Data Sheet

McAfee Web Gateway Cloud Service

Cloud-delivered web security providing ubiquitous protection

Key Benefits

- The most cost-effective way to deploy web security—no on-premises hardware or software required.
- Go beyond basic protection—behavior emulation prevents zero-day malware in milliseconds as traffic is processed.
- Extend protection to off-network users. Cloud-delivery erases the traditional network perimeter.
- Unparalleled management efficiency with the McAfee® ePolicy Orchestrator® (McAfee ePO™) Cloud platform as the unified management console for all Intel Security cloud services.
- Proven architecture: McAfee® Web Gateway Cloud Service is built as a multitenant version of McAfee Web Gateway, the trusted on-premises appliance used by enterprises worldwide.

Defending against sophisticated threats from the web takes advanced technology, but it doesn't have to drive cost and complexity. Delivering web security from the cloud enables security teams to gain the same benefits of advanced threat protection as on-premises appliances, but without the cost of hardware or the resources used to maintain it. As more web access occurs outside the network perimeter, the cloud becomes the consistent point of contact for devices and users as they roam. Instead of building security for traffic flowing into a single location, it is more effective to build security from the endpoint out. Connecting endpoints, and even entire locations, to the cloud provides ubiquitous protection, never exiting the new perimeter which has moved beyond network walls.

Cost-Effective, Ubiquitous Protection

Managing on-premises web security appliances is expensive and takes cycles away from security teams who are often already stretched thin. Deploying web security as a cloud service can drive down total cost of ownership. There are no longer hardware appliances to buy, own, and maintain. All resources formerly used for maintaining appliances, performing tasks such as software upgrades and patching, can be re-allocated to more strategic initiatives within the IT or IT security organization.

Both appliance and cloud service can be used together in a hybrid deployment. Most organizations choose this model to maintain ownership and control of appliances on network, and extend cloud-delivered protection to small remote offices and roaming users.

IT teams who backhaul web traffic from remote offices over multiprotocol label switching (MPLS) circuits for filtering by a web gateway appliance on network benefit immediately from cloud-delivered web security. Backhauling traffic is expensive and adds complexity to the network. Instead, remote offices can route directly to the cloud for protection, eliminating MPLS circuits and simplifying network architecture.

Lastly, employee access to the web is no longer confined to the network perimeter, leaving off-network users and devices unprotected and invisible to IT. Shifting web security to the cloud inverts this perimeter. Web traffic from off-network users and devices can be automatically routed from the endpoint to cloud, maintaining a secure connection when working from home, at an airport, a coffee shop, or any other off-network location. No longer is the network focused on traffic within physical walls. Instead, it is extended out from wherever an endpoint travels.

intel Security

Global, High-Performance Architecture

McAfee Web Gateway Cloud Service is built for the enterprise, and many organizations will gain a higher level of performance than they currently experience on premises. For example, on premises, when there is a need for capacity increase, IT needs to procure and deploy a new appliance, which can take days to weeks. In our cloud, capacity increases take approximately 15 minutes due to the elastic cloud design built into the service.

When an on-premises appliance fails and needs repair, it can take down the internet and damage security posture if allowed to fail open to the web. In the event of a failure at one of our data center locations, our cloud service will automatically re-route all web traffic to the closest, fastest data center location, ensuring immediate continuity.

Our cloud service architecture is also built to "peer" with the internet backbone at the world's largest internet exchange points (IXPs). This eliminates routing hops of intermediate internet service providers (ISPs) who simply add latency to the connection. With less hops to popular content providers such as Microsoft Office 365 and Google, users often gain a faster connection through our cloud service than they would connecting directly to the open internet.

McAfee Web Gateway Cloud Service is global. To view the current locations and status of the data centers where web traffic is processed, visit **https://trust.mcafee.com**. Web content can be delivered in local regional language, so regardless of where a user connects, they see for example, local Google search results.

Defend Against Sophisticated Threats

Security teams often can't keep up with highly sophisticated malware and targeted attacks that evade traditional defenses, causing a drain on resources and constant "firefighting" to keep up with endpoint remediation. Unlike traditional URL filtering and signature-based approaches to preventing web threats, McAfee Web Gateway Cloud Service protects endpoints from zero-day and fileless malware through in-line emulation of files, JavaScript, and HTML. This enables the prevention of zero-day malware before it ever reaches a user and improves block rates

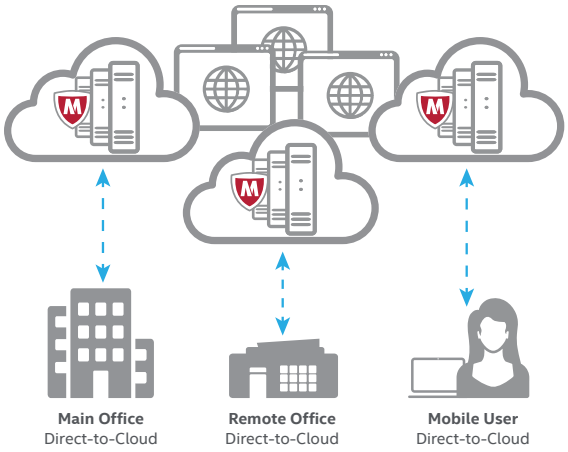

Figure 1. McAfee Web Gateway Cloud Service deployment.

by approximately 20% over URL filtering and signature-based solutions. Security operations benefit from lower costs and greater resource flexibility by reducing the overall number of malware incidents.

Web threats are often delivered through encrypted traffic to hide from web security defenses. Nearly all cloud applications, such as cloud storage or social media, use encrypted traffic by default. McAfee Web Gateway Cloud Service can fully decrypt and inspect HTTPS encrypted traffic, enabling malware prevention and cloud application visibility within encrypted channels.

For most IT teams, it is a challenge to control the proliferation of cloud applications, particularly "shadow IT" and risk driven by user-chosen services. With full visibility into all web traffic, including HTTPS, pre-built reports can show websites accessed, cloud applications in use, and corresponding data points to assess risk. Shadow IT is easily uncovered by comparing what is actually in use to what IT has sanctioned. Cloud applications, especially cloud storage, are also increasingly used as the delivery mechanism for malware. Identifying which applications have delivered malware can help inform policy decisions. With the full scope of what cloud services are being accessed, over 1,600 cloud application controls can be implemented to minimize risk, such as preventing uploads, messaging, or blocking applications outright.

Where in the world is McAfee Web Gateway Cloud Service?

Visit **https://trust.mcafee.com** for live updates and visibility into our data center locations, availability status, and more.

Efficient Security Management

Managing security across multiple consoles and policies is burdensome, especially when on-premises and cloud-based web security are managed separately. In a hybrid environment, there is one management console for both on-premises and cloud deployments, a single set of policies, and one reporting interface.

When deployed alone without on-premises hardware or software, McAfee Web Gateway Cloud Service is managed by McAfee ePO Cloud, the unified management console for all cloud-based security services from Intel Security, along with endpoint security, providing unprecedented efficiency in security management.

Deploying web security for endpoint devices is a challenge, especially routing and authentication. McAfee Client Proxy, an optional endpoint client, automates routing and authentication to our cloud service, ensuring a pervasive connection to the cloud with consistent policy enforcement. McAfee Client Proxy functions seamlessly in a hybrid deployment with on-premises appliances, intelligently routing to the appliance while on network and to cloud service while off network. Additional routing and authentication options are available and can be chosen based on organizational requirements.

Learn More

For more information, visit **www.mcafee.com/webprotection**.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com