Akamai

BUYER'S GUIDE

How to Select a Cloud-Based Secure Web Gateway

Protect a Remote Workforce and Simplify Enterprise Security

Table of Contents

Securing the modern enterprise: rethink data center backhaul

Cloud computing, software as a service (SaaS), mobility, and updated network architectures have revolutionized business practices. But they have also created a perfect storm for IT teams trying to secure the workforce while not limiting the value of these new technologies. Now there's a fresh challenge: Regardless of where enterprises were in their digital transformation, many had to quickly pivot to support a drastic increase in remote users in 2020.

A secure web gateway is a critical component of protecting a corporate workforce, but many enterprises are still using physical appliances deployed in data centers. This hardware requires ongoing management, maintenance, and upgrades, and uses byzantine traffic backhauling to inspect and control web traffic — ultimately degrading performance.

Organizations need a modern, streamlined approach to securing this new reality of a distributed corporate environment. The solution: Dispense with hardware appliances and move that secure web gateway capability to the cloud.

This buyer's guide describes the benefits of cloud-based secure web gateways and what capabilities to look for in a modern web gateway technology.

Increase in remote work creates new IT and security demands

Over the past decade, organizations have steadily increased their remote workforces. That trend has only accelerated in the wake of COVID-19 and is expected to continue well beyond the pandemic. Gartner found that 74% of surveyed CFOs will move at least 5% of their previously on-site workforce to permanently remote positions after the pandemic is over.[1]

At the same time, the number of sophisticated targeted attacks such as phishing, ransomware, and malware has skyrocketed. Fifty-three percent of respondents to a recent survey said they had witnessed a rise in phishing activity since the start of the COVID-19 pandemic.[2] A recent advisory from the U.S. Department of the Treasury stated that demand for ransomware payments has increased during the COVID-19 pandemic as cyberactors target online systems that people rely on to continue conducting business.[3]

Traditionally, organizations secured internet access for on-site users in main and branch locations and remote workers alike by installing security appliances, such as secure web gateways, in their data centers. They would then backhaul all web traffic to that central location for inspection and control.

Enterprises have used these secure web gateways to filter unwanted malware from user-initiated web traffic, prevent users from accessing malicious websites, and enforce company and regulatory policies.

These gateway solutions were originally designed and deployed in environments where most workers used enterprise-managed devices at their desks. But as the number of users working remotely and in branch offices grew, and more traffic went to the public internet to access SaaS applications, organizations began installing multiple redundant secure web gateways in the central data center to maintain satisfactory performance. Purchasing and managing these boxes became increasingly complex, costly, and time-consuming.

> **"The percentage of the IT budget spent on data centers has decreased over the past several years, and now accounts for just 17% of the total."**
>
> — Gartner, 2019 IT Key Metrics Data

Alternatively, organizations added secure web gateway appliances to their branch locations while backhauling traffic for all remote users. Such redundancy led to additional appliance sprawl and its attendant costs, as well as labor-intensive deployment and management.

It also became increasingly difficult to maintain consistent security policies across a large number of locations. Even when organizations deployed virtualized appliances to reduce the appliance sprawl, they still had to deploy and manage extra hardware.

A third approach was hybrid deployment, in which organizations continued to use on-premises secure web gateways for major locations and sent branch web traffic to a cloud-based secure web gateway — while again backhauling traffic for remote employees. This approach preserved existing hardware investments in on-premises equipment. However, it added complexity because organizations ended up managing disparate systems. Not only were the additional equipment and added management much more expensive than a pure cloud approach, it was also difficult to maintain consistent policies across local and cloud-based systems.

> **Gartner predicts that by 2025, 80% of enterprises will shut down their traditional data centers.[4]**

To make matters worse, even as organizations were adopting these increasingly complex solutions, they began to face a scarcity of cybersecurity resources. A study by (ISC)[2] found that it would take a 62% increase to fill the current shortage of needed security workers in the United States.[5]

Why a cloud-based secure web gateway?

Organizations need a modern approach to web security — one that maps against the businesses' cloud strategy, embracing and enabling remote work. A cloud-based secure web gateway brings organizations a high level of security while reducing complexity by connecting directly to the internet to avoid the need for multiple appliances and backhauling.

With a cloud-based secure web gateway, organizations can benefit from:

Reduced security complexity: As a service in the cloud, these secure web gateways eliminate the need to deploy hardware or virtual appliances, as well as configure, manage, and replace/upgrade hardware every three years.

Minimized performance bottlenecks: An internet-based secure web gateway eliminates the need to add extra appliances to cope with increased web traffic loads and rising levels of encrypted traffic. Customers can simply add additional services as required with minimal impact on performance.

Less costly backhauling/hairpinning of traffic: Cloud-based secure web gateways apply security to web traffic without backhauling traffic to allow direct connection to the internet, thereby reducing Multiprotocol Label Switching networking costs.

Better security team efficiency: Because cloud secure web gateways require no ongoing maintenance of hardware or software, scarce security resources have more time to focus on other proactive security measures.

Consistent security policies: Organizations can use policies that are managed centrally but deployed globally — for all users connecting from any device. Even if the organization has different policies for different regions, it can use the same UI to manage them all.

Key requirements for a secure web gateway

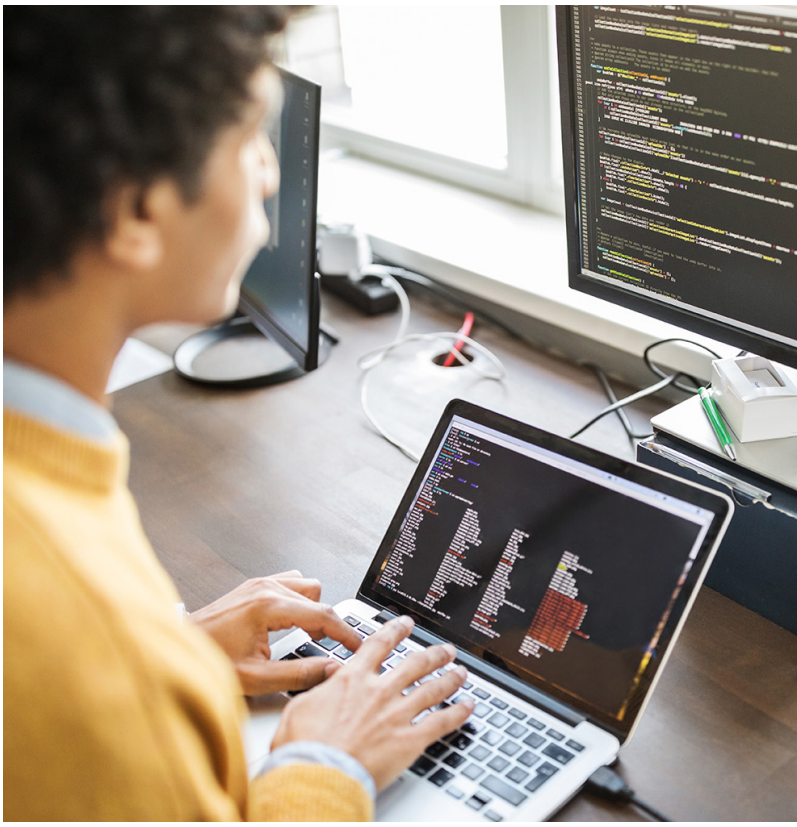
When selecting a cloud-based secure web gateway, it's important to recognize that security is the key requirement. Many legacy secure web gateways include capabilities that solve problems that no longer exist. For example, they include bandwidth control, which was designed for a time when bandwidth was expensive. Or they block employees from using YouTube or Facebook during work hours. Today, these capabilities are no longer necessary, because bandwidth is plentiful and so many people use their mobile devices that organizations are no longer concerned with barring these services on corporate devices.

Today, organizations need a cloud-based secure web gateway that is specifically designed to handle modern security concerns. In particular, the solution should follow a defense-in-depth strategy that employs multiple security measures to provide the highest level of protection. Such an approach should cover all angles of cybersecurity and provide redundant security measures. That way, if one line of defense is compromised, additional layers of defense are in place to stop attacks from slipping through the cracks. This layered approach ensures that threats such as malware, ransomware, and phishing are blocked earlier and faster — and before the user's device is compromised.

A secure web gateway that deploys a defense-in-depth strategy should offer the following security capabilities:

Evaluation of all DNS and URL requests

A cloud-based secure web gateway solution should evaluate all URL and DNS requests against real-time threat intelligence and block malicious



requests early in the kill chain. If the secure web gateway can block threats before an outbound connection is made, the web resource does not need to open or inspect any returned content. This efficiency avoids a computationally intensive process and reduces the amount of traffic the secure web gateway must analyze at the payload stage. The result? Improved overall secure web gateway performance.

The threat intelligence should protect against malware, ransomware, phishing, and low-throughput DNS-based data exfiltration. It should also be purpose-built to deliver protection that is current, relevant, and provides low rates of false positives.

Multiple payload analysis techniques

Because all threats are different and thus no single detection technique or approach can address every type of malware, the secure web gateway solution should include multiple malware analysis engines. These engines should scan HTTP and HTTPS payloads either inline or offline using a variety of identification techniques including signature, signatureless, machine learning, and sandboxing. This analysis will deliver comprehensive zero-day protection against potentially malicious files such as executables and document files.

Zero-day phishing detection

Remote employees continue to face increased phishing attacks since the COVID-19 outbreak. Malicious actors launch these attacks via email, social media, and instant messaging applications, as well as through online file sharing and collaboration channels, to steal corporate credentials that give them entry to the enterprise network. From there, attackers can move laterally to find and exfiltrate data and intellectual property, or promulgate ransomware campaigns.

To identify and block access to a phishing page, most security vendors do the following:

1. **Observe unusual traffic hitting a domain**
2. **Analyze that domain**
3. **Determine if it's a phishing domain**
4. **Add it to the blocklist**
5. **Push blocklist update out to customers**

This process can take hours. And worse still, today's cybercriminals use phishing kits to easily create and launch short-lived attacks, making detection even more difficult. By the time the phishing domain or URL is found, the attack is over. Indeed, the more sophisticated and targeted the phishing attack, the shorter its duration.

But while these campaigns may end quickly, an advanced zero-day phishing detection engine can identify and block them. The recurring elements of these kit-based attacks can be seen in the code of phishing pages. Using this information, it is possible to identify "fingerprints" for these pages that enable accurate identification.

A secure web gateway solution should include a zero-day phishing detection engine that can analyze requested web pages and compare these against "fingerprints" of previously seen phishing pages.

Encrypted traffic inspection

The internet is an inherently insecure channel for data transfer. As a result, encryption of web traffic is now ubiquitous to stop attackers intent on eavesdropping, committing forgery, or tampering with traffic. Transport Layer Security (TLS) is the de facto encryption standard for delivering secure web browsing. TLS creates a secure tunnel between two endpoints, such as a client browser and a web server.

> **The percentage of encrypted web traffic on the internet has steadily increased, from around 50% in 2014 to between 80% and 90% today. Most (96%) of the world's top 100 sites default to HTTPS.**
>
> — Google Transparency Report, 2020

But not all HTTPS traffic is benign. Attackers and malware writers also use encryption to hide their activities, prevent users from accessing files (through ransomware), and secure malicious network communication. A recent study found that nearly a quarter of malware that made an internet connection used TLS to communicate.[6]

To proactively inspect and control HTTPS web traffic, it's necessary to look inside the secure tunnel and examine the encrypted traffic, using a proxy server (trusted intermediary). The proxy server should decrypt the HTTPS traffic into plain text, analyze it, re-encrypt the traffic, and then create another secure connection in a technique called machine in the middle (MITM). MITM inspects requested URLs to determine if they are safe or malicious, provide visibility into TLS encrypted traffic, and protect the enterprise from threats while preserving confidentiality and integrity of traffic to origin websites.

MITM inspections require considerable processing capability. Web browsing can therefore slow down because of latency. The secure web gateway should offer services that improve application performance. It should include a globally distributed network of servers and intelligent software located close to users and data centers worldwide to enable web optimizations that improve application performance and availability.

In addition, the MITM should check that the cloud secure web gateway vendor maintains a centralized list of domains and URLs that do not work correctly and should be bypassed. Furthermore, the cloud secure web gateway should be able to bypass MITM inspection for specific types of sensitive web content, such as in financial services and healthcare.

Integrated data loss prevention

Proactively preventing the loss of personally identifiable information (PII) and other confidential business data is critical given the potential for financial or reputational losses. The cloud secure web gateway should include integrated data loss prevention that is easy to configure and quick to deploy. Frequently updated dictionaries should cover data privacy and protection regulations such as PII, PCI-DSS, and HIPAA, while organizations should be able to easily create custom dictionaries.

Shadow IT identification and management

Users have, at their fingertips, hundreds of thousands of applications to download, install, and use on managed devices — without the awareness of the enterprise security team. But the use of unsanctioned applications can significantly expand the organization's attack surface and increase its risk profile.

> **The average company uses over 1,295 apps and cloud services. More than 95% of these are unmanaged, with no IT administration rights.**
>
> — Cybersecurity Insiders, Cloud Security Report, 2019

A cloud secure web gateway should be able to identify which applications are being used, detect how many users have installed specific applications, and highlight applications that may present a potentially serious security risk. Once identified, the solution should be able to block the entire application or specific application operations (for example, allowing uploads but not downloads).

Protection everywhere for any device

Work style flexibility has seen a massive upward trend over the past decade. Users now work from everywhere — on any device. And, as a result of working from home during the pandemic, 59% of end-user computing for enterprises is moving to mobile devices, augmenting or replacing PCs and laptops. This shift is predicted to continue even after the return to office work.[7]

The move to mobile devices and increased use of Wi-Fi networks can present a crack in any organization's security posture. Enterprises need to be able to apply a uniform, universal level of security — without compromising device performance.

A cloud secure web gateway should proactively identify, block, and alleviate targeted threats such as malware, ransomware, phishing, DNS data exfiltration, and zero-day attacks on any device (iOS, Android OS, Chrome OS), across any network the user joins. The gateway solution should deliver ubiquitous controls and streamlined management, globally, while maintaining optimal device performance.

Secure access to all enterprise applications

A cloud secure web gateway protects users and devices from malware as they access the public internet. But it is just one piece of the security puzzle for an enterprise.

To create a holistic security approach for the entire business, organizations also need to protect corporate-owned and -managed applications — whether they reside in the corporate data center or in an IaaS environment — from nefarious actors. Traditional network security tools protect the network perimeter, but if attackers breach the perimeter (for example, by stealing user credentials or by installing malware on a user device) they can move freely inside the network.

Organizations need a cloud secure web gateway that also offers a Zero Trust Network Access (ZTNA) technology to protect corporate applications. ZTNA is a critical component of Zero Trust security adoption, granting users access only to specific applications (not to entire networks or segments) based on user identity. The solution safeguards user identity through integration with identity and access management, multi-factor authentication (MFA), and single sign-on technologies. By using a ZTNA tool, organizations eliminate the complexity of securely managing devices, or maintaining complex wide area network or virtual private network connectivity. Once properly authenticated, users are granted access to only the applications and data they need, reducing the application attack surface to zero and minimizing the risk of lateral movement. When organizations evaluate a cloud secure web gateway, they should consider the capabilities of

Enterprise Phishing Attacks Are on the Rise

Observed Attacks, March – October 2020

INCREASE IN ATTACKS AGAINST
ENTERPRISES

INCREASE IN ATTACKS AGAINST
CONSUMERS

Source: Akamai Enterprise Threat Protector Secure Web Gateway

the vendor's ZTNA service. Can the service provide access to modern web applications as well as legacy non-web applications? Can the service integrate with the organization's existing identity provider service? Does it support MFA?

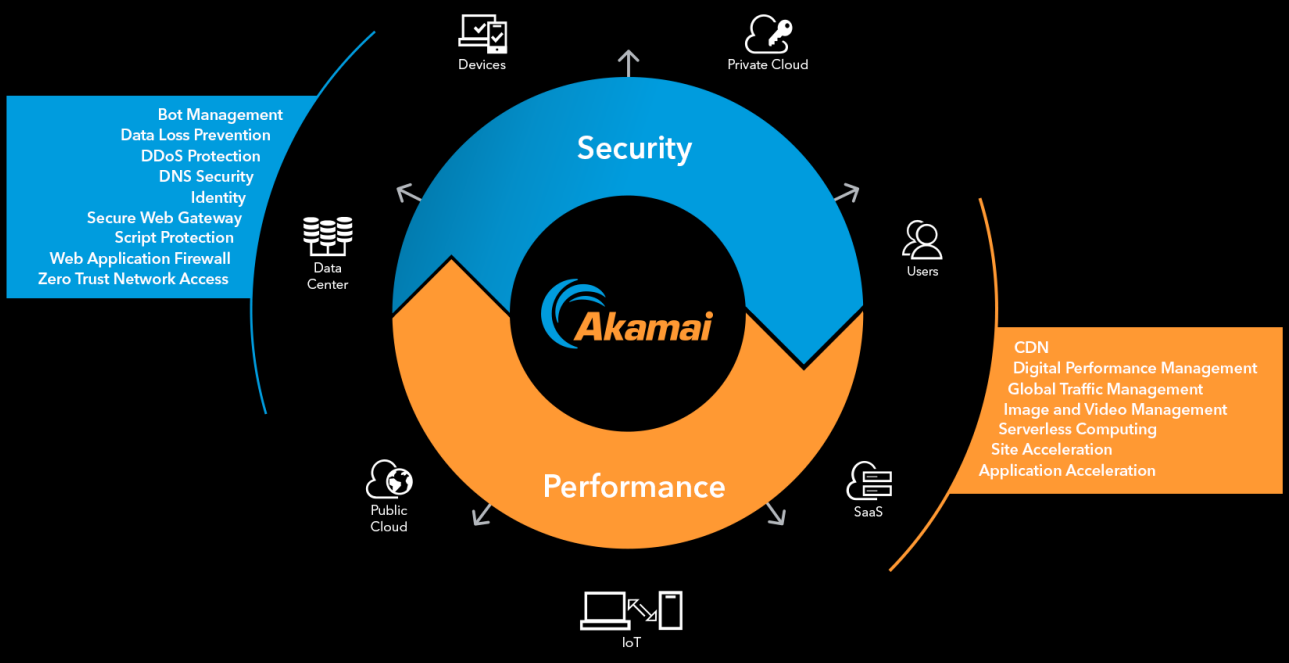
The secure web gateway should integrate and work hand in hand with the ZTNA service such that, if a device is found to be compromised, it will be prevented from accessing any corporate applications. A secure web gateway's logs can augment other threat signals to provide a more accurate picture of a device's security posture. For example, if the device is calling out to command and control servers, the solution should use that as a signal to limit application access until the device is remediated.

By adding secure web gateway and ZTNA capabilities, organizations take a step toward adopting a secure access service edge (SASE) framework. SASE shifts the center of an organization's security effort away from the data center–centric and hardware appliance–centric security architectures that no longer work for today's highly distributed work and business environment. Instead, SASE delivers policy-based access according to the identity of the user and/or device. SASE also provides a wide range of additional security controls, including web application firewall, API security, bot management, and distributed denial-of-service protection for web-facing applications.

> **ZTNA improves the flexibility, agility, and scalability of application access, enabling digital businesses to thrive without exposing internal applications directly to the internet, reducing risk of attack.**
>
> — Gartner, Market Guide for Zero Trust Network Access, Steve Riley, Neil MacDonald, Lawrence Orans, 8 June 2020

Furthermore, security controls are delivered on the SASE platform one internet hop away from the user to provide low-latency access to users, devices, and cloud services anywhere.

Akamai Cloud-Delivered SASE



Optimal performance

While security is paramount, it cannot compromise user experience with slow performance. In addition to providing a defense-in-depth approach to security, a cloud-based secure web gateway should deliver the above services without introducing latency.

To avoid latency, the cloud secure web gateway should be deployed globally with points of presence close to where all users connect. After all, there's little point in replacing one type of backhauling for another.

The cloud platform should also scale quickly to avoid impacting the end-user experience, even under peak conditions. This capacity is particularly important when it comes to inspecting HTTPS traffic, which is growing exponentially and will ultimately compose close to 100% of all web traffic. Inspecting encrypted traffic with minimal impact on end users is critical, as the vast majority of malware is now delivered over HTTPS. The platform should also provide a 100% availability SLA.

> **Office 365 users now make up over half of the 81% of total organizations who have made the shift to cloud services.[8]**

Office 365 integration: It is particularly important to ensure a high level of security and performance for Microsoft Office 365, as many organizations rely on this service as their essential productivity suite. One challenge when deploying a cloud secure web gateway is that O365 — like many other popular SaaS applications — performs poorly when users access its applications via a forward proxy, which performs the TLS MITM inspection.

To avoid impacting O365 performance, it's critical that the cloud secure web gateway be delivered via a global edge platform that can:

- Use the source IP of the request to direct the request to the geographically closest Microsoft O365 data center, rather than to backhauled DNS solutions that would direct the request to the data center closest to the corporate DNS resolver; for example, a user who accesses O365 from Singapore and is routed to an O365 server in New York would have a terrible user experience
- Make sure that secure web gateway server locations are situated close to Microsoft O365 data centers — and that, ideally, these servers and data centers are interconnected
- Provide a one-click O365 traffic optimization setting that uses a list of O365 domains and IP addresses published and updated by Microsoft; requests to these domains should be sent directly to O365 servers in line with Microsoft recommendations, which saves time and effort by eliminating the need to manually update firewalls and other security products when Microsoft adds new domains or IP addresses

Move security to the edge

Rapidly growing remote workforces are increasingly vulnerable to cyberattacks, which, in turn, are becoming more frequent and severe. The best cloud-based secure web gateway solutions will focus exclusively on meeting these modern security demands by delivering a proven defense-in-depth functionality. They will also enable modern enterprise security models like Zero Trust and SASE by securing access to the internet for all users, no matter where they are located.

A comprehensive cloud secure web gateway should evaluate all DNS and URL requests, provide multiple payload analysis techniques, address zero-day phishing, inspect encrypted traffic, integrate data loss prevention, identify and manage shadow IT, and provide protection everywhere for any device — all while delivering a high level of performance and integrating with enterprise application security technologies. With such a solution, organizations can reduce security complexity, eliminate costly backhauling, improve security team efficiency, and support consistent security policies.

Learn more about Secure Internet Access Enterprise, Akamai's cloud-based secure web gateway, and start a free trial at akamai.com.

1. https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2
2. https://www.helpnetsecurity.com/2020/09/02/phishing-attacks-pandemic/
3. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
4. https://blogs.gartner.com/david_cappuccio/2018/07/26/the-data-center-is-dead/
5. https://www.brinknews.com/a-global-shortage-of-cybersecurity-professionals-leaves-businesses-at-risk/
6. https://news.sophos.com/en-us/2020/02/18/nearly-a-quarter-of-malware-now-communicates-using-tls/
7. https://www.mobolize.com/2020/10/29/mobolize-announces-technology-partnership-with-akamai-to-enable-security-on-mobile-devices/
8. https://blog.goptg.com/microsoft-office-365-statistics#:~:text=According%20to%20Bitglass%2C%20usage%20of,the%20shift%20to%20cloud%20services

Akamai powers and protects life online. Leading companies worldwide choose Akamai to build, deliver, and secure their digital experiences — helping billions of people live, work, and play every day. With the world's most distributed compute platform — from cloud to edge — we make it easy for customers to develop and run applications, while we keep experiences closer to users and threats farther away. Learn more about Akamai's security, compute, and delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on Twitter and LinkedIn. Published 11/22.