Skyhigh Security

Skyhigh Security Secure Web Gateway (SWG)

Intelligent web security to protect your extended workforce

Skyhigh SWG for Cloud Granted FedRAMP High Authorization

Skyhigh Secure Web Gateway for Cloud has been granted Federal Risk and Authorization Management Program (FedRAMP) High Authorization. Increasingly, federal government agencies and government contractors are adopting cloud technologies to improve efficiency, support agility, and reduce costs. The FedRAMP authorization will allow these organizations to implement Skyhigh SWG, part of the Skyhigh SSE portfolio, to provide continuous secure access for the hybrid workforce, protect vital government information, and protect against today's advanced threats.

For more information about Skyhigh Security in the FedRAMP Marketplace, click here.

How we work has changed radically over the past several years. It's apparent that the shift to a hybrid, work-from-anywhere work model is here to stay: now that the pandemic has receded, more than 70% of U.S. employees plan to continue in a hybrid work environment.[1] Meanwhile, with more users requiring access to the web and cloud services, the attack surface continues to grow and so does the volume of cybersecurity incidents. With corporate data rapidly shifting to AI tools, data uploads to AI apps have grown by 80%. Furthermore, 11% of all files uploaded to AI applications contain sensitive corporate content, while less than 10% of enterprises have implemented data protection controls for data entering AI apps.[2]

Organizations are finding that they need to transform how they handle their networks and traffic in a world where valuable data resources no longer reside on corporate servers. They need a better way to protect sensitive data and users from advanced web-based attacks, exfiltration, and malware.

Skyhigh Secure Web Gateway (SWG) protects remote users from zero-day threats and data from exfiltration when they access the internet. It provides secure, continuous web connectivity for every device, user, and location. With integrated cloud access security broker (CASB) capabilities, a comprehensive, advanced data loss prevention (DLP) engine, and integrated remote browser isolation (RBI) at no extra cost, Skyhigh SWG is a complete, 100% cloud-based solution for keeping your users, their devices, and corporate data safe from web-based attacks.

Skyhigh SWG: best-in-class solution

With the volume and variety of internet threats increasing today, cloud-native SWGs have become indispensable for any organization that seeks to build security resilience—and especially for those that are on a cloud transformation journey and have adopted a hybrid or fully remote work model. Organizations are concerned about cloud or network outages, which may impact performance, lack of control over and visibility into the cloud operations, and protection for sensitive corporate data stored, used, and shared in the cloud.

Cloud-native Skyhigh SWG allays those concerns by extending protection between the boundaries of the corporate network, enabling secure web connectivity for every device, user, and location. As part of the Skyhigh Cloud Platform, Skyhigh SWG brings elevated security to your network and cloud transformation with infinitely scalable cloud capacity—without the need for expensive, high-maintenance appliances. As a best-in-class solution, Skyhigh SWG delivers exceptional performance and 99.999% availability, along with the industry's leading advanced threat protection capabilities, to ensure minimal latency and robust security. This is especially important, considering the rapid surge in cloud usage, with traffic to AI applications increasing by 200% over the last year, compared to 23% for non-AI applications, creating new bandwidth and traffic demands across hybrid environments.

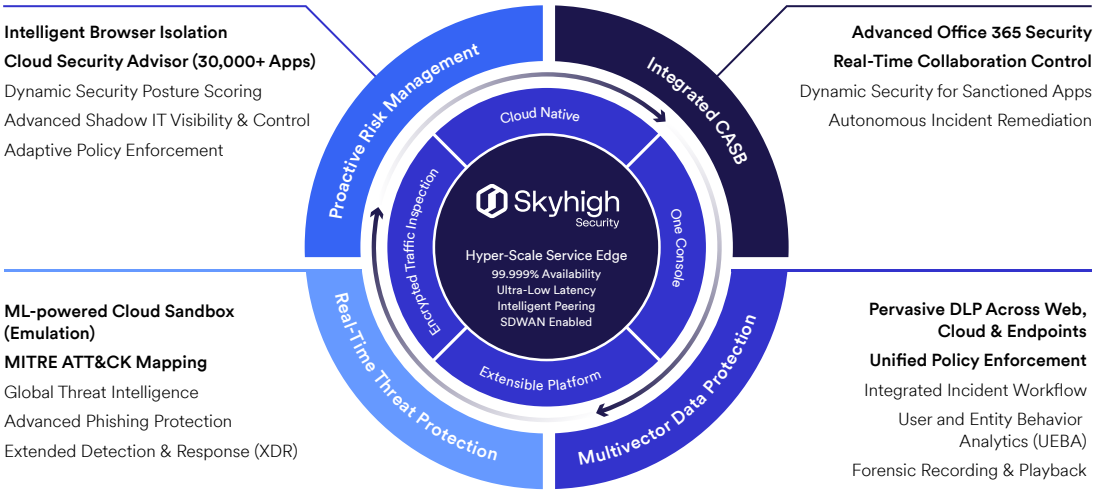
1 Source: https://www.gartner.com/en/documents/4013396
2 Source: https://www.skyhighsecurity.com/lp-2025-cloud-adoption-and-risk-report.html

KEY ADVANTAGES

- Provides unparalleled, advanced data protection to all websites and cloud applications and services.
- Maintains 99.999% service availability for continuous connectivity by re-routing web traffic as needed.
- Increases your cloud capacity in as little as 15 minutes, no longer waiting days to deploy a new appliance.
- Neutralizes zero-day threats and other malware with advanced threat protection, including built-in, fully integrated RBI.
- Expand visibility and control over access to cloud applications, including Shadow IT, and expand visibility and control over cloud usage to tackle the growing Shadow AI problem, where the average enterprise now utilizes 3,500 total cloud services (up from 2,400 in 2023) and 320 unsanctioned AI cloud applications operating outside IT oversight.
- Accelerates your digital transformation to Skyhigh SSE.

Now you can empower your remote and hybrid workforce with a security service edge (SSE) that processes traffic for unauthorized access, data risk, and threats from anywhere in the world—without compromising security or speed. Centrally managed Skyhigh SWG applies the same consistent policies and level of protection when your users go to the cloud, regardless of whether they are working from home or at remote offices.

To further simplify your technology stack and minimize management complexity, Skyhigh SWG converges fully with your SD-WAN. And, if mergers and acquisitions (M&A) are on the horizon, you'll find it easy to add new users and get them up and running quickly.



Unmatched protection: DLP, threat protection, and RBI

Skyhigh SWG secures users and data with unified advanced protection.

Its industry-leading DLP engine safeguards your sensitive data and users across all vectors: the web, Security-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), and private applications. Integrated with Skyhigh SWG, the DLP engine protects sensitive data from flowing out of your organization or being accessed by the wrong people in real time. This prevents your data from being uploaded to unauthorized websites. DLP policies are enforced through multiple methods, and, if incidents arise, you can swiftly remediate issues based on severity through quarantine, deletion of malicious content, coaching users, and other techniques.

Enterprise-grade threat protection scans content for viruses and malware, detecting known or zero-day threats in real time. Emulation sandboxing stops threats in their tracks and isolates them from your environment, allowing you to analyze how they work and what you can do to stop them. Automated threat protection controls reduce the number of alerts and incidents that security teams need to respond to.

BUSINESS BENEFITS

Zero-day malware protection

- Keep threats from ever reaching your users with multi-layer security and fully integrated RBI.

Unparalleled protection for sensitive data

- Protect sensitive data by extending zero trust principles beyond access to data use with the most advanced DLP framework in the industry.

Uninterrupted access with minimal latency

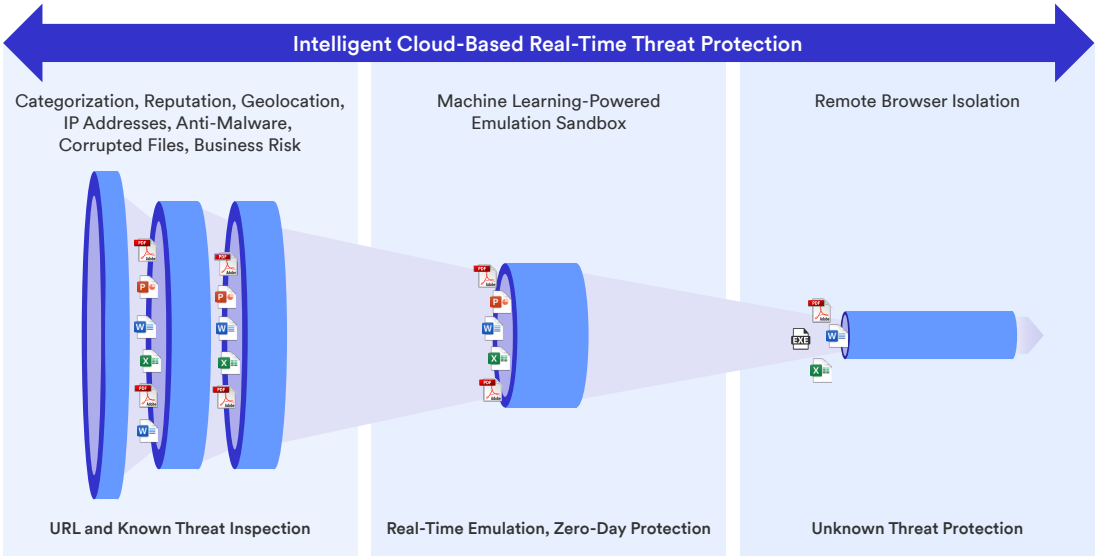
- Provide users with continuous access to the internet, corporate networks, and cloud applications, and empower your remote workforce to be more productive with 99.999% uptime covered by a strong SLA.

Reduced total cost of ownership and management complexity

- Ease the burden on security teams with single-console management for policies, incidents, and workflows across multiple environments, enjoy cost savings from reduced hardware and elimination of expensive MPLS traffic, and increase performance, reliability, and scalability.

Also fully integrated at no extra cost is Skyhigh Security's remote browser isolation (RBI) technology, which provides a safe and seamless web browsing experience for users. It automatically eliminates threats from potentially malicious websites, emails, links, ads, and downloads by ensuring that malicious code never comes near a user's device. It also leverages user and entity behavior analytics (UEBA) so you can gain insights into user web activities to help you maintain compliance and monitor insider threats.

Consistent policies, data protection, and visibility across isolated and non-isolated traffic work together to help you improve overall operational efficiency. Since Skyhigh SWG fully converges with the Skyhigh Cloud Platform, you can add additional security services as required—all managed by the same console.



Skyhigh SWG for Hybrid: extend your on-premises policies to the cloud

Combine the strength of appliances with the power of the cloud. The hybrid deployment mode for Skyhigh SWG allows organizations the flexibility to move to the cloud at their own pace, while keeping the necessary on-premises appliances – all managed from a single console. This hybrid model extends the same classifications and security policies for web access for both on-premises and cloud users in just a single click. This means that you can enforce the same sophisticated policies for your entire hybrid workforce, while avoiding the additional time and effort of rewriting your policies from scratch.

Skyhigh Security is the first, and one of the only, vendors to offer this powerful deployment mode.

The industry-leading data-first Skyhigh Security Service Edge (SSE) Platform

Skyhigh Secure Web Gateway is part of the unified Skyhigh Cloud Platform that integrates multiple innovative security technologies—Zero Trust Private Access (ZTNA), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), and Remote Browser Isolation (RBI) —all managed from the same central console. The Skyhigh Cloud Platform enables fast, reliable, and safe work-from-anywhere and digital transformation by securing web, cloud, and private applications.

KEY USE CASES

Comprehensive, advanced protection against online threats

- Protect users from malware and data loss with multi-layer security: scan all downloads against known and unknown threats with our machine learning-based emulation sandbox and against potentially malicious sites with RBI.

Flexible access control

- Integrate with the Skyhigh CASB Cloud Registry to restrict access to unsecure or non-corporate websites based on categories, reputation, and risk. Apply different policies to personal and corporate tenants, prevent potential infections and data loss, and enforce corporate internet browsing policy.

Advanced data protection:

- Apply DLP policies to web traffic and sensitive data to prevent exfiltration of sensitive data to unsanctioned cloud applications while monitoring usage through a single, easy-to-use dashboard.

Robust policy engine:

- Take advantage of predefined features, and augment them with your own use cases without waiting for product revisions.

The Skyhigh Cloud Platform addresses the complexity of remote workforce deployments with centralized visibility and incident management, adaptive and tailored access control, end-to-end data protection, and advanced threat protection. By partnering with leading SD-WAN vendors, Skyhigh Security delivers cloud security with a simplified, reliable, and low-latency service that aligns with your roadmap for your SSE journey.

Being data-aware means that the Skyhigh Cloud Platform provides modern data protection policies for data in motion and data at rest that determine what can be accessed, what can be shared, and how it can be used. It goes beyond zero trust by monitoring user actions to identify risky behavior: sites visited, personal or work devices, employee or contractor, type of data, and many other factors. It ensures sensitive data is accessed, shared, and stored appropriately.

Large enterprises across all sectors—from government agencies to financial institutions—look to Skyhigh Security to protect their data across their hybrid infrastructure. Our customers include nearly half of the Fortune 100 and more than a third of the Fortune 500.

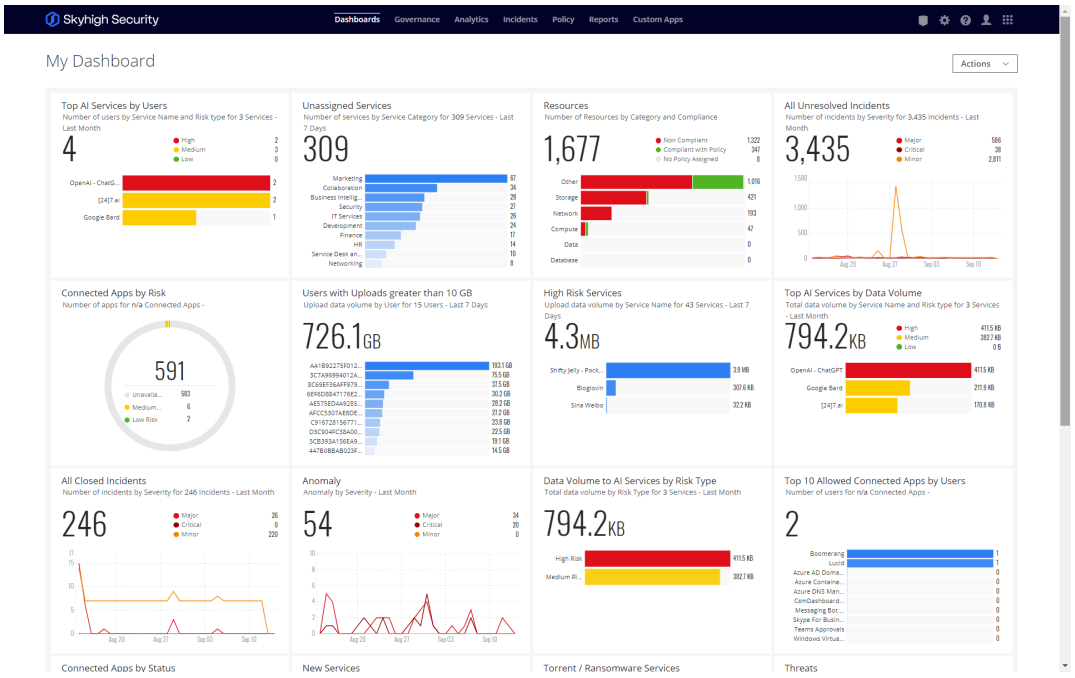


Figure 3. A single pane of glass management interface to manage web-based and cloud-based risks and threats.

Skyhigh Cloud Firewall

- For an extra layer of security for web traffic, Skyhigh SWG also integrates seamlessly with Skyhigh Cloud Firewall, which extends protection to all IP-based ports and protocols (UDP, TCP/IP, RDP). When Skyhigh Cloud Firewall detects HTTP and HTTPS traffic on non-standard ports, it routes that traffic to Skyhigh SWG. Only the traffic that needs deep content inspection is sent to Skyhigh SWG, while the rest takes a faster path for better throughput. Skyhigh Cloud Firewall even uses the same client as Skyhigh SWG, making it easy to deploy and manage.

Skyhigh SWG features

The industry's most advanced data protection engine: Protects sensitive data from being uploaded to unauthorized websites across all vectors—web, SaaS, IaaS, and private applications—through multiple advanced technologies:

- **Exact data matching (EDM):** Accurately fingerprints large structured data stores with billions of cells 1,000 times faster than other solutions and swiftly deploys data protection rules to prevent exfiltration and inappropriate sharing across all applications.
- **Indexed document matching (IDM):** Safeguards unstructured data in text documents and image files through fingerprinting and indexing. IDM detects proprietary information in PDFs, documents, JPEG images, and more. Once data is fingerprinted, you can add a DLP policy rule to leverage that indexed data and further reduce the risk of data loss.
- **Optical character recognition (OCR):** Extracts text out of documents and images and scans these for sensitive information, empowering you to prevent data misuse, loss, and theft.

Enterprise-grade threat protection: Provides zero-day malware protection by integrating RBI, machine learning, emulation-based sandboxing, and real-time global threat intelligence.

- **Natively integrated RBI:** Offers the most powerful form of web threat protection available, preventing malicious code from touching the end user's device. RBI is available at no extra cost, something that no other vendor in the market can claim.
- **Cloud risk mitigation:** Allows users to securely use the web and cloud apps from anywhere and stay productive.
- **Automated threat protection controls:** Reduces the number of alerts and incidents that security teams need to respond to.
- **Consistent policies, data protection, and visibility:** Applies the same level of capabilities across isolated and non-isolated traffic, improving overall operational efficiency.

Fully customizable Policy Code: Modify the code for the web policy as needed. This empowers you to address even the most unique use cases, without having to wait for future releases. This incredible level of granularity and customization takes your policies beyond out-of-the-box setup.

Application visibility and control: Blocks access to websites based on categories, reputation, or risk. It applies different policies to personal and corporate tenants, prevents potential infections and data loss, and enforces internet browsing policy. You gain expanded visibility and control over access to cloud applications, including Shadow IT.

URL and category filtering: Blocks access to risky and/or malicious content and phishing sites and prevents malware.

For More Information

Provide your remote workforce with continuous, high-performance connectivity while protecting them from web-based threats and preventing data exfiltration with Skyhigh SWG.

Visit us to learn more, or contact your sales account manager or partner.

About Skyhigh Security

When your sensitive data spans the web, cloud applications, and infrastructure, it's time to rethink your approach to security. Imagine an integrated Security Service Edge solution that controls how data is used, shared, and created, no matter the source. Skyhigh Security empowers organizations to share data in the cloud with anyone, anywhere, from any device without worry. Discover Skyhigh Security, the industry-leading, data-aware cloud security platform.

For more information visit us at skyhighsecurity.com

Skyhigh Security

3099 North First Street
San Jose, CA 95134
888.847.8766
skyhighsecurity.com

Skyhigh Security is a registered trademark of Musarubra US LLC. Other names and brands are the property of these companies or may be claimed as the property of others. Copyright © 2026.
July 2026. DS-EN-000001-02