The Top Security Gaps in Appliance Sandboxes

Did you know there are gaps in your appliance sandbox? We'll fill you in so you can Mind the Gap.

If your company owns an appliance sandbox, you clearly have an advanced threat prevention strategy. Most mature companies do, and it's no doubt the one type of attack that causes your c-suite to lose the most sleep. Nothing can strike more fear into a security organization than the lurking possibility of a chart-topping breach.

But when it comes to stopping the next zero-day, is your current sandbox up to the task? While traditional sandboxing is incredibly powerful, understanding where it excels and where it falls short is the first step to improving your company's ability to stop threats.

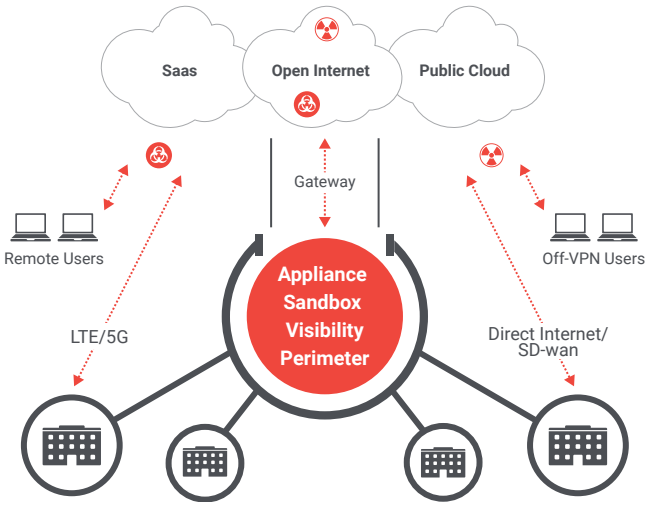
On the following pages, we'll present the top security gaps in your sandboxing appliance, and show you how to fill them.

Security gap #1: Your target is on the move

It goes without saying that your users and data are your most important assets. That's why you work so hard to protect them, and it's why you bought an appliance sandbox in the first place.

To excel in their jobs, users are often required to work wherever business takes them and whenever they're needed. Such mobility gives users—and the organizations where they work—a competitive advantage. But it puts your sandbox at a disadvantage. Once users leave your network, your sandbox goes blind, leaving users exposed and you in the dark. And if there's one thing security experts understand it's that bad things happen in the dark.

And then there's the issue of network attrition. What's network attrition? Much like the loss of employees seeking greener pastures, your network traffic is looking elsewhere, as well. It's something that happens over time, but every SaaS app you've embraced has robbed your network of traffic. And with that traffic goes precious visibility, the lifeblood of your security.



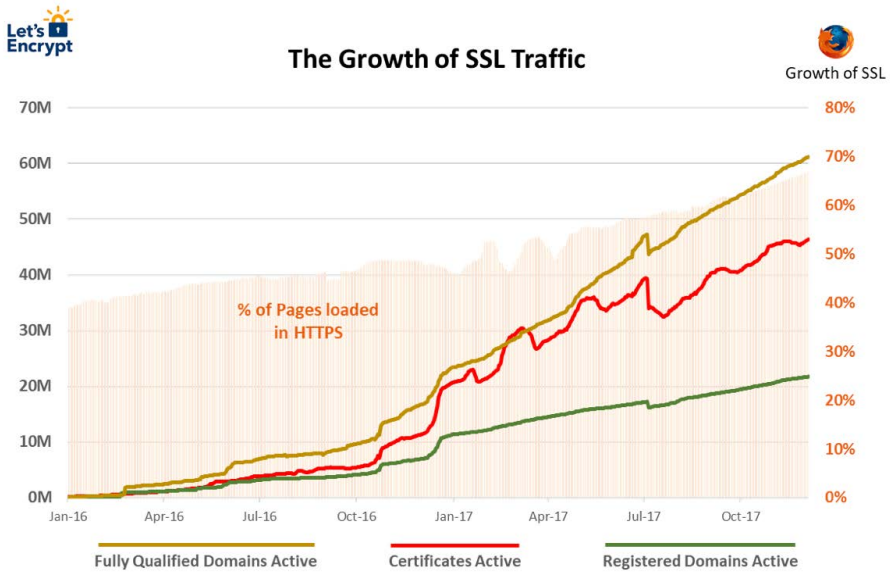
Traditional sandbox appliances go blind when your users leave your network or you break out traffic from your branches. When your apps transition to SaaS, you lose even more visibility as traffic diminishes on your network. The end result is a security gap that exposes your users and data.

How Zscaler minds the gap

Sandboxing is essential for zero-day protection, but only if you can deliver it to all your users every time they connect to the internet. While you may have your network users covered, layering Zscaler Cloud Sandbox over your off-network users or branch office internet breakouts helps close appliance sandbox security gaps. Since this traffic will connect to Zscaler first before the internet, you'll get always-on zero-day protection for these branch offices and users, no matter the connection or location. So, for about the price of a cup of coffee a month per user, you can use Zscaler to strengthen your current sandbox protection strategy. And since it's a service, there's no hardware to deploy or manage.

Security Gap #2: It's spelled SSL

Mozilla, the developer of the Firefox browser, reported that almost 70 percent of internet traffic is now using HTTPS. It's a trend that's been building, and it's becoming a big-time challenge for IT organizations. Most companies inspect only a fraction of their encrypted traffic—it's simply to too taxing for security hardware to do at any scale. And with free certificate authorities like Let's Enrypt growing in popularity, hackers now have the opportunity to enable a whole new level of covertness for their malware.



The growth of SLL traffic has been staggering, as the diagram to the left highlights. On the right axis, you can see that almost 70% of all traffic loaded in Firefox browsers is over HTTPS.

The growth of SSL is in part due to free certificate authorities like Let's Encrypt. As of the end of 2017, over 45 million certificates were active. The Let's Encrypt free and automated model has made the process of encrypting traffic so painless that hackers can now readily embrace SSL to help hide their malicious content and exploit security gaps in inspection.

A recent analysis of the Zscaler global cloud platform shows that over half of all malware seen is now hiding in SSL traffic.[1] Because decrypting and re-encrypting SSL traffic is so compute intensive, much of this traffic goes uninspected. Adding third-party SSL inspection hardware can help diminish the bleeding, but this approach usually falls far short. The total cost and network routing gymnastics required to attain and maintain complete SSL visibility is far out of reach for most organizations.

How Zscaler minds the gap

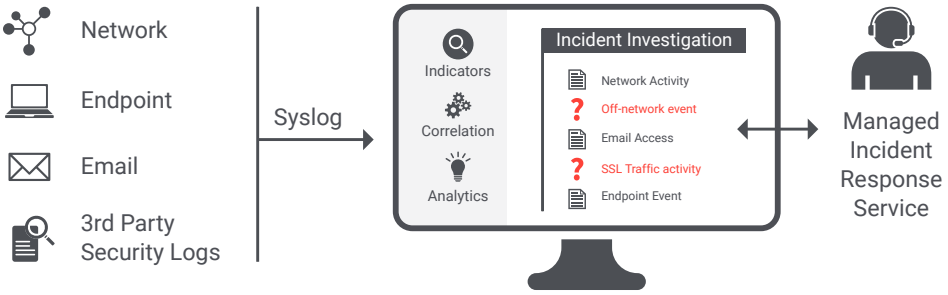
Purpose built for security and scale, SSL inspection is core to the Zscaler cloud platform DNA. With the ability to deliver unlimited inbound and outbound SSL inspection, you can easily bring zero-day protection to ALL your encrypted traffic. You can use our certificates or bring your own—and administration is a snap. Once you load the certs into the Zscaler cloud, they are instantly available across all 100 Zscaler data centers, which means you don't have manage certs across multiple gateways and appliances. You can even use our API to automatically rotate your certificates as often as you want. Best of all, you'll finally be able to inspect ALL your SSL traffic for advanced threats and zero-days.

[1] *https://www.zscaler.com/blogs/research/ssltls-based-malware-attacks*

Security gap #3: Threat Hunting services are only as good as your visibility

The lifeblood of your advanced threat strategy is visibility. Finding and stopping the stealthiest attacks requires a level of log reading that many organizations lack, especially in light of the current shortage of IT analysts. For this reason, many companies outsource log analysis to a managed incident response service. These teams of experts help customers by hunting threats emerging with their network using in-depth detection, investigation and response techniques.

However, your logs won't show what your systems haven't seen, and as we know from mobility trends, there's a whole world happening outside your security perimeter. Users want to get to their cloud apps and to the open internet with minimal resistance, which for remote users means bypassing the VPN and thereby avoiding your security gateway and appliance sandbox. Add to that the inevitability that most traffic happens over SSL, and it adds up to a large portion of your security picture that your current sandbox and incident response experts can't see or use for investigation purposes.



For many organizations, hiring a managed incident response service is an attractive option to help add value to the threat data captured within an organization.

Although the service can help consolidate logs and identify emerging user threats, much of today's user activity happens off network and is encrypted—factors that hinder security but that hackers are all too eager to exploit.

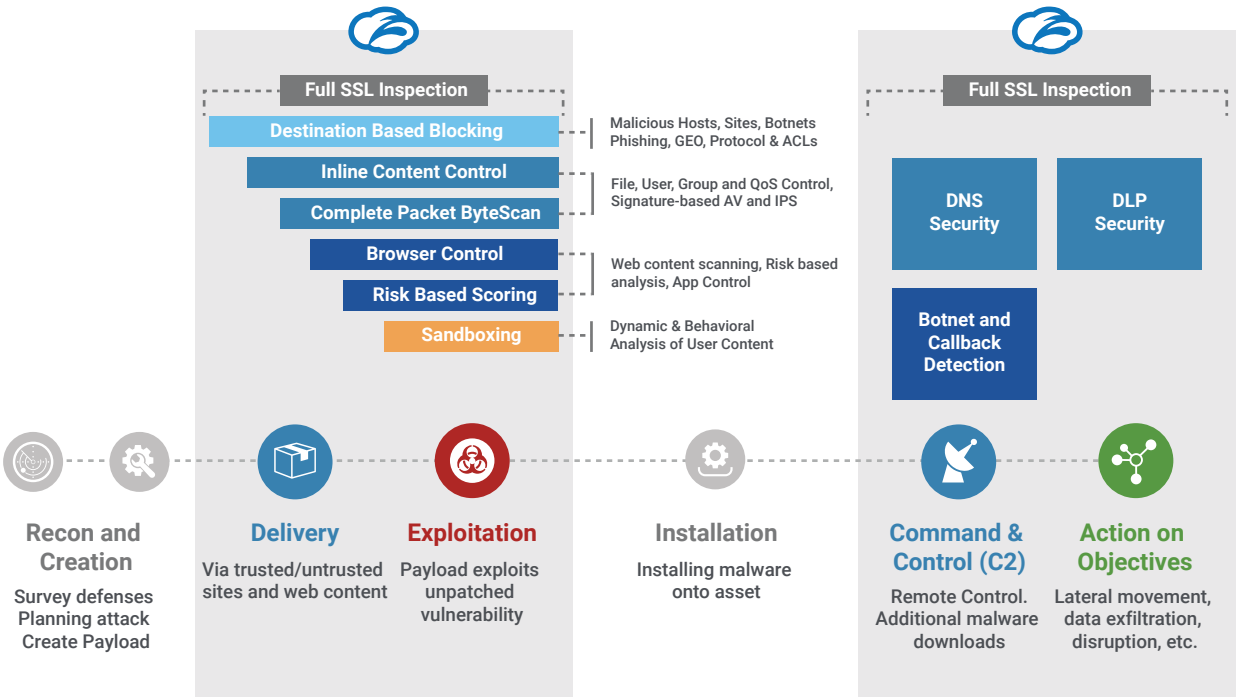
How Zscaler minds the gap

One of the key advantages of Zscaler and Zscaler Cloud Sandbox is always-on security, regardless of where and how your users connect. Delivery from the cloud across 100 data centers means you get follow-the-user visibility 24 hours a day. By layering Zscaler onto your existing sandbox infrastructure you can restore the security waystation between your off-network users and branch offices and their internet connections. With support for syslog streaming, you can then send this comprehensive visibility back into Managed Incident Response service or any SIEM you may be using. By combining the Zscaler platform's in-depth visibility across SSL with your existing early warning systems, you will have an uninterrupted picture of every user's activity 24/7 across your organization. Threat investigations will go faster, and emerging threats can be stopped more quickly.

So where do we go from here?

While traditional sandboxing is essential to increase visibility, the best advanced threat security strategy is always defense in depth. There are many new technologies designed to address zero-day protection at every level of the security stack, and organizations must find the best approach that minimizes risk, balances budget and easily fits into their infrastructure.

In the end, it's a good idea to focus on how adequately you can disrupt the malware kill chain, and the security redundancy available in the event that one level of your security ecosystem fails. Endpoint, network, visibility, and policy control should all work together to help keep the bad guys as far away from your data as possible. When building a security strategy, many architects start with the assumption the endpoint is already compromised. In the presence of that reality, what additional layers on the network do you need to maintain an adequate level of visibility, control, and risk mitigation for all your users?



The Zscaler Security Architecture is designed from the ground up with an additive approach to defense in depth. Multiple layers work together to help deliver redundant protection against advanced threats and zero-days, while providing much needed visibility across hard-to-inspect SSL traffic.

Regardless of your approach to zero-day protection, a solid security strategy starts with understanding and addressing your security gaps. By layering Zscaler onto your existing sandbox infrastructure, you can deliver continuous sandboxing protection for all users, peel back the inspection barriers of all your SSL traffic, and strengthen your existing sandbox investment.

Learn more about **Zscaler Cloud Sandbox** or reach out to us if you'd like to **get a demo** of how Zscaler Cloud Sandbox help you mind the gap!

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