SOLUTION BRIEF

Zscaler Cloud IPS

Complete IPS visibility and threat protection in a cloud-first world

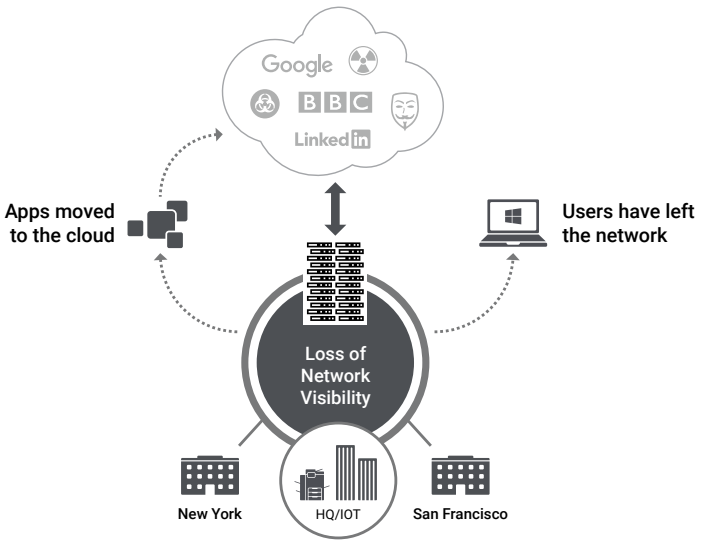
SOLUTION OVERVIEW

IPS is essential, but traditional IPS has become essentially worthless

In today's world, IPS is essential for good security hygiene. Offered as a stand-alone solution, or incorporated in NGFWs or UTMs, the technology is more pervasive than ever before. But while most companies have some form of IPS in place, there new questions about its effectiveness. Due to the increase in user mobility and the skyrocketing use of cloud services, users and apps have been leaving the network—taking with them precious visibility, the lifeblood of IPS. As your users access applications off the network and often away from VPN, they leave your IPS investment and internet security running blind.

Today's IPS solutions are primarily built for server protection, and that's an issue, because today's attacks primarily target users. While protecting the server still has its place, having an IPS that can follow the user and provide always-on inspection of the user connection is fundamental to stopping today's intrusions.

Traditional IPS approaches have difficulty scaling to meet the inspection demands of today's organizations. Adding to that challenge, a majority of threats now reside in SSL-encrypted traffic[1], but there are limits to the amount of SSL traffic IPS hardware can inspect. As internet traffic and user demands increase, organizations must constantly balance the need for performance and the amount of traffic they can inspect. And they must often compromise by inspecting less, thereby increasing threat exposure and organizational risk.



Today's IPS solutions are struggling to deliver the protections they promised

Move your IPS to a higher level with Zscaler™ Cloud IPS

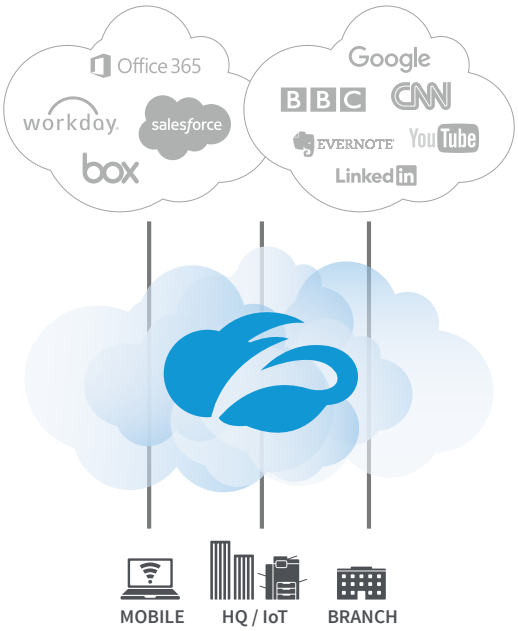
Zscaler Cloud IPS helps organizations restore complete threat protection in a cloud-first world. By delivering IPS from the cloud, all users and offices get always-on IPS threat protection and coverage, regardless of connection type or location. Zscaler Cloud IPS also restores full visibility into user, app, and internet connections, as all traffic on and off network is fully inspected. Because Zscaler Cloud IPS is delivered as a service from the global Zscaler cloud, you get unlimited capacity to inspect all your user traffic, even hard-to-inspect SSL traffic.

[1] https://www.zscaler.com/blogs/research/rise-ssl-based-threats-1

Always-on IPS, always-on protection

Most IPS solutions reside in the data center and lack the ability to deliver visibility and control to off-network traffic. These IPS solutions lose more visibility and control every day, as mobility and SaaS take users and apps off the network. In addition, newer connections—such as SD-WAN, 5G, and direct-to-internet—all encourage organizations to embrace the internet as their corporate network. All these technological shifts have diminished the value of traditional IPS and hindered its ability keep users safe.

Zscaler Cloud IPS delivers IPS from the cloud, which allows IPS to follow the user, regardless of connection type or location. Every time a user connects to the internet or an app, Zscaler Cloud IPS is there. It sits between the connection, providing needed IPS threat visibility that traditional IPS solutions have lost. Organizations can finally restore their lost visibility and threat protection.



Scale IPS and SSL inspection effortlessly

One of the major challenges facing traditional IPS solutions is the ability to scale traffic inspection—and correctly sizing IPS solutions is a real guessing game. What seems like the right size can quickly become insufficient as user demands grow, and that triggers costly hardware refreshes. Even more challenging is the need for SSL inspection.The growth of SSL traffic is staggering—Google reports that over 80 percent of enterprise traffic is now encrypted[2]. But SSL inspection is performance intensive, which is why most IPS hardware solutions fall far short of the task. The result is organizations can't inspect all their SSL traffic, and with a majority of threats now hiding in SSL[1], that's a serious risk.

Zscaler Cloud IPS turns the inspection challenge into an effortless afterthought. Because Zscaler Cloud IPS is delivered from the Zscaler Cloud Security Platform, inspection is elastically scaled based upon demand. Every user gets unlimited inspection capacity, so you never have to guess how much inspection you'll need going forward. Best of all, SSL inspection is native in the Zscaler cloud, so you have the freedom to inspect all your encrypted traffic. No more security compromises, and no more hardware refreshes!

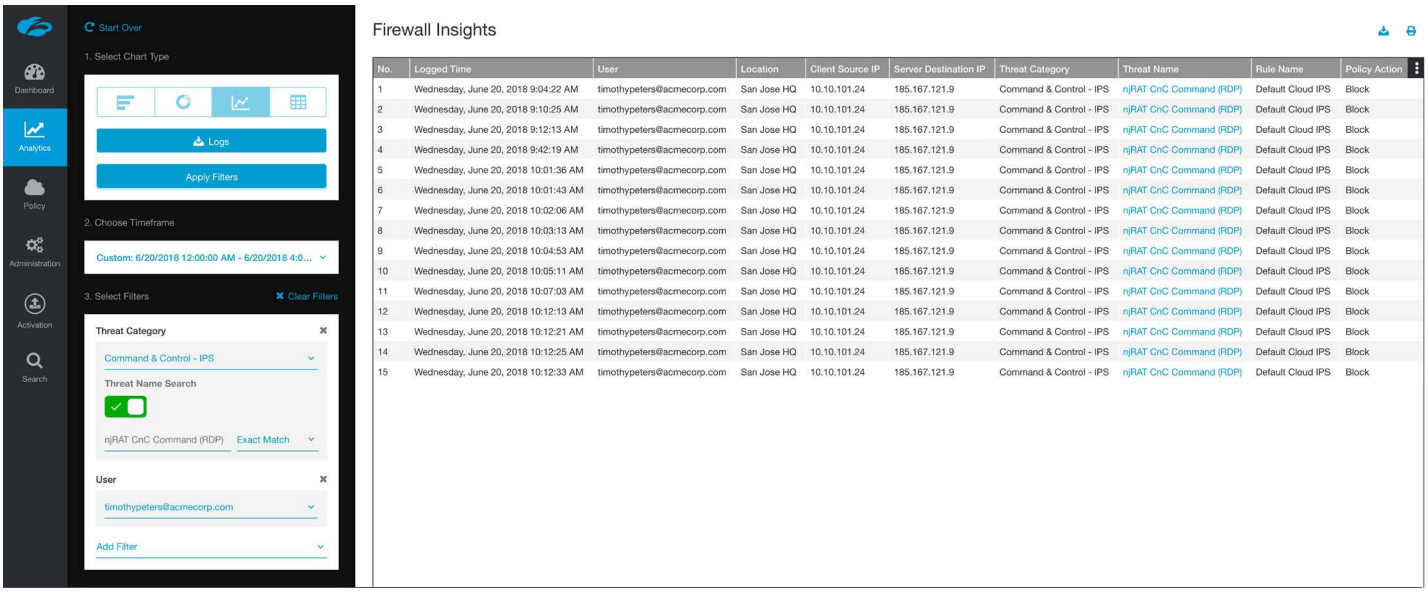
ZSCALER CLOUD IPS BENEFITS

- **Unlimited capacity:** Inspect all user traffic, and elastically scale to demands without capacity limitations.
- **Full SSL inspection:** Deliver full SSL inspection to all your traffic. Find more threats where they hide without inspection compromises.
- **Fully integrated:** Built on the Zscaler security stack as a service, you get IPS fully integrated with firewall, sandbox, DLP, and CASB—turn on the services you need now and add others as your needs change.
- **Transparent updates:** Zscaler Cloud IPS is constantly updated with latest threat coverage. No more change windows or manual updates.
- **Smarter threat intelligence:** Because it processes tens of billions of security requests every day, the Zscaler cloud helps you detect threats faster and produces fewer false positives.

[2] https://transparencyreport.google.com/https/overview

Full integration for context and correlation

To reduce risk, you need to understand the meaning of your alert data. Key to this task is bringing in full user and application context from external sources and correlating this data. However, many IPS solutions struggle to deliver. The reason? The meaningful context and correlation of threat data requires thoughtful integration of all your security systems. With most solutions, this means "some assembly required," and, in practice, organizations often find themselves with a full blown science experiment as they try to get disparate systems to work together.



No.	Logged Time	User	Location	Client Source IP	Server Destination IP	Threat Category	Threat Name	Rule Name	Policy Action
1	Wednesday, June 20, 2018 9:04:22 AM	timothypeters@acmecorp.com	San Jose HQ	10.10.101.24	185.167.121.9	Command & Control - IPS	njRAT CnC Command (RDP)	Default Cloud IPS	Block
2	Wednesday, June 20, 2018 9:10:25 AM	timothypeters@acmecorp.com	San Jose HQ	10.10.101.24	185.167.121.9	Command & Control - IPS	njRAT CnC Command (RDP)	Default Cloud IPS	Block
3	Wednesday, June 20, 2018 9:12:13 AM	timothypeters@acmecorp.com	San Jose HQ	10.10.101.24	185.167.121.9	Command & Control - IPS	njRAT CnC Command (RDP)	Default Cloud IPS	Block
4	Wednesday, June 20, 2018 9:42:19 AM	timothypeters@acmecorp.com	San Jose HQ	10.10.101.24	185.167.121.9	Command & Control - IPS	njRAT CnC Command (RDP)	Default Cloud IPS	Block
5	Wednesday, June 20, 2018 10:01:36 AM	timothypeters@acmecorp.com	San Jose HQ	10.10.101.24	185.167.121.9	Command & Control - IPS	njRAT CnC Command (RDP)	Default Cloud IPS	Block
6	Wednesday, June 20, 2018 10:01:43 AM	timothypeters@acmecorp.com	San Jose HQ	10.10.101.24	185.167.121.9	Command & Control - IPS	njRAT CnC Command (RDP)	Default Cloud IPS	Block
7	Wednesday, June 20, 2018 10:02:06 AM	timothypeters@acmecorp.com	San Jose HQ	10.10.101.24	185.167.121.9	Command & Control - IPS	njRAT CnC Command (RDP)	Default Cloud IPS	Block
8	Wednesday, June 20, 2018 10:03:13 AM	timothypeters@acmecorp.com	San Jose HQ	10.10.101.24	185.167.121.9	Command & Control - IPS	njRAT CnC Command (RDP)	Default Cloud IPS	Block
9	Wednesday, June 20, 2018 10:04:53 AM	timothypeters@acmecorp.com	San Jose HQ	10.10.101.24	185.167.121.9	Command & Control - IPS	njRAT CnC Command (RDP)	Default Cloud IPS	Block
10	Wednesday, June 20, 2018 10:05:11 AM	timothypeters@acmecorp.com	San Jose HQ	10.10.101.24	185.167.121.9	Command & Control - IPS	njRAT CnC Command (RDP)	Default Cloud IPS	Block
11	Wednesday, June 20, 2018 10:07:03 AM	timothypeters@acmecorp.com	San Jose HQ	10.10.101.24	185.167.121.9	Command & Control - IPS	njRAT CnC Command (RDP)	Default Cloud IPS	Block
12	Wednesday, June 20, 2018 10:12:13 AM	timothypeters@acmecorp.com	San Jose HQ	10.10.101.24	185.167.121.9	Command & Control - IPS	njRAT CnC Command (RDP)	Default Cloud IPS	Block
13	Wednesday, June 20, 2018 10:12:21 AM	timothypeters@acmecorp.com	San Jose HQ	10.10.101.24	185.167.121.9	Command & Control - IPS	njRAT CnC Command (RDP)	Default Cloud IPS	Block
14	Wednesday, June 20, 2018 10:12:25 AM	timothypeters@acmecorp.com	San Jose HQ	10.10.101.24	185.167.121.9	Command & Control - IPS	njRAT CnC Command (RDP)	Default Cloud IPS	Block
15	Wednesday, June 20, 2018 10:12:33 AM	timothypeters@acmecorp.com	San Jose HQ	10.10.101.24	185.167.121.9	Command & Control - IPS	njRAT CnC Command (RDP)	Default Cloud IPS	Block

Zscaler Cloud IPS enables you to have all threat and alert data in one place, with complete user, file, and app context. Streaming to a SIEM allows further integration into the SOC ecosystem.

With Zscaler Cloud IPS, you get a fully integrated platform from day one, with no assembly required. Built from the ground up as a full security stack delivered as a service, the Zscaler Cloud Security Platform provides multiple threat technologies that expertly work together to unify and correlate your threat data. Cloud Firewall, Cloud Sandbox, DLP, CASB, and web and content filtering are all integrated into a unified multi-tenant cloud service. Turn on the services you need, when you need them, as demands grow. Because all relevant threat data is in one place, you get full user, file, and app context and the correlation you need to understand your risk posture. Best of all, integration makes policy configuration a snap. No more jumping around to multiple consoles to take action on your threat analysis.

TRANSPARENT IPS UPDATES

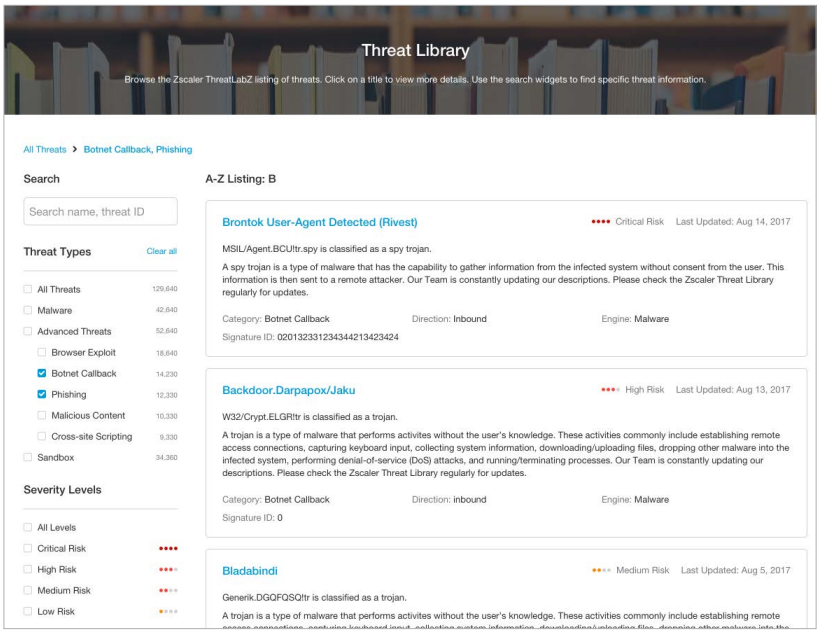
Maintaining an IPS can strain IT resources. Consistently testing and deploying IPS signatures is time consuming, error prone, and often requires restrictive change windows. As a result, many companies fall behind on updates, which increases risk. Delivered as a service, Zscaler Cloud IPS is constantly updated transparently with the latest vulnerability coverage. Users will always get the latest threat protection, and you'll save time and effort.

SMARTER THREAT INTELLIGENCE

With the Zscaler cloud platform. you get millions of users and thousands of companies around the world—including many in the Forbes Global 2000—sharing threat data and intelligence. Zscaler is constantly tracking emerging threats across the cloud and closely collaborating with industry, military, and security organizations to keep the cloud updated. As a result, you get smarter threat intelligence designed to stop emerging threats quicker and reduce corporate risk.

Zscaler Threat Library

Available as an essential tool across the complete Zscaler platform, the Zscaler Threat Library allows administrators and SOC personnel to perform in-depth analysis of threat detections. Search or filter for keyword, vulnerability, or attack category to better understand the threats triggered within your organization and the risks associated with those events.



We can help you bring IPS into the modern era

Zscaler can make your IPS deployment more simple, smooth, and successful, so you can effortlessly scale complete threat protection to all your users. As a completely integrated solution in the Zscaler Internet Access platform, Cloud IPS allows you to easily add more services to your installation as your security requirements grow. We'd love to show you all the amazing things you can do with Zscaler platform services, so feel free to request a demo and more get information.

Zscaler purpose-built multi-tenant cloud security platform

ACCESS CONTROL
- CLOUD FIREWALL
- URL FILTERING
- BANDWIDTH CONTROL
- DNS FILTERING

THREAT PREVENTION
- ADVANCED PROTECTION
- CLOUD SANDBOX
- ANTIVIRUS
- DNS SECURITY
- CLOUD IPS

DATA PROTECTION
- DATA LOSS PREVENTION
- CLOUD APPS (CASB)
- FILE TYPE CONTROLS

POWERED BY PATENTED TECHNOLOGIES

SSMA™
All security engines fire with each content scan — only microsecond delay

ByteScan™
Each outbound/inbound byte scanned; native SSL scanning

PageRisk™
Risk of each object computed inline, dynamically

Nanolog™
50:1 compression, real-time global log consolidation

PolicyNow™
Policies follow the user for same on-premises, off-premises protection

About Zscaler

Zscaler enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a multi-tenant, distributed cloud security platform that protects thousands of customers from cyberattacks and data loss. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com