Cisco Secure Access and Chrome Enterprise Integration

A powerful combination of local and cloud-based security to protect users, data, and applications

Cisco® Secure Access and Chrome Enterprise work together to deliver robust workforce protection for browser-based applications and resources. This joint solution offers a streamlined way to access applications while safeguarding against data breaches and phishing attempts, and also enforces Zero Trust access controls. Employees and the extended workforce can work confidently with transparent and easy-to-manage identity, Data Loss Prevention (DLP), and other security controls. Together, Cisco Secure Access and Google Chrome Enterprise Premium enable you to protect your private applications and maintain control over your sensitive data, allowing users to work securely from anywhere on any managed or unmanaged device.

This integration brings browser-based threat and data protection from Chrome Enterprise to web apps secured by Cisco Secure Access. As more work activities occur on web applications, an integrated enterprise browser and Security Service Edge (SSE) solution can strengthen and simplify endpoint and access security as part of a broader zero trust approach.

Benefits

Overall, this integration delivers an advanced set of security and control capabilities along with a streamlined user experience and simplified management processes.

Advanced, granular, Zero Trust security

The joint solution protects users, data, and apps through streamlined Zero Trust access from managed and unmanaged devices with granular controls. In addition, independent user-to-app traffic streams and hidden app locations provide unmatched protection against reconnaissance, active threats, and lateral movement. Lastly, an efficient combination of browser and cloud-based DLP controls secure sensitive data, including outgoing and incoming generative AI-related content, and protects against copying, pasting, printing, and screenshots.

Frictionless user experience

A good user experience is critical to preventing user subversion of security controls. This solution improves the end user process by removing the need for the manual, multi-step, agent, and VPN connection process, significantly simplifying the user experience. It provides a one-step, fast connection to private applications from the Chrome Enterprise browser though Cisco Secure Access, making it easier for users to access work resources from a wide variety of devices and locations. Users' devices go through an automated and seamless trust process instantly at login, which ensures they have a strong security posture.

Simplified management

Streamlining administrative tasks is another major goal in complex security and networking environments. It starts with the deployment process, where agentless device trust capabilities simplify this process. To improve detection times, make investigations easier, and facilitate rapid remediation, data is shared from ChromeOS to Cisco Extended Detection and Response (XDR) and will be expanded to include Chrome Enterprise. In the future, policies for private applications created in Cisco Secure Access will be shared with Chrome Enterprise for better visibility and local enforcement as appropriate.

Better together

Cisco Secure Access (SSE solution) protects users, data, and devices as they securely access private applications, SaaS applications, and the internet, from on or off the corporate network. It provides seamless and secure access from anything to anywhere leveraging modern and secure protocols. Users enjoy a better experience, IT/security teams simplify operations, and the organization increases security via granular controls. Cisco's SSE solution unifies multiple cloud-native capabilities such as Secure Web Gateway (SWG), Zero Trust Network Access (ZTNA), Digital Experience Monitoring (DEM), AI security, Firewall as a Service (FWaaS), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), Remote Browser Isolation (RBI), DNS-layer security, and more.

Google Chrome Enterprise brings organizations a secure and reliable enterprise browser that employees love, with key management tools for IT and important local security capabilities. Organizations using Chrome Enterprise benefit from Google's world-class threat intelligence, AI-powered security features, and Zero Trust access via Google's secure global network, ensuring data protection and user safety. Chrome Enterprise includes threat protection that delivers content inspection and data loss prevention, anti-malware, and anti-phishing using frontline intelligence and AI, dynamic URL filtering, and site categorization.

The unique combination of these two tools results in higher user productivity and increased threat protection across distributed work environments. Cisco's Secure Access delivers a robust set of secure internet access and secure private app access, as well as security functions. Chrome Enterprise browsers provide an automated device trust process and rich set of local security functions. Together they deliver improved security posture and increased user satisfaction along with a more flexible and streamlined management process.

Key use cases

- **Secure replacement for Virtual Desktop Infrastructure (VDI)**
  Virtual desktop environments have historically been a popular way to give remote or part-time workers access to a controlled set of applications. In today's world the need for this type of dynamic access is growing. Unfortunately, VDI and other traditional remote access methods have many disadvantages when compared with more modern solutions. VDI is expensive to deploy and manage. Significant changes in the amount of traffic, number of users, and applications require a cumbersome set of administrative tasks and upgrade costs. The security posture for VDI on its own is low, and organizations usually have to subscribe to multiple separate security tools to try and protect their users, data, and applications. The integrated combination of Cisco Secure Access and Chrome Enterprise Premium provides a modern, streamlined approach that is simpler to deploy and manage. It delivers a unique combination of local and cloud-based security that protects your organization and data. This low-cost approach provides additional adaptability to accommodate business and workforce changes in a rapid and efficient manner.
- **Flexible support for multiple BYOD scenarios**
  Most organizations allow BYOD for access to a set of applications, and recent developments have increased the variety of user and device types that need to be supported. Identity and data security are important concerns in all of these extended use cases. Cisco Secure Access and Chrome Enterprise provide a flexible solution that enables any browser capable device and enforces a consistent set of security to detect and block threats.
- **Contractor least privilege access**
  Utilization of contractors is a common practice in the current dynamic business environment. The ability to quickly and efficiently onboard and activate new contractors and give them the appropriate “least privilege” access to the applications they need is essential. The Cisco Secure Access and Chrome Enterprise solution provides a highly efficient method to handle the full lifecycle of secure access for contractors. Quick activation, high performance access to the appropriate resources and an immediate, secure disengagement is essential for a positive contractor experience and a secure outcome for the organization.

Additional resources

- Cisco Secure Access and Chrome Enterprise Solution Guide
- Cisco Secure Access
- Chrome Enterprise