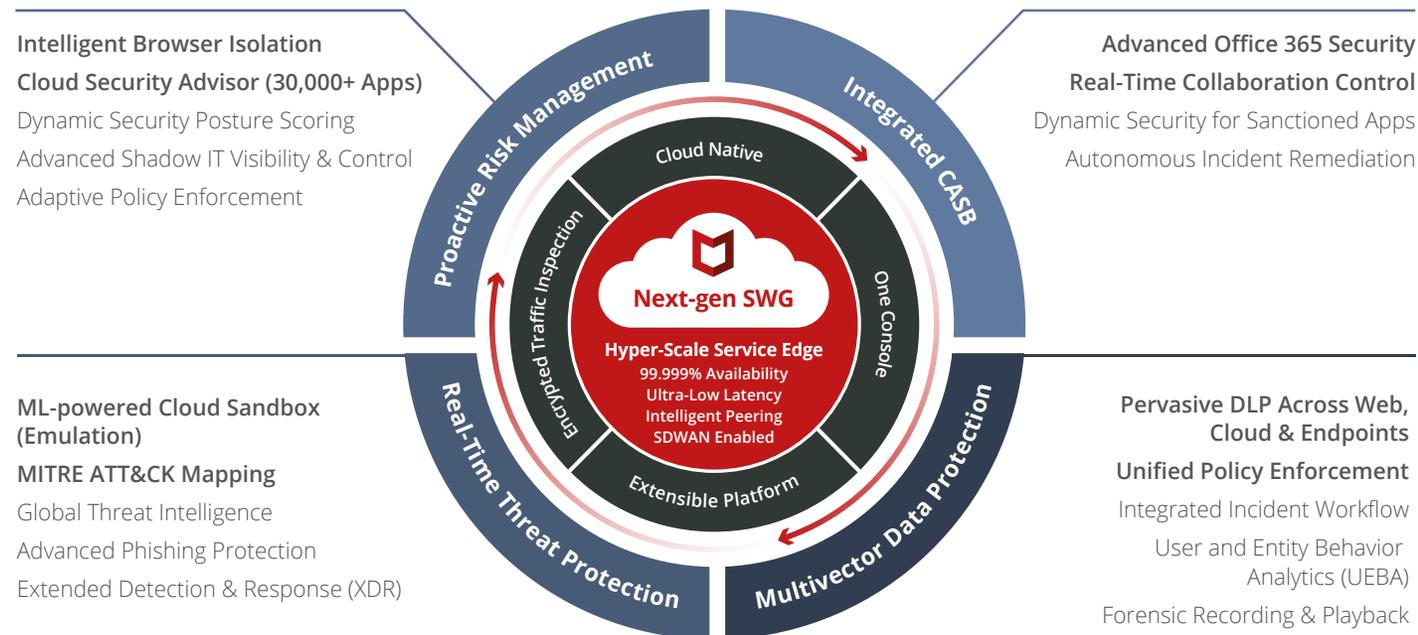**McAfee™**

Intelligent, Hyper-Scale Next-gen Secure Web Gateway Platform for SASE

Blazing fast, low-latency, 99.999% uptime cloud-native web security

Today, with increased cloud adoption, more than 80% of corporate network traffic is destined for the internet. Backhauling internet traffic to a traditional web architecture depends on redirecting this internet-bound traffic through a traditional on-premises web gateway and can be costly. As traffic spikes in an increasingly work-from-home world, the network slows to a halt and employee productivity suffers. McAfee® Next-gen Secure Web Gateway helps simplify the implementation of secure access service edge (SASE) architecture and accelerates secure cloud adoption. Furthermore, it provides advanced threat protection, unified data control, and the capability to efficiently enable a remote and distributed workforce.

McAfee Next-gen Secure Web Gateway

Intelligent Browser Isolation
Cloud Security Advisor (30,000+ Apps)
Dynamic Security Posture Scoring
Advanced Shadow IT Visibility & Control
Adaptive Policy Enforcement

Advanced Office 365 Security
Real-Time Collaboration Control
Dynamic Security for Sanctioned Apps
Autonomous Incident Remediation

ML-powered Cloud Sandbox (Emulation)
MITRE ATT&CK Mapping
Global Threat Intelligence
Advanced Phishing Protection
Extended Detection & Response (XDR)

Pervasive DLP Across Web, Cloud & Endpoints
Unified Policy Enforcement
Integrated Incident Workflow
User and Entity Behavior Analytics (UEBA)
Forensic Recording & Playback

Proactive Risk Management
Integrated CASB
Real-Time Threat Protection
Multivector Data Protection

Cloud Native
Encrypted Traffic Inspection
One Console
Extensible Platform

Next-gen SWG
Hyper-Scale Service Edge
99.999% Availability
Ultra-Low Latency
Intelligent Peering
SDWAN Enabled

Key Advantages

- Maintained 99.999% service availability against the 240% increase in cloud usage during the pandemic-related lockdown
- Fully neutralize ransomware and other advanced malware with intelligent and transparent Remote Browser Isolation
- Real-time protection with Gateway Anti-malware
- Easily extend existing on-premises DLP policies to the cloud in one click and under one minute
- Unrivaled visibility and control with the industry's largest cloud application repository, with more than 30,000 applications
- Backed by global intelligence with real-time telemetry from over one billion sensors
- Save 35% to 40% annually by eliminating on-premises hardware

Connect With Us

[Twitter] [Facebook] [LinkedIn] [YouTube] [RSS] [SlideShare]

McAfee unifies web gateway cloud service with remote browser isolation (RBI), cloud access security broker (CASB) technology, and data loss prevention (DLP) capabilities to provide a cloud-native next-gen secure web gateway service that protects organizations from zero-day threats and enforces data protection across endpoints, networks, and clouds. By converging these core technologies into one solution, McAfee enables organizations to implement a simplified SASE architecture that delivers:

- Comprehensive visibility and consistent controls over data from device to cloud
- Consistent threat protection with unified management and investigations
- Direct-to-cloud infrastructure with enterprise scale and resilience

Hyper-Scale Service Edge

Keeping remote workers productive, data secured, and endpoints protected can be overwhelming at times. McAfee Next-gen Secure Web Gateway provides organizations with the scalability and security to support today's remote workforce and distributed digital ecosystem.

Instead of backhauling internet traffic to the corporate headquarters, McAfee delivers robust native support for virtually any SD-WAN solution via site-to-site and site-to-cloud deployments, leveraging industry standard

Dynamic IPSec and GRE protocols. To date, McAfee has certified interoperability with six of the industry's leading SD-WAN vendors, including Viptela (Cisco), VeloCloud (VMware), and Citrix, with even deeper partnerships forged with Silver Peak, Fortinet, and Versa Networks through The McAfee® Security Innovation Alliance program, one of the industry's largest technology partnership programs.

Furthermore, McAfee offers a true cloud-grade service with consistent 99.999% availability. From March 2020 to June 2020, McAfee saw an industry-wide cloud security service load increase, ranging from 200% to 700%. While other security vendors faced similar surges and suffered significant downtime, McAfee maintained its 99.999% availability throughout this time. McAfee Next-gen Secure Web Gateway helps ensure availability, lower latency, and maintain user productivity from wherever your team is working.

Why Five 9s Matter

Difference in allowed downtime based on uptime service-level agreement (SLA):

	99.999% uptime	99.99% uptime	99.9% uptime
Day	0.9 sec	9 sec	86.4 sec
Week	6 sec	1 min	10 min
Month	26 sec	4 min	44 min
Year	**5 min**	**52 min**	**525 min**

Figure 1. Downtime calculation example.

Business Benefits

Better user experience
- Uninterrupted access to the internet, corporate networks, and cloud applications, even when cloud usage spikes
- Seamless browsing experience, with intelligent and transparent Remote Browser Isolation

Highest level of protection
- Stop threats from ever reaching the users with layered protection, including global intelligence, cloud risk databases, zero-day protection, and integrated Remote Browser Isolation.
- Stay out of data breach news and compliant with regulations with sophisticated multi-vector DLP features.

Simplification and reduced total cost of ownership
- A single pane of glass management for policies, incidents, and workflows across multiple environments.
- Cost savings from reduced hardware and elimination of expensive MPLS traffic
- Increased performance, reliability, and scalability

Proactive Risk Management

With increasingly stringent compliance regulations and costly data breach incidents, McAfee Next-gen Secure Web Gateway proactively protects users, data, and applications to help organizations minimize their cloud and web attack surface. It offers integrated RBI, automatically mitigating the risk from unknown websites. Not only does it ensure unknown threats from ever reaching the endpoints, it accomplishes this in a fully transparent way so that the user experience is not hampered.

Furthermore, McAfee has the industry's largest cloud application repository—more than 30,000 applications in its cloud database with 55 attributes each. This provides real-time insights to McAfee® MVISION Cloud Security Advisor that generates automated risk scoring in relation to industry best practices and peers, as well as prescriptive guidance to improve an organization's security posture.
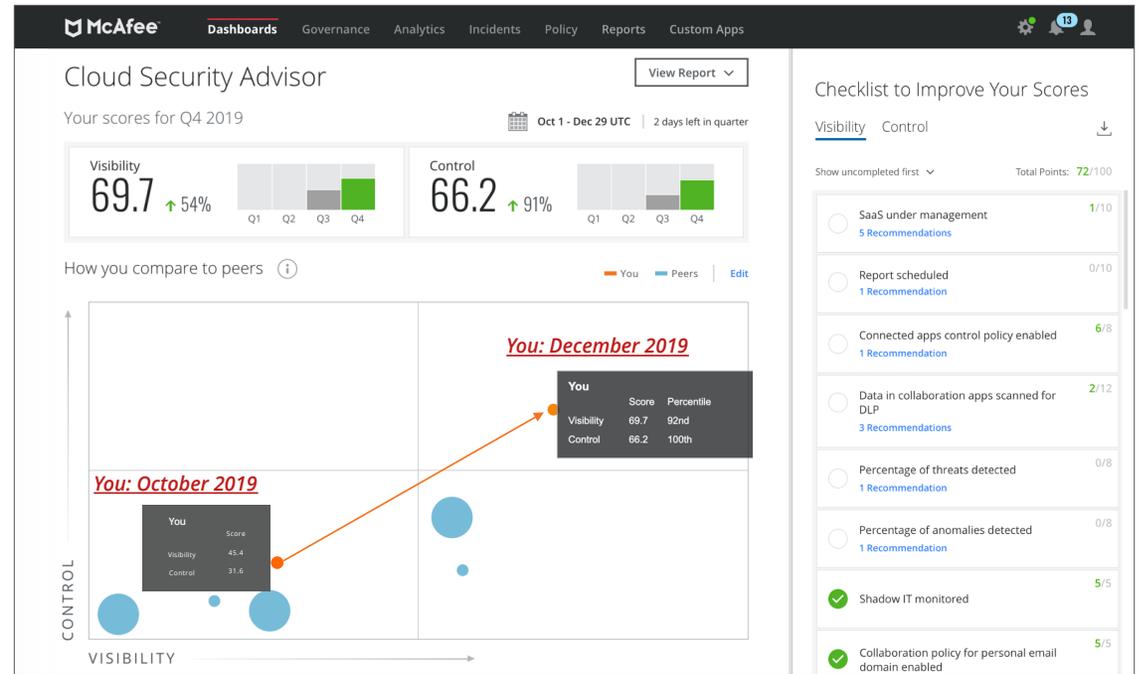

Figure 2. A real-world customer who improved visibility by 54% and control by 91%. Improvements resulted from blocking high-risk services and enabling low-impact DLP and collaboration limitations.

- Take advantage of the industry's largest cloud application repository (more than 30,000 applications)
- Leverage global intelligence with real-time telemetry from over one billion sensors

Integrated CASB

More than 95% of companies today use cloud services, and 83% store sensitive data in the cloud.[1] Personal devices can attempt to access enterprise cloud services such as Microsoft 365. McAfee Next-gen Secure Web Gateway integrates with McAfee MVISION Cloud (CASB) to help organizations control access to all cloud services and protect against threats that occur within them from a single console.

Granular yet flexible, Cloud Application Control provides the users the ability to upload or download documents based on the risk score of the cloud application. Tenant Restriction can differentiate between personal and corporate accounts for cloud services like Microsoft 365, blocking personal accounts from accessing corporate services. With McAfee Next-gen Secure Web Gateway, administrators have access to both McAfee CASB and our cloud-native secure web gateway from a single management interface, which provides unified policies that deliver unprecedented cloud control, keeping users safe from threats and data safe from accidental loss. In addition to managing sanctioned applications, McAfee offers granular policies for unsanctioned applications for completely visibility and control.

Figure 3. A single pane of glass management interface to manage web-based and cloud-based risks and threats.

- Leverage superior SaaS-aware data and threat protection with in-depth SaaS registry of more than 30,000 services

Real-Time Threat Protection

As the web continues to grow and evolve, web-borne malware attacks grow and evolve as well. Ransomware, phishing, and other advanced web-based threats are putting users and endpoints at risk. McAfee Next-gen Secure Web Gateway provides real-time zero-day malware and advanced phishing protection. This multilayered approach integrates dynamic threat intelligence for URL, IPs, file hashes, and real-time protection against unknown threats with machine-learning and emulation-based sandboxing.

Furthermore, McAfee Next-gen Secure Web Gateway provides the capability to decrypt, inspect, and re-encrypt SSL/TLS traffic so that threats and sensitive data cannot hide in encrypted traffic. McAfee also integrated its secure web gateway technology with McAfee® Extended Detection and Response (McAfee® XDR) technology to improve SOC efficiencies.

Remote Browser Isolation

Remote Browser Isolation (RBI) offers secure web browsing experience for end users by preventing elements of a web page from reaching or attack a client browser. McAfee prevents unknown threats from ever reaching endpoints by integrating intelligent yet transparent Remote Bowser Isolation leveraging powerful machine learning analysis on real-time telemetry from over one billion sensors. This powerful combination of security and excellent performance also simplifies the adoption of a Secure Access Service Edge (SASE) to provide customers with a transparent user experience that requires no change in behavior.
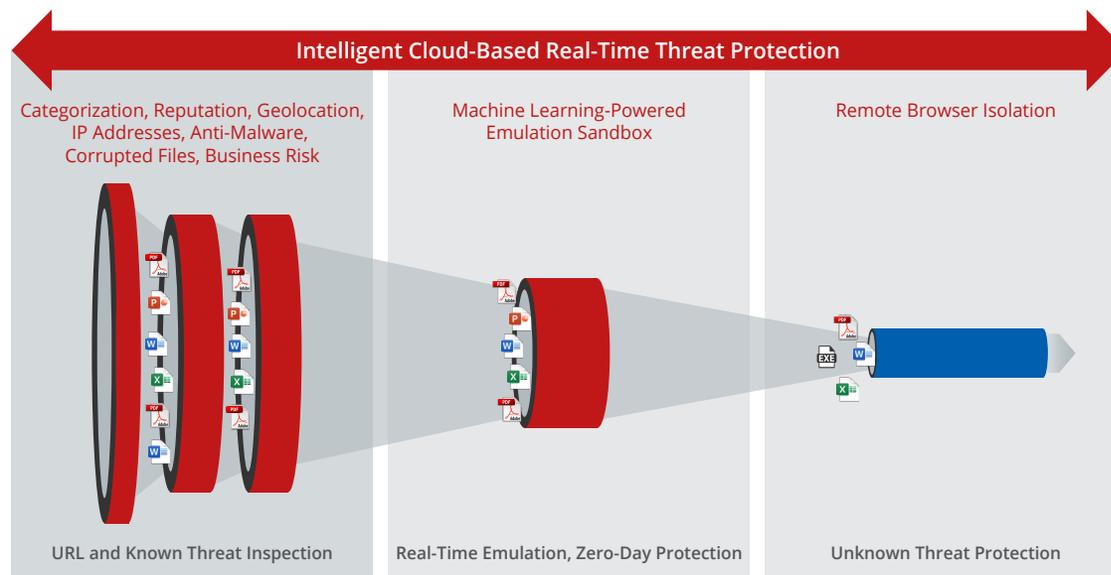

Figure 4. Defense-in-depth architecture provides zero-day malware protection with integrated multilayer security.

- Employ nine layers of protection technologies to ensure that threats never reach endpoints.
- Eliminate 20% more threats with real-time emulation sandbox and integrated Remote Browser Isolation.

Multi-vector Data Protection

More than 95% of companies today use cloud services, yet only 36% of companies can enforce data protection rules in the cloud at all. McAfee Next-gen Secure Web Gateway offers an effective way to enforce protection with built-in DLP templates and inline data protection workflows to help organizations comply with regulations. Its device-to-cloud data protection offers comprehensive data visibility and consistent controls across endpoints, users, clouds, and networks. When incidents do happen, administrators are able to manage investigations, workflows, and reporting from a single console. Integrated user and entity behavior analytics (UEBA) further protect business sensitive data by detecting and separating normal users from the malicious or compromised ones.

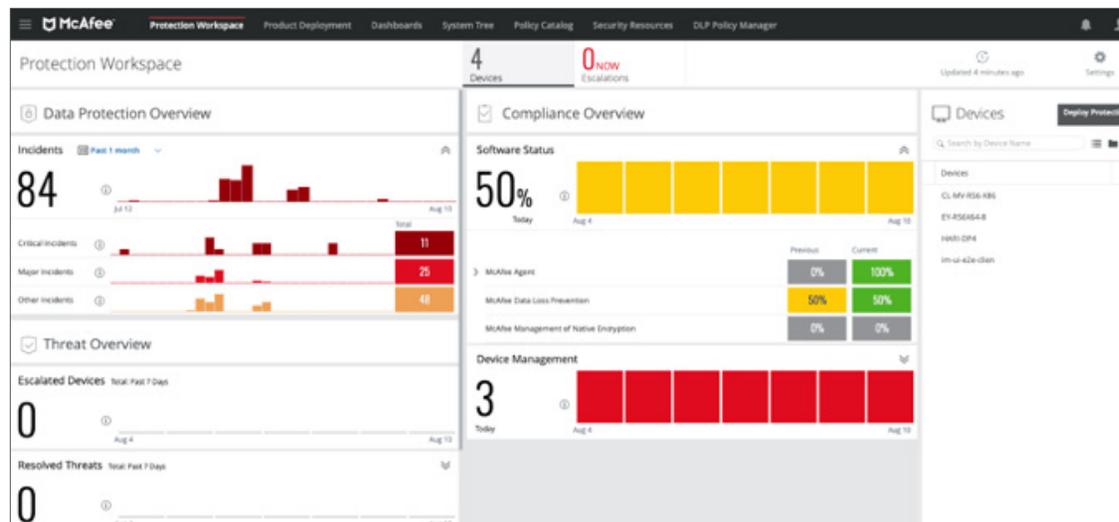- Extend existing DLP policies to the cloud with one click and in under one minute

Figure 5. Protection Workspace offers a consolidated view of compliance and data protection.

Summary

McAfee Next-gen Secure Web Gateway is a cloud-native web security solution that protects organizations from zero-day threats and enforces data protection across endpoints, networks, and clouds. It enables organizations to implement a simplified SASE architecture that delivers the security, scalability, and availability that is required for a distributed and remote workforce.

Learn More

For more information visit https://www.mcafee.com/enterprise/en-us/solutions/next-gen-swg.html.

1. McAfee Cloud Adoption and Risk Report, 2019

![McAfee]

6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com