to have free wireless access everywhere—not just in coffee shops and hotels but in small businesses and enterprises as well. It's become a "must do," yet "free" WiFi isn't free for the host. There are liability issues and user conflicts. If one guest is trying to surf offensive sites next to another or hacks into a third party, the organization has to protect itself from liability.

While there are solutions that can help mitigate some of these risks, it's more critical than ever for enterprises to have a comprehensive and streamlined way to maintain visibility and control over their outbound security infrastructure.

> "Complex enterprises with large mobile populations (where Web security as a service delivery will be required), complex demilitarized zone/website/data center firewall requirements, and complex/granular Web user security requirements should keep NGFW and SWG products and services separate, but ensure that reputation services can be integrated across the two security control areas."[1]

F5 Secure Web Gateway Services

F5 Secure Web Gateway Services give organizations a strategic point of control in the network to efficiently manage these challenges. They help organizations prevent asset loss, increase employee productivity, and ensure compliance for their business.

Prevents Asset Loss

The F5 solution provides a breadth and depth of coverage that gives enterprises comprehensive web security to protect their assets from malware, spear phishing, and APT attacks.

The broadest coverage

Blocking malicious URLs is crucial to the retention of corporate assets. A secure solution does this in two ways. First, it prevents connections to sites that host malware. Second, when malware does make its way into the enterprise, it prevents the exfiltration of corporate assets to a malware drop site.

Secure Web Gateway Services use the most comprehensive categorization database to block access to more malicious sites than any other solution. The threat intelligence behind Secure Web Gateway Services analyzes more than 5 billion web requests every day to produce a categorization database of 40 million website URLs.

The deepest coverage

Exfiltration of corporate data by malware is a top challenge for enterprises. Even though F5's technology clearly has the broadest coverage across malicious websites, it does not sacrifice its depth of security. Secure Web Gateway Services have individual payload security classification engines that examine specific threat surfaces such as:

- Exploitable Java platforms
- Malicious iFrames
- Keyloggers and spyware
- Infected Adobe PDF
- Vulnerable Flash applications
  By inspecting both payloads and web pages, the solution keeps malware out and corporate data in. Unlike other solutions, Secure Web Gateway Services combine categorization and malware analysis on a single platform to streamline the security infrastructure.

  Other solutions try to consolidate malware detection capabilities using multiple point products. This results in the need for enterprises to purchase an antivirus detection device with a separate license and pair it with another gateway to fill the gap for malware detection. Capital and operating expenses increase along with deployment complexity.

  By covering the full depth of potential threat surfaces with one complete solution, Secure Web Gateway Services offer a simpler, more cost-efficient, and more secure way for enterprises to protect corporate data.

Interoperation with data loss prevention solutions

Secure Web Gateway Services interoperate with today's leading data loss prevention (DLP) solutions and assist the critical DLP infrastructure through the following enhancements:

- Provide hardware-assisted decryption of connections and payloads, which

Why isn't a NGFW enough?

88% of outbound traffic is web.2 NGFW tries to monitor thousands of protocols, few of which are web or are used in the enterprise. The F5 Secure Web Gateway focuses exclusively on web and applies its intelligence exactly where it's needed most.

many DLP systems cannot do—or cannot do for all SSL connections.
- Pre-identify the user so the DLP solution doesn't have to.
- Preselect the connections that should be examined by the DLP. For example, if an organization allows Netflix internally, Secure Web Gateway Services can ensure that no Netflix traffic is sent to the DLP.

By applying the intelligence of Secure Web Gateway Services, organizations can dramatically reduce the amount of traffic the DLP must process. This prevents the DLP from being overwhelmed, improves efficiency, and saves the CapEx that would otherwise be required for more DLP resources.

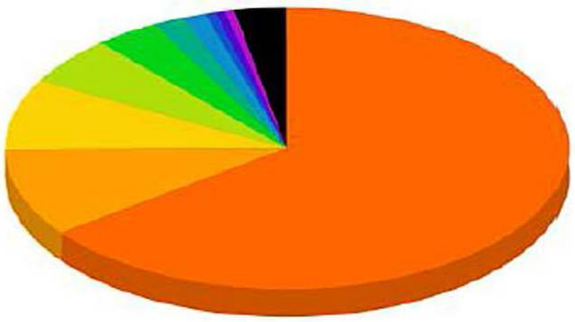
Increases Employee Productivity

HR magazine printed a particularly alarming statistic in 2013: "Around 14 percent of the workforce in the UK spend nearly 50 percent of their workday on the Internet for personal use." [3] This statistic may reflect similar malingering patterns across the world.

The F5 solution gives IT administrators the visibility they need to understand their employees' Internet usage in aggregate and on an individual basis. Administrators can use this categorization and reporting information to take steps to improve employee productivity.

Rich reporting

System administrators can use the F5 graphical user interface to view and export various security analytics reports. These reports empower administrators with total visibility of outbound and inbound web traffic, Internet use, and policy enforcement.



Details

#	Category	Request Count
1	Streaming Media	7336
2	Information Technology	1144
3	Search Engines and Portals	923
4	Advertisements	622
5	Shopping	418
6	News and Media	205
7	Internet Radio and TV	147
8	Business and Economy	67
9	Private IP Addresses	65
10	Social Web - Facebook	62
11	Others	340

Total Entries: 43

Figure 1: Rich reporting on aggregate and individual use

User identification

F5 Secure Web Gateway Services interface with an agent in the enterprise directory to map addresses to usernames, devices, and other contextual information related to network login activity. This allows administrators to see who is accessing Internet resources without requiring that they log in to Secure Web Gateway Services. They can pair this information with directory queries to configure specific policy based on a user's group membership or any other user attribute.

Bandwidth policies

A common productivity problem for organizations is the time employees spend watching videos that aren't related to their work. Secure Web Gateway Services recognize thousands of websites as entertainment sites. Administrators can use bandwidth policies to control not just access but how much access employees have to this category of websites.

For example, some employees might require periodic access to video websites to do their jobs. However, the organization doesn't want employees watching all the viral videos that would normally propagate around the office every day. Secure Web Gateway Services can enforce this policy, allowing only a certain number of users to view any one video within a period of time.

Media streaming sites like Netflix are another type of entertainment site to which Secure Web Gateway Services can control access. Organizations can block them all the time, only during regular business hours, or at other times to meet their business needs. For example, some organizations might want them available only after hours (for employees who have to be present but not necessarily engaged).

Ensures Compliance

Organizations can use Secure Web Gateway Services to create compliance zones for both users and services.

User access/SSO

Secure Web Gateway Services can be configured to interoperate with enterprise single sign-on (SSO) tools (via SAML and other technologies) to convert Internet access login into authenticated access to enterprise portals and SaaS applications. This means the enterprise gains policy-based control and monitoring of who can access which websites, at which times, and with which risks involved.

Guest access captive portals

Organizations often need to provide guests with secure Internet access, whether it's a guest wireless network or a contractor subnet for a set of independent contractors. Administrators can use Secure Web Gateway Services to authenticate guest users or, if authentication is not required, to require the guest user to accept the terms of use. Secure Web Gateway Services will then protect guest users from malicious sites and malware.

The enterprise can set different restrictions, such as removing productivity locks for wireless guests but leaving tighter restrictions in place for contractors. By using a captive portal and requiring users to comply with an acceptable usage agreement, the organization gains additional protection from liability.

Protected zones for compliance

Secure Web Gateway Services can also help organizations enforce compliance on servers as well as users. For example, the PCI DSS standard requires servers in the cardholder data environment (CDE) to go through a controlling forward proxy to access resources across the Internet (such as update services). Deploying Secure Web Gateway Services around a CDE provides this compliance while securing the outbound connections as well as the communications.

Safety as an enterprise policy

Typically, when users fail to use "safe search" mode, they can be exposed to malware and malicious URLs in their unfiltered search results. Secure Web Gateway Services can detect and block links embedded inside these search results, effectively making "safe search" a company-wide policy.

Conclusion

Changing Internet usage patterns, WiFi-everywhere expectations, and the increased use of SSL encryption for confidentiality present a host of challenges to organizations' outbound security efforts. But there's no reason organizations should sacrifice depth or breadth of security when implementing solutions to fight malware and ensure appropriate Internet usage.

With F5 Secure Web Gateway Services, enterprises can solve these challenges at a single point of control. The solution can inspect and monitor SSL traffic—an increasingly vital part of ensuring outbound security. It also helps complementary solutions like DLP operate more efficiently by offloading functions and ensuring that the DLP receives only the traffic it need to process.

By implementing a comprehensive solution that prevents users from bringing malware into the enterprise and that monitors compliance, organizations can protect their business from costly data loss and liability. F5 Secure Web Gateway Services give organizations the control and visibility they need to ensure secure and efficient outbound Internet use.

---

[1] Gartner, Next-Generation Firewalls and Secure Web Gateways Will Not Converge Before 2015, John Pescatore, Peter Firstbrook, Lawrence Orans, Greg Young, refreshed 19 September 2012

[2] Sandvine, 1H 2013, Global Internet Phenomena Report

[3] HR magazine, Jan. 2013, Employees spend up to half the working day surfing the Internet for personal use

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 www.f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com