Ready to Switch from Symantec (Blue Coat)?

Your digital transformation is underway, but you won't get there with an appliance-based proxy gateway.

There was a time when gateway proxy and URL filters like Symantec's (Blue Coat) appliances were the best approach for delivering network security. But with applications moving to the cloud and many users working off-network, such network security approaches are deficient. Organizations must adopt a cloud-first mentality.

Why? The cloud and mobility have broken traditional network security. Your users now need fast, secure access to the internet and their cloud apps regardless of where they're connecting. One workaround is hair-pinning users back into your network for scanning before heading out to the cloud, but firewalls and other appliances tend to tip over as traffic demands rise. Traffic from SaaS apps like Microsoft 365 (formerly Office 365) easily overwhelm appliances with their long-lived sessions, and the inspection demands of SSL are too much to process. Even if the traditional stack did work, it's too difficult to create consistent protections across disjointed on-premises solutions.

It's time to transform, and it's up to IT departments to lead the way, helping their organizations adopt a cloud-first mentality. The good news is that IT has always been out in front, driving meaningful technological change. So break free from the snares of legacy, roll up your sleeves, and save the day once again!

DON'T GET STUCK WITH A BROKEN CLOUD STRATEGY

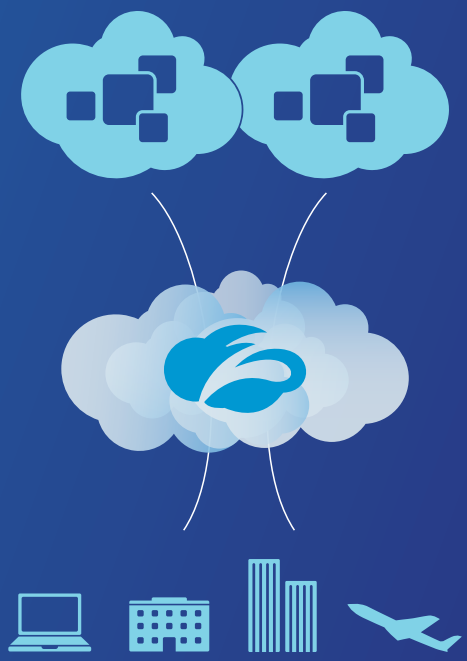
Driving transformation in your company starts with a cloud platform you can trust. The first step to transcending the appliance doldrums is to move your security to the cloud. Cloud-delivered security easily and seamlessly goes everywhere your users go. No matter the connection, device, or location, cloud-delivered security will always be between your users and cloud apps, protecting every connection.

Symantec's (Blue Coat)—now Broadcom's—approach to cloud security, on the other hand, forces you to maintain a hybrid setup that only adds to the complexity the cloud is designed to reduce. Think of it this way: If you were to move to Salesforce, would you want to buy and maintain on-site Salesforce appliances as well as using the cloud-based platform? Of course not. Vendors like Symantec (Blue Coat) that force you into these types of hybrid footprints are ill-prepared to deliver true cloud solutions that carry the promise of agility, performance, and simplicity. It's important to have the clarity to not let half-measures and inertia from legacy approaches "cloud" your cloud strategy.

DO EMBRACE A CLOUD THAT TRULY TRANSFORMS

Zscaler™ built a cloud-native solution because it was always the company's vision to help customers move securely to the cloud—not just protecting certain users and apps, but protecting all of them. Zscaler cloud security services are delivered by a multitenant, global architecture designed from the ground up for performance and scalability. It is distributed across more than 150 data centers on six continents, which means that users always have a short hop to their applications.

Because all the security services you'll ever need are easily enabled in the Zscaler cloud, you get amazing simplicity but incredible performance and security. Add to that an industry-leading 99.999% SLA that processes the business-critical traffic of 450 of the Forbes Global 2000 organizations, and you have a platform you can trust.

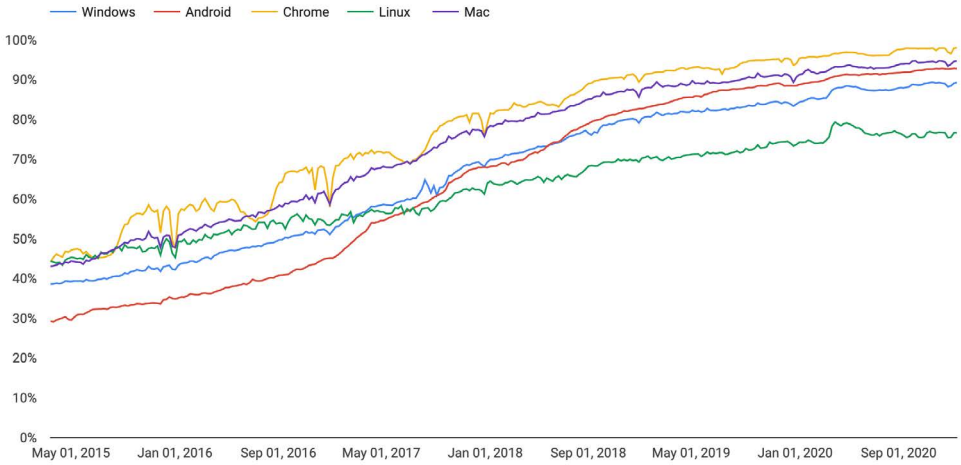


FAST. SECURE. RELIABLE.

DON'T MISS THE THREATS HIDING IN YOUR TRAFFIC

The growth of SSL is undeniable. The graph below shows the volume of HTTPS traffic that passes through Google servers. In four years, encrypted traffic has doubled, topping 90 percent with some platforms.

Percentage of pages loaded over HTTPS in Chrome by platform



With the increase in encrypted traffic, you might expect to see a similar increase in the use of encryption for hiding malware—and you'd be right. The majority of threats are now delivered within encrypted traffic, made possible through the use of free, easy-to-obtain SSL certificates. Full SSL inspection is essential. But, can your Symantec (Blue Coat) proxy appliances keep up with the demand? Sure, you could throw mounds of hardware and money at the problem, but it's a losing battle of hardware refresh cycles and network routing complexity. Not to mention the cost. The upshot of all this complexity and cost is that most organizations only inspect limited amounts of SSL traffic. You end up losing valuable visibility into traffic and that puts you at risk. And, it just doesn't have to be that way.

DO INSPECT ALL YOUR TRAFFIC, NO COMPROMISES

The Zscaler cloud is built on a unique, cloud-native, inline proxy architecture. This means that as a consumable service, you can easily inspect every single packet of your SSL traffic without impacting performance. With a full security stack that includes Advanced Cloud Firewall, IPS, Advanced Cloud Sandbox, CASB, URL Filtering, DLP, and more, you get full protection for your SSL traffic from all those hidden threats that can sneak past your Symantec (Blue Coat) proxy appliances. So, go ahead, throw as much encrypted traffic at us as you want, and we'll inspect it. And because Zscaler services are charged per user, pricing is simple and predicable. No surprises.

DON'T STRUGGLE WITH MICROSOFT 365 TRAFFIC

Microsoft 365 has become the most popular SaaS application on the planet. You've probably rolled it out in your organization. But as a Symantec (Blue Coat) customer, there's a good chance you're struggling with the demands of this traffic. To keep Microsoft 365 applications humming, you must provide fast connections to the Microsoft cloud. Key Microsoft 365 apps also require sending all ports and protocols to Microsoft applications.

Many IT departments find their Symantec (Blue Coat) proxy appliances can't scale and have to be bypassed in order to get Microsoft 365 working properly. What's the point in having these appliances if you can't enforce the access and policy controls you need on your most critical business traffic?

> When compared to backhauling data across the corporate WAN, the user is most likely going to get better performance by egressing Office 365 network traffic to the Internet close to their location where it can be connected to Microsoft's global network.
>
> **Microsoft, Office 365 network connectivity overview, June 2019**

DO SCALE MICROSOFT 365 THE RIGHT WAY

With Zscaler, you can route Microsoft 365 traffic the way Microsoft recommends—using direct internet connections. These connections should route traffic directly to the Microsoft cloud from branch offices and remote sites, bypassing appliances, and without backhauling to a data center. With direct internet connections secured in the cloud, you get a fast, local, and direct internet experience for your Microsoft 365 traffic.

How does it work? Zscaler improves the Microsoft 365 user experience in multiple ways. With secure local breakouts and local DNS, users get the fastest connection to the internet. Zscaler peers with Microsoft in internet exchanges around the world, enabling fast connections to the Microsoft 365 cloud. What's more, the rest of your branch office internet connections get the power of Zscaler security, so users can access the internet securely, without the slowing effects of backhauling and appliances.

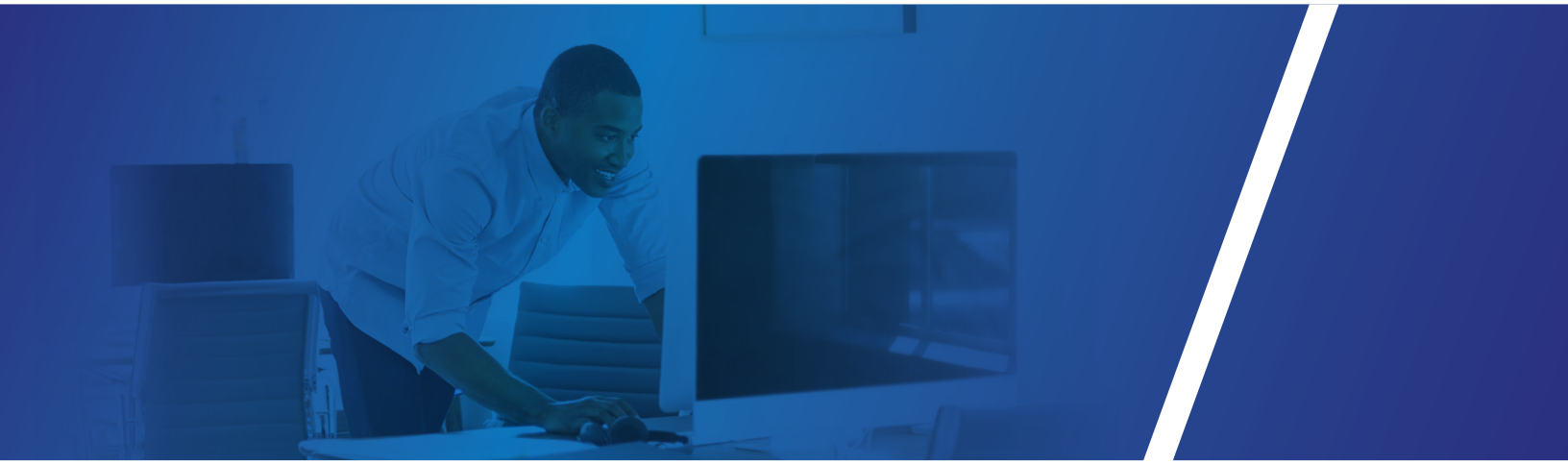
DON'T BE UNPREPARED FOR THE NEXT THREAT

Security is always a game of cat and mouse. A new threat comes out and a new preventive measure follows. As security professionals, it's the game we unfortunately have to play, and with such high stakes, we have to play to win. There are hundreds of thousands of new threats discovered every day.

Can your Symantec (Blue Coat) proxy appliance—can any appliance—keep up with the updates demanded by these threats? To keep your users safe, you'd be updating appliances constantly. And if there's something IT professionals know well, it is the challenge of change windows. Updates are always difficult to stay on top of, which is why many appliances are multiple versions behind on security updates. It's a situation you shouldn't have to find yourself in.

DO SAY GOODBYE TO THE CHANGE WINDOW

Imagine a world in which you never have to perform an update. That's the world you'll be in with Zscaler. As a subscription service, you needn't do a thing about updates—the Zscaler platform is always up to date. In fact, we perform 175K+ unique security updates every day. We aggressively put protections in our cloud for all those new and emerging threats we find and share amongst our 40+ threat-sharing partners. Even better, you get thousands of other Zscaler customers working for you. For any threat that's detected anywhere in the world on our cloud, protection is cascaded across the entire global cloud within seconds. It's security the way it ought to be.



WHERE DO YOU GO FROM HERE?

It's time to break free from the constraints of Symantec (Blue Coat) for good. Zscaler makes it easy to improve security and the user experience immediately for employees on- and off-net without any infrastructure changes. Then, as you send all cloud-bound traffic through Zscaler, you can phase out security appliances in your gateways and reserve your private links for traffic going to the data center, slashing MPLS costs. And, because policies follow users, your employees get identical protection in branch offices, headquarters, or on the road.

Best of all, with Zscaler you can modernize your infrastructure and become a fully cloud-enabled organization, free from the limitations of slow, cumbersome gateway appliances. The future is in the cloud, and we'll help you get there securely.

Find out why thousands of organizations, including 450 of the Forbes Global 2000, send all their traffic through Zscaler for uncompromising security, reduced complexity, and a fast user experience.

Learn More

Built 100% in the cloud, Zscaler delivers the entire security gateway as a service. By securely connecting users to apps, regardless of device, location, or network, Zscaler is transforming enterprise security. That's why more than 4,000 organizations and 450 of the Forbes Global 2000 have moved to Zscaler.