citrix

Solution Brief

Secure Internet Access

Securing the Hybrid Workforce with Comprehensive, Cloud-delivered Security

One Cloud-Delivered Security Service to Protect All Web and SaaS Access

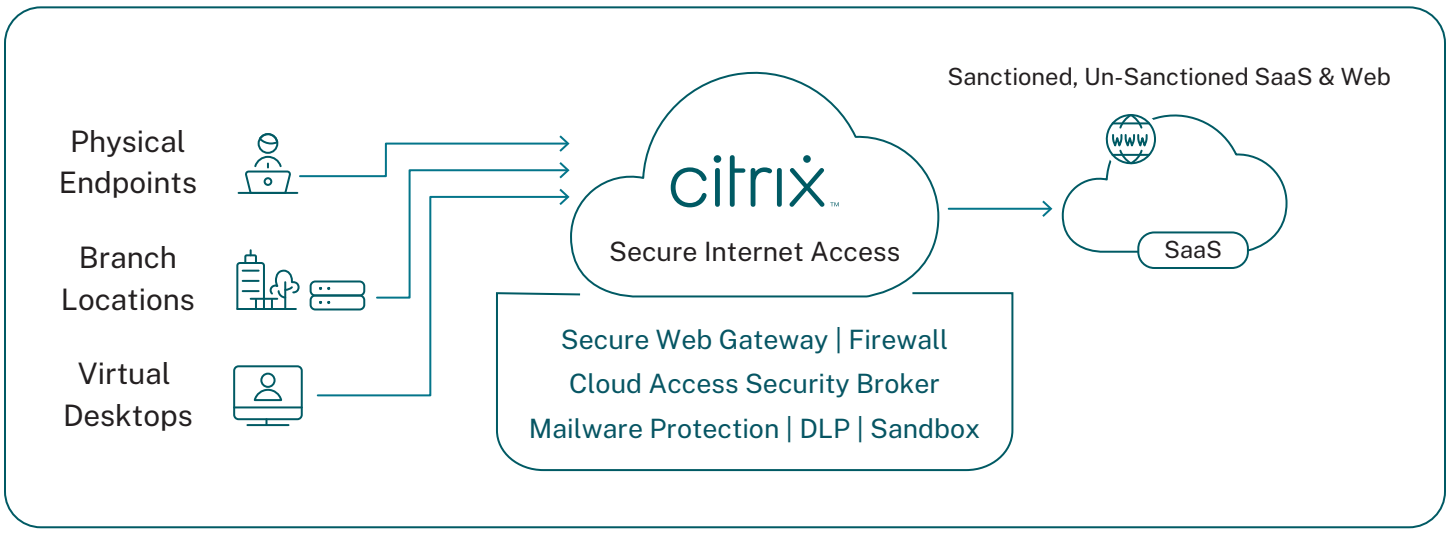
Your enterprise data is only as secure as your most vulnerable endpoint. As threats become more sophisticated, are almost always encrypted, and evolve faster than patches can be pushed, traditional security solutions fail to protect hybrid workers, while also impacting application experience and increasing operational costs.

Cloud-delivered security solutions are the answer and Citrix Secure Internet Access (CSIA) offers the functionality needed for strategic network and security modernization. CSIA is a comprehensive, cloud-delivered security service. It replaces traditional, on-premises security appliances with a globally available, highly resilient, and scalable cloud, delivered through over 100 points of presence (PoP).

Every point of presence has a full security stack, including secure web gateway (SWG), firewall, intrusion prevention system (IPS), malware protection, sandbox, data loss prevention (DLP), cloud access security broker (CASB), and anomaly detection. All these security services can be consumed based on your specific security needs.

CSIA operates between your users and your apps and web (in-line). This means all traffic, including SSL/TLS, is protected against the latest, most advanced cyberthreats, without added latency from backhauled connections. In addition, global peering with popular application and cloud services reduces the number of hops to access business-critical services.

CSIA offers multiple options for steering traffic to the nearest points of presence. This includes a lightweight software agent on popular endpoint operating systems, ensuring that all your remote and home-based workers remain protected, everywhere.



Minimize Risk Exposure

Minimize exposure by managing access to:

- Up to 81 web categories
- URLs, URLs containing risky keywords
- Up to 11 browsers and 13 operating systems
- Geo locations, IP addresses and ports
- Evasive apps and services (e.g., Tor, Psiphon)
- High-risk protocols (e.g., SSH,RDP, SSL on non-standard ports)

Block Malware

Identify and block threats in all traffic:

- Inspect SSL/TLS at scale to block encrypted threats
- Block latest malware with near real-time updates from 10+ threat engines
- Analyze behavior of suspicious files and URLs in a cloud sandbox
- Over 60 IPS rule categories with automated updates from 3rd party systems
- Granular anomaly detection and alerts

Prevent Data Loss

Prevent data loss from careless and malicious insiders, malware:

- Block access to personal accounts, e.g., Office 365, Gmail, Google Drive, Slack
- Block file uploads to storage apps, e.g., Box, Dropbox
- Detect sensitive data even in encoded and encrypted streams, e.g., PII and Credit Cards in Base64 and Zip files
- Granular, combinational rules using Boolean operations
- File capture for forensics and optimization

Identify & Manage SaaS

Identify and control sanctioned and unsanctioned SaaS access:

- Identify and enforce in-line control on shadow IT
- Granular control on social apps, e.g., block comments on Facebook for everyone except marketing teams
- Block specific SaaS services, e.g., individually control 18 services from Google
- Restricting HD playback on YouTube, block streaming apps, bandwidth shaping for specific domains

Alert on Risk & Incidents

Accelerate incident identification with user and network analytics:

- User risk dashboard based on behaviour analysis
- Real-time user activity monitoring with alerts
- Log forwarding to Splunk (no need for forwarding service)
- Native dashboards including DLP, intrusion prevention, and bandwidth consumption
- Automated, schedulable reports based on custom or pre-built templates

Partial functionality list

Challenges Solved with Citrix Secure Internet Access

Protection without compromise: CSIA offers all the functionality you need to protect web and SaaS access. A cloud-native architecture ensures full SSL/TLS inspection at scale. Web filtering and access controls such as blocking browsers or operating systems with known zero-day vulnerabilities minimizes risk exposure. The latest threat intelligence updates and behavioral analysis capabilities within a cloud sandbox environment identify and block even the most advanced malware. Powerful DLP engines ensure that sensitive data cannot be exfiltrated by careless insiders, malicious insiders, or malware. CASB controls, including integration with Microsoft CAS, enables identification and granular control on sanctioned and unsanctioned SaaS apps. Finally, user-level analytics enables proactive risk identification and remediation even for mobile and home-based workers. All of this is delivered as a unified service without the need for hardware or manual updates.

Secure employees everywhere: CSIA is critical to protect every employee within your hybrid workforce when they access web and SaaS applications. A software agent installed on each employee endpoint device steers traffic

Sample Policy Set with Citrix Secure Internet Access

(The below is only a sample and hence only represents fractional amount of the functionality in CSIA)

- Register following instances in with static public IPs of
  - Usa-west1 with static public IP: 114.229.173.25
  - Emea-west1 with static public IP: 146.221.165.20
  - Apj-east1 with static public IP: 104.100.120.25
- Block web categories relating to Adult Content, Drugs, Guns & Weapons, Violence & Hate
- Block download of .py, .js and .jar files for all user groups except software developers
- Block use of Tor, Psiphon, OpenVPN, BitTorrent, OpenSSL
- Block SSL on non-standard ports, RDP connections
- Only allow Microsoft domain “acme.com”
- Block Job Search on LinkedIn for all employees
- Block posts, comments, uploads, chats, games on Facebook and Twitter for all employees except marketing
- Block file uploads to DropBox, Box and Google Drive
- Block access from any country except USA, Brazil, United Kingdom, Italy, France, India or Singapore
- Only allow access to “Acme Corp Videos” library on YouTube by all employees except marketing
- Detect credit card numbers, credit card stripe data or PII in any egress data, even if encoded or compressed as Base16, Base64, Zip, GZip, or RAR; enable capture of violating file
- Report events where packet sizes do not match the value specified in the packer header length field
- Stream malware and reputation defense feeds from threat intelligence engines for malware scanning
- Detect and alert if traffic from any of the following deviates by 20% away from baseline
  - FTP port 21
  - SSH port 22
  - Telnet port 23
  - DNS port 53
- Generate a report on the following queries:
  - Top Infections
  - Top Domains Hosting Malware
  - Tops Devices by Infections
  - Advanced Threat Analysis

to CSIA ensuring all employees remain consistently protected with the full security service regardless of their physical location. This makes CSIA a critical component of VPN replacement initiatives where fast and secure access is required. Employees protected by zero trust network access (ZTNA) for internal apps or digital workspace solutions for sanctioned apps, must be protected by CSIA when accessing web and SaaS applications.

Reduce trouble tickets from poor application performance: CSIA is distributed across over 100 PoPs globally, enabling users to connect to the nearest PoP, thus minimizing latency. CSIA is a cloud-native service that auto scales as more users or applications are added, or as the volume of SSL/TLS traffic increases. Additionally, CSIA is built on a single-pass architecture that ensures all encrypted data packets are decrypted and inspected by all policy engines concurrently. This helps delivers a better user experience than traditional service chained architectures in which data packets are decrypted and inspected multiple times.

Modernize yet simplify: Citrix converges multiple security capabilities that are often delivered by separate security vendors into one cloud-delivered service. This means there is no hardware to manage, and software and threat intelligence updates are automated. Simple licensing upgrades also allow scaling to new users and adding new security services with ease. Integration with other Citrix or 3rd party services like Microsoft CAS and Splunk is easy through comprehensive API integrations.

Accelerate your journey to Secure Access Service Edge (SASE): Your SASE architecture implementation can begin with CSIA and extend to zero trust network access (ZTNA) and SD-WAN based on your IT roadmap timelines. Integrations between Citrix products make this transition simple. These include:

- Single UI experience with Citrix zero trust access, SD-WAN, and analytics solutions
- Automated and highly available connectivity between Citrix SD-WAN appliances and CSIA[1]
- Single vendor experience for easier procurement, implementation, and troubleshooting

Only subset of PoPs shown on the map

How is Citrix Secure Internet Access Different?

Data privacy and control with instance-based architecture: While CSIA is a cloud-native service, you can provision segregated 'instances' or 'nodes' within your deployment. These 'instances' offer you greater control on your data, ensuring sensitive information, such as encryption keys, remain within the confines of the instance. This simplifies meeting privacy and regulatory compliance requirements, such as GDPR.

Static IP addresses for SaaS and cloud service integration: Each enterprise customer instance is allotted static IP addresses which can be added to permit/deny lists of upstream SaaS and cloud applications. This simplifies integrations with upstream services.

Protection for all workers with broad OS support, including ChromeOS and Linux: CSIA Cloud Connector agent is supported across Windows, MacOS, ChromeOS, iOS, Android, and Linux. This ensures that your security architecture can protect users even as you support mergers and acquisitions, Choose Your Own Device (CYOD) initiatives, or Linux-based IoT deployments.

Does not break existing shared desktop deployments: Citrix Virtual App and Desktops (CVAD), terminal services, remote desktop services, and Windows 10 multi-user deployments offer shared desktops, which enable multiple users to use the same machine. This model reduces costs by increasing user density per machine. CSIA also allows granular, per user security policy even in shared deployment models.

Unified management and single-vendor logistics: Citrix SIA is managed from the same Citrix Cloud console as all other Citrix products enabling a familiar and seamless single-pane-of-glass administration experience across Citrix products. Automation between Citrix products, such automated and 'dual resilient' tunnels between Citrix SD-WAN and CSIA, further accelerates operations. Streamlined licensing, shared technical support and customer success teams, and strong integrations between Citrix products ensures operational ease and agility, now and in the future.

Predictable per-user pricing: CSIA is available in three easily consumable Editions with minimal "add-ons" to ensure transparency in pricing.
For instance:

- Essential functions such as SSL decryption and log streaming are included as default functions in the Basic Edition
- Advanced or Premium Editions offer all functions for Malware Protection and Data Loss Prevention, without "add-ons" needed for complete functionality

Pricing is per user, rather than per device, with each user allowed multiple devices. This ensures that your costs remain the same, even though your employees may eventually add new tablets, mobile phones or laptops to their work environment.

Achieve Multiple IT and Business Objectives with One Solution

CSIA offers comprehensive, cloud-delivered functionality through a unique architecture that offers greater privacy and control of your data. It protects all your employees, regardless of their location, against the most advanced threats. Automation, management plane integrations, licensing and logistical alignment with other Citrix products delivers a uniquely simple experience in procurement, implementation, training, support, and scale. As a result, you benefit from:

Lower cyber risk	→	Lower risk to revenue and reputation loss
Higher agility and scalability	→	Business resiliency, support organic and inorganic growth
Higher IT operational ease	→	Redirect focus on strategic projects
Better app performance	→	Better employee collaboration, productivity, and morale

For more information about Citrix Secure Internet Access, **request a product demonstration.**

[1] Note – CSIA can interoperate with any SD-WAN vendor in your environment. However, Citrix SD-WAN is recommended since automations between Citrix SD-WAN and CSIA simplify and accelerate your operations.

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States