Advanced Security
How Zscaler Tackles Emerging Web Threats with High Speed, Real-Time Content Inspection in the Cloud
A Zscaler ThreatLabZ Report

ABSTRACT
Leveraging a purpose built architecture capable of high-speed content inspection, the Zscaler solution inspects all web traffic in real-time. Content inspection occurs bi-directionally and covers not just the URL, but also all headers and the full content of all requests and responses. This level of inspection even takes place for SSL encrypted payloads. Inspection at this level is vital to ensure security on the web today, which is dominated by dynamic, user-supplied content. This is achieved without introducing noticeable latency thanks to a globally distributed architecture designed from the ground up, specifically for a Security-as-a-Service delivery model.
CONTENTS

ATTACKER EVOLUTION 2
SAAS CHANGES THE PLAYING FIELD 3
TRADITIONAL APPROACHES WEB SECURITY 3

INSPECTION 4
TRADITIONAL CLIENT-SIDE SECURITY 4
Desktop Antivirus 5
URL Filtering 5
ZSCALER’S APPROACH TO CLIENT-SIDE SECURITY 6
Destination Analysis 6
Antivirus/AntiSpyware 7
Full Content Inspection 7
Browser Control 8
Interrogator™ 9

ADVANCED SECURITY 9
NETWORK EFFECT 9
PARTNERS 9
Malicious URLs 10
Phishing 10
Botnets 10
Vulnerabilities 10
PAGE RISK INDEX 10
History 10
A New Approach 11
Control Categories 12
Scoring 13
FUNCTIONALITY 13
Botnets 13
Malicious Active Content 13
Phishing 14
Communication 14
Cross Site Scripting 14
Control Access to Suspicious Destinations 14
P2P Control 14

CONCLUSION 14
Attacker Evolution

In nature, those that adapt to changes in their environment survive and prosper. The individuals that attack computer networks are no different. The information technology environment has evolved significantly over the past decade and attackers have adjusted their tactics along the way. Attacks have shifted from servers to web applications and on to web browsers. Along the way, attackers have evolved from individuals motivated by curiosity, to well funded criminal organizations seeking profit. Unfortunately, enterprises have largely failed to keep pace and continue to use dated methods to thwart attacks.

Attackers that once targeted enterprise servers have now realized that it is far easier to exploit client machines thanks to weak defenses and naive users. Buffer overflows in publicly exposed server-side services have been replaced by multi-faceted, client-side attacks leveraging social engineering, web browser vulnerabilities and trusted, yet vulnerable web applications. Web 2.0 technologies, while empowering developers to produce intuitive, user-friendly applications, have also raised the bar on complexity, ensuring that vulnerable web applications are an accepted part of life on the Internet. The web browser has become a portal for attackers, allowing them to access sensitive data on desktop and mobile devices, while often permitting complete control of a machine as it is recruited into a botnet army. Enterprises must shift focus and adapt if they expect to defend against modern attacks.

SaaS Changes the Playing Field

Cloud delivered security or Security-as-a-Service (SaaS) solutions have begun to emerge in an effort to tackle the challenge of web browser security. SaaS solutions offer an inherent and critical advantage over traditional hardware or software based Secure Web Gateway (SWG) products. SaaS solutions are able to protect mobile devices just as easily as they protect assets on the Local Area Network (LAN). This is game changing. Enterprises are becoming increasingly reliant on remote employees and ‘road warriors’ working from laptops, tablets and smartphones. Moreover, new mobile platforms such as Apple’s iOS (iPhone, iPad and iPod Touch) do not permit applications to run in the background. Traditional host based security measures are simply no longer an option. When it comes to mobility, we’re being forced to rethink security for end users. Attackers have recognized this shift. They know all too well that remote workers are unlikely to be protected by LAN-based defenses, and mobile devices therefore constitute a ‘target rich’ environment. SaaS vendors can inspect web traffic regardless of location but only a few vendors, such as Zscaler, offer ‘true SaaS’ by requiring that no additional software run on the client device – a critical requirement for mobile devices. This not only ensures that remote assets can be protected ‘out of the box’, but also reduces the cost and complexity associated with managing the overall solution.

Traditional Approaches Web Security

Latency is the enemy of web security. If the web browsing experience is degraded by security controls, users simply will not accept the solution. It cannot be avoided. Security introduces latency, as packets must be inspected in real-time. The deeper the level of inspection required, the more CPU cycles are consumed and, as a result, the potential for slowing web traffic increases. Throughput degradation is a challenge for appliance vendors and it is exacerbated in the multi-tenant environment introduced in SaaS based solutions. Vendors recognize this and have been forced to limit the depth of content inspection in order to avoid introducing latency when inspecting web traffic. Without a high-speed, scalable infrastructure, deep inspection simply cannot be achieved. While competitors have built their
web proxy solutions on top of existing technologies in order to bring solutions to market quickly, the Zscaler infrastructure was built from the ground up with the sole purpose of creating the fastest infrastructure possible to permit deep, bi-directional inspection of web traffic.

**Figure 1 - Content Inspection Throughput**

**Inspection**
Web pages must be reviewed and evaluated in order to implement security. All security solutions do this. What is not always apparent is the depth of inspection that takes place. The deeper the level of inspection performed, the greater the risk of introducing latency to web browsing. As such, most vendors limit inspection to only what can be done quickly. URLs can be quickly matched against block lists, but such an approach offers protection only against known attacks and doesn't take into account the dynamic nature of the majority of web content.

**Traditional Client-Side Security**
Historically, enterprises have approached client-side web security by leveraging two primary technologies – URL filtering and host-based anti-virus/anti-spyware. While both remain important components in an overall defense-in-depth strategy for end-user security, these technologies alone are failing to keep up with emerging web-based threats. As noted in figure 2, both approaches have significant limitations in today's threat landscape.
Desktop Antivirus
Desktop antivirus, while enjoying nearly 100% penetration in the PC market tends to perform adequately against known threats with relatively static exploits, that situation is now the exception rather than the rule. Exploit developers regularly leverage services to monitor which antivirus vendors have deployed signatures for a given exploit variant and, when spotted, subtle changes are made to the exploit until it again evades detection. This cat and mouse game is one that will continue indefinitely and unfortunately, attackers have the upper hand as signature based antivirus can’t detect what it doesn’t yet know about.

Beyond challenges in keeping up with detecting new threats, any host based security control also suffers from the limitation that it can be disabled on the device, with appropriate permissions. This may mean that a user with administrative privileges intentionally disables an antivirus program perceived to slow down performance, or more likely is disabled or neutered by a new exploit that wasn’t caught. Gartner agrees that “signature-based anti-malware detection is increasingly ineffective against an explosion in the number of malware variants as well as an increase in the number of financially motivated targeted attacks.”

URL Filtering
URL filtering can be a beneficial productivity control, but provides limited value when it comes to security. URL filters tend to work primarily at the domain level, not at the level of individual URLs. Given the dynamic nature of web content today, it simply isn’t possible to statically categorize individual web pages, as they are generated on the fly, based on user preferences. While blocking Facebook.com may add value if a corporate policy prohibits access to social networks due to productivity concerns, it does little to secure the network from malicious web content. Attackers are no longer setting up malicious sites, hosted on domains that they control, and then trying to convince users to visit them by sending

spam email. Today, they are leveraging otherwise legitimate sites either by infecting a vulnerable web application or by abusing overly liberal rules for user supplied content. Therefore, while the domain itself may be perfectly fine, a single page or piece of content may be infected with malicious content. This situation may last for only a few hours until it is cleaned up. Simply blocking URLs and domains may catch low hanging fruit but full, real-time content inspection is required to ensure that dynamic threats don’t bypass enterprise defenses.

**Zscaler’s Approach to Client-Side Security**

There is no silver bullet when it comes to protecting end users from web-based threats. Zscaler therefore, employs a layered approach to quickly identify malicious content, regardless of end user device or location - even when the threat may not have been seen before. Our approach begins by quickly identifying threats that we already know about and moves to full content inspection to ensure that even new malware buried deep within an otherwise legitimate page doesn’t slip through the cracks. This is all achieved without introducing noticeable latency for the end user, thanks to an architecture designed from the ground up to be deployed in a SaaS model. All content is subjected to every level of inspection unless malicious content is definitively identified at a lower level. Shortcuts are not taken avoid performance hits. Such an approach is not required, due to the inherent scalability of the Zscaler Cloud.

**Figure 3 - Zscaler’s Approach to Client Side Security**

**Destination Analysis**

All security vendors block malicious sites by identifying requests to known malicious URLs. But many only provide this level of protection as it limits the level of inspection required – only the URL needs to be parsed and matched against a black list of malicious sites. For Zscaler, this is only the most basic level of protection, leveraged to quickly filter out known malicious content without the need for deeper inspection. Even at this level, however, Zscaler has some inherent advantages. As a SaaS vendor, Zscaler sees billions of web request each and every day. This provides Zscaler ThreatLabZ with a broad view of what is actually happening on the Web at any given time, including the emergence of new threats and how they are spreading. With a distributed and centrally managed global Cloud, Zscaler can identify the
presence of a threat targeting one customer and instantaneously leverage that knowledge to protect all other customers by blocking access to that same threat.

**Antivirus/AntiSpyware**
While anti-virus/anti-spyware (AV/AS) has its limitations, it has long been an accepted security solution for enterprise desktops. The same is not true when employed as an in-line solution in the majority of enterprises. One is not a replacement for the other. Rather, in combination, host and network based AV/AS solutions are complimentary and represent an important component of a defense-in-depth approach to web security. In-line AV/AS is especially important for mobile devices such as tablets and smartphones for which host based AV/AS is not even an option, either due to limited computing power/battery life, or because the mobile platform simply doesn’t allow it.

Host based AV must receive regular signature updates. Should that process be delayed or blocked altogether for a variety of reasons, a machine can become infected. In-line or network AV/AS will provide protection in situations where host based solutions are either not up to date or have been disabled. The latter is a common problem when the machine has become infected. Malicious code often seeks to disable AV/AS to ensure that subsequent signature updates do not detect and quarantine the initial infection. Employing network based AV/AS ensures that a single point of failure does not exist when detecting malicious binaries.

Implementing in-line AV/AS in a web security solution is challenging. Once again, due to the real-time nature of the web, latency can quickly be introduced when running AV/AS engines in-line. This is especially true for SWG appliances that provide in-line AV/AS using an entirely separate third party appliance, which communicates with the SWG via Internet Content Adaptation Protocol (ICAP). ICAP is a message transmission protocol commonly used to permit standardized communication between devices, but such a setup is inefficient and creates unacceptable latency for most enterprises. Zscaler has taken a different approach by implementing AV/AS capabilities directly within the gateway responsible for content inspection. Moreover, files are scanned in phases to further streamline the process. If, for example, the first 1MB of a 100MB file is found to be malicious, the file will be blocked immediately, without requiring the full download to complete. Additionally, hashing algorithms are continually employed to quickly identify content that has previously been scanned. The result is in-line AV/AS at unprecedented speed, resulting in transparent protection for end users.

**Full Content Inspection**
A typical web request leads to dozens of responses from multiple web servers resulting in hundreds of kilobytes of data. Mashups and user-supplied content ensure that much of the content received has not been vetted in any way to ensure that it is not malicious in nature. For these reasons, all web content received must be considered to be untrusted regardless of the source.

Beyond this, legitimate sites are regularly compromised and serve as a catalyst for attackers who are then able to leverage the site to attack the many trusting users visiting it each day. Attacks are also highly dynamic in nature. Two people can request the same content at the same time and one will be attacked and the other won’t. Why? Because one user is running an outdated component such as a browser plugin that is subject to attack, is coming from the geography being targeted or is just the unlucky recipient of a payload delivered at random intervals to thwart detection. Regardless, it is clear
that modern web threats require in-line solutions, inspecting the actual content being delivered to the end user. Basing security decisions solely on previously cached results is simply not enough.

Deep content inspection, which permits high-speed pattern matching of all content regardless of location, without introducing latency, is a significant but necessary challenge. Threats identified at this level simply cannot be identified ahead of time for the simple reason that they don’t exist ahead of time. Dynamic content requires real-time inspection. Deep inspection covers not just the URL, but also all headers and the full body of all requests and responses. This must also be done even when the content is in an SSL encrypted tunnel – something that could not be achieved without a global architecture of proxy technologies designed specifically for this purpose. Zscaler is able to achieve this level of inspection in a SaaS solution because the system was designed from the ground up with full content inspection of all traffic as the goal.

Browser Control
Attacks have adjusted their tactics now, rather than exploiting known web browser vulnerabilities, that enterprises tend to patch fairly quickly, attackers are instead targeting vulnerabilities in browser plugins. Unfortunately, enterprises tend to have poor patch management capabilities over browser plugins, despite the fact that employees are likely to have adequate privileges to install plugins at will.

Consider the data shown in Figure 4. It is truly frightening to see just how common it is for employees to be using browsers with outdated plugins, many with known vulnerabilities. It is for this reason that exploit kits, collections of known exploits packaged together for ease of use that are bought and sold in the underground, target browser plugins. The popular Blackhole exploit kit for example tends to focus on Java and Adobe Reader vulnerabilities. Looking at these statistics, it is clear that attackers have identified the weak link to the enterprise security chain. Unfortunately, most enterprises have yet to even begin tackling this challenge.

A key differentiator of the Zscaler Advanced security suite that addresses outdated browser plugins is delivered in our Secure Browsing functionality. Secure Browsing queries the Document Object Model of the web browser to identify not only the browser type and version number but also the version of common plugins that have been installed. This information is then checked against a Zscaler maintained database to identify and provide a warning should outdated plugins be identified.

Figure 4 - Most Outdated Web Browser Plugins - Q3 2011
**Interrogator™**

Zscaler strives to provide the most comprehensive in-line real-time protection available. At the same time, we also recognize that new threats are identified every day and that we must take a multi-pronged approach to identify even those threats that neither our partners nor we have seen before. That’s where Interrogator comes into play. Interrogator is a proprietary technology designed by Zscaler to further ‘interrogate’ suspicious transactions offline by performing tests that simply could not be done inline without negatively impacting performance.

![Interrogator Diagram](image)

**Figure 5 - Interrogator Workflow**

Interrogator is a technology platform, consisting of a series of ‘blades’, each designed to further analyze web content from a unique perspective. Suspicious content is continually identified and fed into Interrogator blades by data mining processes, that continually monitor Zscaler NanoLogs looking for traffic deemed to be suspicious for a variety of reasons. This includes the location where content resides, the nature of the content itself, the fact that the request came from a potentially infected machine. The deliverable from any given blade may flag the content as malicious, benign or maintain the suspicious tag. Malicious content is then automatically blocked in-line for all subsequent requests. Benign traffic is dropped and suspicious traffic is then fed to another blade for further ‘interrogation’.

**Advanced Security**

Zscaler is the only SaaS based web security solution capable of achieving deep, real-time inspection at all levels. With high-speed gateways deployed around the world and geoIP technology, web traffic is always routed to the Zscaler Enforcement Node (ZEN) in the closest geographic proximity. This eliminates needless latency caused by inefficient routing. Once traffic reaches the ZEN, Single Scan, Multi-Action scanning running on a purpose built system allows inspection engines to efficiently scan content in a single pass to implement security at all levels. This architecture permits security controls that can inspect content bi-directionally, at any level, whether or not it is encrypted.

**Network Effect**

Beyond the ability to implement security in real time, SaaS architecture permits unique abilities to identify previously unknown threats and leverage this knowledge to protect all clients. This is known as the network effect. The knowledge that can be obtained from the system, grows exponentially as new users are added. Zscaler taps into this potential by implementing off-line processes to further inspect content using methods that simply could not be performed in real-time due to the time involved to perform the depth of analysis necessary.
Partners
Sharing information with trusted partners is essential to maintaining awareness of emerging threats. Zscaler constantly evaluates partner data feeds to identify those that will improve threat knowledge and enhance client protections. Partner data feeds are integrated in the following four separate domains.

Malicious URLs
On a daily basis, thousands of pages are identified that are known to be hosting malicious code. The code is designed to compromise web browsers accessing such pages by way of known and unknown vulnerabilities. When malicious URLs are identified, block lists leveraged by global ZENs can be instantaneously updated, ensuring that users are transparently protected.

Phishing
Phishing has become a lucrative industry for attackers. Setting up sites designed to social engineer victims into sharing confidential data such as credit card and social security numbers is easy to do. The sites can be quickly assembled and disappear shortly after they first emerge. Receiving multiple feeds identifying such sites and quickly disseminating the information to gateways where it can be leveraged is critical to protecting against phishing attacks.

Botnets
The growth of botnets is one of the greatest threats facing enterprises today. For this reason, Zscaler works with partners to identify known botnet command and control (C&C) servers. With such information, it is possible to continually monitor outbound requests to identify those destined for C&C servers, indicating the presence of infected machines on a given network.

Vulnerabilities
Vulnerabilities are continuously being discovered in applications. Zscaler not only monitors public sources to ensure that signature based protections are deployed for applicable client side vulnerabilities, but also participates in a variety of private and commercial programs. In doing so, Zscaler gains access to vulnerability details ahead of the general public, enabling the deployment of signatures so that customers can be protected from attack simply by surfing the web via Zscaler’s global ZENs.

Page Risk Index
Many times, a definitive rule exists for blocking malicious content. Perhaps, an antivirus signature has returned a positive response or a user has attempted to access a URL, that has been previously black listed. In such cases, blocking is a straightforward, binary decision. Access to the requested content is either blocked or allowed, based on a pre-defined security policy. New threats emerge every day, however, signatures have not yet been written. As such, the concept of reputation plays an important role in providing comprehensive security to end-users.

History
IP reputation has become standard functionality for email security vendors. The idea being that if spam email has previously been identified from a particular source IP address, that same address has an increased likelihood of delivering spam going forward. The more spam detected, the higher the likelihood that subsequent email messages will also be spam. This concept worked well for email security as an IP address is a reasonable and consistent identifier for an email server. Web security vendors have attempted to adapt this same concept. An IP address is not a strong identifier for sources of malicious content on the web as a single web server may host content from multiple sources. As such, vendors have attempted to translate the concept of IP reputation to that of domain reputation. Vendors
calculate a reputation score for a given domain based on a variety of static variables such as the results of periodic security scans. While this approach can provide insight into the security reputation of a given site, it is of limited effectiveness, especially in an environment driven by dynamic, user-supplied content where reputation scores are continually changing.

A New Approach

The size and growth rate of the Internet, combined with a trend toward increasing volumes of dynamic, user-supplied content, ensures that static measures of web reputation alone will never be adequate. Requests will always be made for which no definitive data is available to determine if the request represents a security risk. Content isn’t static so how can a static reputation score expect to succeed? Two users can request the same content at the same time and receive markedly different results. Why? A variety of factors could play a role. The response could be customized based on individual user preferences, different browser versions or the geographic location where the request originated. Perhaps the page contains random content such as a banner ad. In short, static reputation scores simply cannot provide an accurate assessment of dynamic content. For that reason, dynamically calculated variables are required to automatically assess the risk for any given web request/response scenario. No individual metric will provide an accurate risk score for all scenarios. Rather, it is necessary to leverage a blending of a variety of risk indicators and apply appropriate weighting to each variable to achieve a comprehensive risk index or score. An ‘in the Cloud’ security model is an ideal environment to calculate such a risk score as it ensures that all requests and responses pass through a central processing node and therefore allow for complete inspection of all data to and from a given resource.

Calculating a dynamic risk score is a challenging proposition. The score must be calculated ‘on the fly’ for every individual request. Numerous variables must individually be calculated and then combined into an overall risk score. The calculated score must then be compared to a predefined risk threshold in order to make a block/allow decision, and this must occur without adding latency to the browsing experience of each and every user. Thanks to high performance Cloud-based architecture developed by Zscaler, we
have been able to implement the first ever 100% dynamically calculated reputation score for web content. Known as Page Risk Index (PRI), Zscaler’s patent-pending approach to web reputation is a comprehensive weighting of a variety of risk indicators in two separate and distinct control categories – domain analysis and content analysis. A PRI score is calculated for each and every web request, which is then compared to previously established thresholds in order to determine how the request should be handled.

**Control Categories**

The various risk indicators will be drawn from two separate control categories. Each category is defined below along with a summary of some of the key risk categories:

1. **Domain Analysis** – A weighted risk score is calculated for the domain hosting the content requested.
   a. **Geography** – Using geoIP technology, the geographic source of the content is determined. Based on a statistical analysis of the geographic distribution of past malicious content, a risk score is assigned.
   b. **Categorization** – Certain content categorizations such as pornography, shareware, etc. have a higher statistical likelihood of hosting malicious content.
   c. **TLD** – Given the availability and cost of certain top level domains (TLDs), analysis shows that some are more likely than others to host malicious content.
   d. **Domain** – A variety of partner data feeds are inspected to determine if the domain has historically been a source of malicious content.
   e. **Past Results** – Historical results are taken into consideration when calculating the overall domain risk score.

2. **Content Analysis** – A weighted risk score is calculated by inspecting all content returned for a given request. The inspection is done in real-time and all content is inspected.
   a. **Injected Content** – Attackers commonly inject malicious content into otherwise legitimate websites. Page content is inspected to identify code injected into a web page, designed to
directly initiate a browser attack or redirect the browser to an alternate page hosting malicious content.

b. Hidden Content – HTML code such as zero-pixel IFRAMES/images are designed to pull content from a third party domain without providing a visual indicator.

c. Obfuscated Content – Attackers will commonly obfuscate malicious content such as JavaScript in an effort to hide the true purpose of code or complicate debugging efforts.

d. Vulnerable Content – Attackers may include content designed to trigger known web browser vulnerabilities.

e. Potential Attacks – Content inspection may reveal potential attack vectors.

Scoring
All variables within both the page and domain risk index categories are appropriately weighted. A total PRI score is then calculated with a value between 0 and 100. Enterprises can control the acceptable risk level based on their own risk tolerance. When a dynamic PRI score is calculated which exceeds the pre-defined threshold set via the Zscaler administrative UI, the content will be blocked and logged. Administrators will then be able to review blocked requests via the reporting capabilities within the Secure module.

PRI scores would not need to be calculated during a request for which a definitive rule was in place, which allowed or disallowed the request outright. Having a separate block list rule, that prohibits any traffic to Site X would be an example of a situation for which a PRI calculation would not be required. Any request to Site X would be denied and there would not be any reason to perform a PRI calculation. The PRI score would instead be calculated in those situations where a rule was not in place to definitively determine if a given request should be allowed or denied. The PRI score, when compared to a predefined and customizable risk threshold, would then be used to determine if the request is permitted.

Functionality
Leveraging the bi-directional deep inspection capabilities previously discussed, Zscaler has deployed protections against a variety of attacks. A ‘defense-in-depth’ approach is applied on a continual basis.

Botnets
Monitoring the destination of outbound traffic is used to identify direct interactions with known C&C servers. Botnet research is conducted to then additionally deploy signatures that can identify unique patterns within traffic for various botnets. In doing so, newly deployed botnet C&C servers can continually be identified and blocked.

Malicious Active Content
Sites hosting malicious content are continually identified through partner feeds, internal data mining and content-based inspection. Known vulnerable ActiveX controls are also blocked when identified within response bodies. With the prevalence of vulnerable ActiveX controls installed on typical Windows systems, this has become one of the most popular attack vectors leading to compromised PCs.
Phishing
Block lists provide an efficient approach to identifying known phishing sites. A variety of block lists are combined from partner feeds and internal data mining efforts, ensuring broad coverage. Such lists are continually updated and provide effective protection against known phishing sites. Sites are however continually emerging and block lists alone are not sufficient. Heuristic detection methods are therefore additionally employed. Real-time response body inspection allows for the recognition of traits commonly found on phishing sites, thereby identifying previous unknown phishing sites.

Communication
Both infected machines and end users seeking to bypass other security controls employ unauthorized communications. Zscaler has researched common IRC clients and anonymizers to deploy detections based not on block lists but on unique patterns within the communication protocols. This ensures that traffic is blocked regardless of destination.

Cross Site Scripting
Cross-site scripting (XSS) is by far the most prevalent web application vulnerability found on otherwise legitimate websites. XSS can be leveraged by attackers to control scripting languages such as JavaScript, which are then executed within browsers visiting vulnerable sites. Zscaler employs two separate approaches to identify XSS vulnerabilities. The first monitors requests and identifies the presence of active script when such content in not appropriate. The second patent pending approach injects a unique Zscaler cookie into communication with any domain. When content from the cookie is identified in any subsequent request, attempts to steal the cookie’s content—the typical goal of XSS attacks—can be thwarted.

Control Access to Suspicious Destinations
Employing geolIP based technologies, Zscaler is able to empower administrators to block content coming from any geographic location.

P2P Control
By researching popular applications in the P2P categories of file sharing, anonymizers and VoIP applications, Zscaler is able to identify and block alternate protocols being tunneled through HTTP/HTTPS transactions.

Conclusion
With a globally deployed, high-speed architecture, Zscaler has implemented a platform capable of the deep content inspection necessary for robust security in a SaaS solution. The Zscaler platform permits all levels of inspection, regardless of end user device or location. With the ability to conduct bi-directional, real-time inspection, emerging threats can be addressed without the need to deploy and manage software internally. Protections are maintained, managed and updated continuously without any necessary intervention on the part of those responsible for administering the service within the enterprise. Policies can be updated and reports reviewed through an intuitive web portal that enables for uniform protection of all enterprise clients regardless of location.