

# Zscaler Is A Leader Among SaaS Web Content Security

Excerpted From The Forrester Wave™: SaaS Web Content Security, Q2 2015

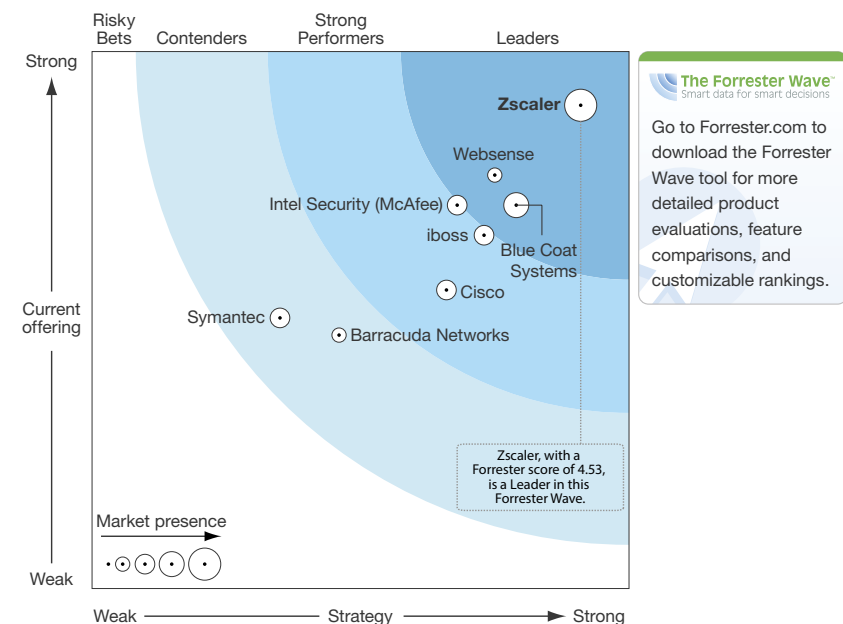
by [Rick Holland](#) and [Kelley Mak](#)

with [Stephanie Balaouras](#), Claire O'Malley, and Peggy Dostie

## ZSCALER IS A LEADER AMONG SAAS WEB CONTENT SECURITY

Since its founding in 2008, Zscaler has found great success in its SaaS web content security business. Zscaler's vision is to provide security-as-a-service and has built its entire platform as such. The solution covers all of the basics in threat detection, URL filtering, and application control, but also provides advanced malware analysis features such as sandboxing and emulation. Its range of traffic redirection options makes it easy to get traffic to the Zscaler cloud from a multitude of devices. Zscaler also has excellent integration capabilities with an exposed API and the ability to ingest threat intel. Customers had only good things to say about the service, mentioning that the company focused on the customer and listened to their requests. Zscaler does not have robust DLP features but plans to strengthen these going forward.

Forrester Wave™: SaaS Web Content Security, Q2 2015



See below for more information on Zscaler's current offering, strategy, and market presence.



### Headquarters

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA, 02140 USA  
Tel: +1 617.613.6000 • Fax: +1 617.613.5000 • [www.forrester.com](http://www.forrester.com)

## Zscaler Evaluation Overview

### CURRENT OFFERING

Threat detection	Zscaler uses at least two antivirus engines. Zscaler has static code analysis. Zscaler has IP, URL, and attachment reputation. Zscaler has real-time classification of uncategorized URLs for super-categories considered high-risk. All other uncategorized URLs are classified manually.
Automated malware analysis	Zscaler inspects office documents, binaries, DLLs, and archive files. Zscaler inspects web content such as JavaScript, Flash, and Java applets. Zscaler has a virtualization-based sandbox. Zscaler performs browser emulation. Zscaler performs operating system emulation.
URL filtering	Zscaler categorizes all web objects on a web page. Zscaler supports traffic shaping. Multiple URL-filtering categories can be applied to a single web page. Time-based quotas are possible. Bandwidth-based quotas are possible.
Application control	Zscaler can identify specific applications and apply policy to them. Zscaler can control specific actions within applications. Specific policies do not exist for Office 365, Google Apps, or Salesforce. DLP technology is leveraged here.
Data loss prevention — discovery and analysis	Zscaler does not support regular expressions. Zscaler only supports DLP fingerprints through a partnership with Symantec. Zscaler does not support fuzzy logic pattern matching. Zscaler DLP technology is proprietary. DLP technology can inspect encrypted traffic.
Data loss prevention — policy support	Zscaler has policy templates for PCI, PHI, and PII. Custom keyword lists can be created. DLP solution can monitor, log, alert, and block. Solution cannot force encrypted uploads to file sharing sites. DLP offering integrates into a broader on-premises DLP solution.
Endpoint support	Zscaler has a Mac OS X agent that supports 10.9 and up. Zscaler has a Windows agent that supports Windows 7 and up. There is PAC file support. There is an on-demand VPN for mobile operating systems. There is a native Android application.
Traffic/protocol inspection	Zscaler can inspect all web traffic, including encrypted traffic. Zscaler can also enable/disable SSL inspection by application, by website, by department, and by user.

#### CURRENT OFFERING

Traffic redirection	IPsec tunnel is supported. GRE tunnel is supported. Host-based redirection is supported. Proxy chaining is supported. DNS is supported.
Deployment models	Zscaler can be deployed as SaaS. Zscaler can be deployed as hybrid with centralized reporting and administration. Zscaler can be deployed as an on-premises appliance, and is working toward an on-premises virtual appliance in summer 2015. Zscaler has an endpoint agent. Zscaler has private cloud deployments.
Data center and SaaS operations	Zscaler maintains more than 100 public and private data center locations throughout the world. To achieve this, it has partnered with many world-class data center providers such as Equinix, Internap, Level 3 Communications, Tata Sons, Telehouse, Intermark, and others. Its providers are SAS70/SSAE16 and ISO 27001 certified. Zscaler also peers with major carrier, deploying direct interconnections with the backbone Internet carriers.
Multitenancy and privacy	Zscaler is a true multitenant environment. Content is never stored at rest and is encrypted in transit. All log information is stored on separate log servers which are encrypted at rest and in transit.
Authentication	Zscaler supports authentication to multiple directories. Zscaler supports SAML. Zscaler supports directory syncing through an on-premises connector. Zscaler supports client agent-based authentication. Zscaler supports explicit user authentication.
Integrations	Zscaler's APIs are exposed for customer integration. Zscaler can ingest STIX content. Zscaler can ingest threat indicators in an automated fashion. Zscaler is capable of ingesting customer provided threat indicators. Zscaler can export CSVs of SIEM log data.
Reporting	Zscaler has 63 default reports. Customers can also create custom reports. Out-of-the-box incident response reporting does not exist.

#### CURRENT OFFERING

Administration	<p>The same administration interface is used to manage email content security offerings.</p> <p>Report-only access can be granted.</p> <p>Granular role-based administration rights can be granted.</p> <p>Multiple concurrent administrators are supported.</p> <p>Hybrid deployments are managed from a single interface with unified reporting and administration.</p>
Dashboards	<p>Dashboards can be customized on a per-admin basis.</p> <p>Dashboards can be rearranged to suit customer preferences.</p> <p>Dashboards can be drilled down into to expand analysis.</p> <p>Dashboards retain state at each step of drilling down with “bread crumb” navigation.</p> <p>The solution provides eight preconfigured dashboards.</p>
Regional support	<p>Zscaler has North America coverage.</p> <p>Zscaler has Europe coverage.</p> <p>Zscaler has Asia Pacific coverage.</p> <p>Zscaler has South America coverage.</p> <p>Zscaler has Middle East coverage.</p>

#### STRATEGY

Developers, sales, and total employees	<p>Forrester estimates there are 160 developers working on the SaaS offering.</p> <p>Forrester estimates there are 100 salespeople selling the solution.</p> <p>Zscaler has close to 600 employees.</p>
Solution pricing model	<p>The list price for 10,000 users is \$19.15 per user per year. This suite includes all types of malware detection, including sandboxed detection of binaries and DLLs. Full SSL inspection is also included.</p> <p>For 50,000 users, the list price is \$17.50 per user per year. There is no difference in the service whether it is deployed as a pure cloud or with some on-premises software. Zscaler offers the same SLAs (availability, latency, and malware catch rate) for all customers. Most Zscaler customers are deployed as pure SaaS. Regardless of the package, Zscaler reports are always available. In this example, the customer will have full access to detailed cloud applications reports or mobile device and application reports. Customers pay only when they need to setup policy. After subscribing to additional features, enablement requires only a configuration change.</p>

## STRATEGY

Technical functionality satisfaction	Zscaler's solution is significantly above customers' expectation because it covers many critical security functions, works well, and has good reporting. Zscaler's strategy for the future is significantly above customers' expectations because they include customers' thoughts in consideration and customers are excited for Zscaler's future offerings. Zscaler adequately and frequently communicates its road map to customers.
Account management satisfaction	Zscaler's technical support is significantly above expectations because they are responsive and are very flexible in custom development. Zscaler's account management is significantly above expectations because customers develop good relationships and feel that Zscaler understands their environment. Customers find Zscaler's CEO to be very engaged with Zscaler's customers. Zscaler was able to provide sufficient customer references to Forrester on time.
Service-level agreements	Zscaler has a transparent public site that displays SaaS POP availability ( <a href="https://trust.zscaler.com">https://trust.zscaler.com</a> ). Zscaler offers SLAs which includes the following: <ul style="list-style-type: none"><li>- Availability: The Zscaler network will be available to accept the customer's outbound requests 100% of the time.</li><li>- Latency: Average latency of 100 milliseconds or less per transaction.</li><li>- Virus capture rate: Zscaler captures 100% of all known viruses transmitted through its system.</li></ul> Zscaler has not had an SLA violation in the past year.

## MARKET PRESENCE

Revenue and revenue growth	Forrester estimates Zscaler's SaaS offering revenue grew more than 100% over the previous fiscal year.
Installed base and growth of installed base	Forrester estimates Zscaler has 5,001 to 10,000 customers.
Verticals	Zscaler's top verticals are manufacturing (includes technology), healthcare, retail, government and military, and financial services.

## WHY READ THIS REPORT

### FROM THE FORRESTER WAVE™: SAAS WEB CONTENT SECURITY, Q2 2015

In Forrester's 26-criteria evaluation of web content security delivered as a software-as-a-service (SaaS) solution, we identified the eight most significant providers in the category — Barracuda Networks, Blue Coat Systems, Cisco, iboss, Intel Security (McAfee), Symantec, Websense, and Zscaler — and researched, analyzed, and scored them. This report provides an overview of the web content security market and discusses why organizations should consider shifting from traditional on-premises web gateways/forward proxies to a SaaS model. The report details our findings about how well each vendor fulfills our criteria and where they stand in relation to each other, to help security and risk (S&R) professionals select the right partner for their SaaS-delivered web content security.

---

*Forrester Research (Nasdaq: FORR) is a global research and advisory firm serving professionals in 13 key roles across three distinct client segments. Our clients face progressively complex business and technology decisions every day. To help them understand, strategize, and act upon opportunities brought by change, Forrester provides proprietary research, consumer and business data, custom consulting, events and online communities, and peer-to-peer executive programs. We guide leaders in business technology, marketing and strategy, and the technology industry through independent fact-based insight, ensuring their business success today and tomorrow.*

© 2015 Forrester Research, Inc. All rights reserved. Forrester, Forrester Wave, RoleView, Technographics, TechRankings, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective owners. Reproduction or sharing of this content in any form without prior written permission is strictly prohibited. To purchase reprints of this document, please email [clientsupport@forrester.com](mailto:clientsupport@forrester.com). For additional reproduction and usage information, see Forrester's Citation Policy located at [www.forrester.com](http://www.forrester.com). Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. 107122\_Zscaler