SECURE EDGE DATASHEET

Product Overview

As distributed workforces become prevalent, the way we secure the network edge is changing, giving way to new cloud-based architectures. With so many options available, organizations need the flexibility to leverage existing investments and seamlessly transition to a cloud-delivered architecture, securely and at their own pace. Juniper Secure Edge provides full-stack Security Service Edge (SSE) capabilities to protect access to web, SaaS, and on-premises applications and provide users with security that follows them wherever they go. When leveraged with Juniper's AI-Driven SD-WAN, Juniper Secure Edge provides a best-in-suite SASE solution that helps deliver seamless and secure end-user experiences that leverage existing architectures and grow as you expand your SASE footprint.

Product Description

Juniper® Secure Edge delivers full-stack Security Service Edge (SSE) features, including Firewall as a Service (FWaaS), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), and advanced threat prevention. It empowers organizations to secure their workforce wherever they are. Users have fast, reliable, and secure access to the applications and resources they need, ensuring great user experiences. IT security teams gain seamless visibility across the entire network, all while leveraging their existing investments, helping them transition to SASE at a pace that is best for your business.

Secure Edge capabilities are all managed by Security Director Cloud, your portal to SASE managing on-premises, cloud-based security, and cloud-delivered security — all within a single user interface (UI). When you add this together with Juniper's unique AI-driven SD-WAN solution, you have a cost-effective and reliable way to adopt a SASE architecture, regardless of where you are on that journey.

Architecture and Key Components

Organizations can support their remote workforce with Juniper Secure Edge. Whether they are in the office, at home, or on the road, Juniper Secure Edge provides secure access to the applications and resources workers need with consistent security policies that follow users and devices without having to copy over or recreate rule sets.

Juniper Secure Edge provides support for remote users wherever they are, where you can install a PAC file on remote devices and route those users to the nearest Secure Edge Point of Presence (PoP).

Similarly, for campus and branch users where Juniper AI-Driven SD-WAN is deployed, you can connect each site to the nearest Secure Edge PoP. Additionally, you can offload your security services to the nearest cloud. This process provides you with the benefits of several unique Juniper technologies, including Session Smart Routing, App Control, AppQoS, Mist AI insights, anomaly detection, and automated troubleshooting.

These services, combined with Juniper's full-stack SASE offering, enable organizations to protect applications and provide users with consistent and secure access, whether in the office, at the campus, or on the move.

Juniper Secure Edge creates a seamless SASE experience powered by AI that can take organizations from wherever they are — whether starting on-premises or in the cloud — and creates a common networking and security policy framework. By building on Juniper's expertise in using AI to optimize the network experience, Secure Edge leverages AI to enhance the experience for security practitioners so that risk decreases while simultaneously improving the end-user experience.

Figure 1: Secure Edge securely connects users in any location directly to application resources they need without sending traffic back to a centralized location for traffic inspection and threat protection.

Features and Benefits

Firewall-as-a-Service (FWaaS)

FWaaS identifies applications and inspects traffic for exploits and malware with over 99.5% effectiveness.

Juniper's FWaaS provides all next-generation firewall (NGFW) features as a service, delivered via Juniper's managed cloud. It leverages public cloud points of presence, ensuring fast access to applications anywhere users are, whether they are "on the network" or not. This unique architecture enables Secure Edge to provide traffic inspection and control with ultra-low latency.

Secure Web Gateway (SWG)

SWG protects web access by enforcing acceptable use policies and preventing web-borne threats.

Juniper's SWG provides web traffic control through granular URL-based policies, content inspection, selective SSL decryption, and Encrypted Traffic Insights to protect against web-based attacks even when decryption isn't possible. The SWG filters out non-compliant web sites and removes malware from allowed web traffic. To accomplish this, the SWG includes URL filtering, intrusion prevention, selective SSL inspection, and machine-learning-based malware detection that also profiles HTTPS connections for malicious traffic.

Cloud Access Security Broker (CASB)

CASB provides visibility into SaaS applications and granular controls to ensure authorized access, threat prevention, and compliance.

Juniper's CASB secures SaaS applications from unauthorized or inadvertent access, malware delivery and distribution, and data exfiltration. It allows organizations to leverage their existing technology investments, whether customers are starting on-premises with campus and branch use cases, in the cloud with remote workforce use cases, or a hybrid approach.

Data Loss Prevention (DLP)

DLP classifies and monitors data transactions and ensures business compliance requirements and data protection rules are followed.

Juniper's DLP reads files and classifies content, such as credit card numbers, social security numbers, and addresses, and tags the file as containing a specific type of data. That data gets consumed by the organization's DLP policy. This policy is essential; as an organization adds granular controls for documents, they can add tags such as HIPAA and PII. If a user attempts to remove data from the organization, Juniper's DLP stops that from happening.

Advanced Threat Prevention

As the threat landscape evolves and security risks accelerate, you can no longer rely on a single device at the network edge to identify and block threats. Instead, you need a threat-aware network that frees your security analysts to focus on hunting unknown threats and further reduces risk to your organization.

Advanced Threat Prevention discovers zero-day malware and malicious connections, including botnets and command and control (C2), even when traffic cannot be decrypted. It enforces granular mechanisms, such as file quarantine and reduced access rights.

As part of Juniper's Advanced Threat Prevention, Juniper SecIntel provides threat intelligence to all points of connection across the network to block malicious traffic, creating a threat-aware network. To reduce risk, SecIntel can be deployed at the WAN edge, across wired and wireless LANs to increase threat visibility, and at enforcement points within the network.

Secure User Access

Support the remote workforce in the office, at home, or on the road with fast and secure user access to the applications and resources people need to do their jobs effectively. Security policies are based on identity and follow the user wherever they go.

The follow-the-user policy provides automated access to third-party contractors through granular risk-based controls, locking down third-party access as an attack vector. Secure Edge policy can be configured so that third-party access to resources requires additional verification, and access can be automatically revoked according to a scheduled end date. Contractors and third parties will no longer have access once their contracts are complete.

Users have seamless and secure access to corporate resources without jumping through hoops associated with multiple authentication portals or backhauling traffic to a data center.

Administrators can control their risk level by ensuring that consistent security policy is applied to users, whether accessing sensitive resources from their couch or browsing the Internet from the office.

Single-Policy Framework

Secure Edge uses the same policy framework as the SRX Series Firewalls. This means that administrators can easily apply policies created for their SRX Series firewalls to remote users and branch sites routing to the nearest Secure Edge point of presence.

Administrators do not need to recreate policies by hand or determine where to place each rule. Secure Edge does all this automatically, making it much easier to ensure that user, device, and application security rules are consistent across the edge and into the data center, creating fewer policy gaps, eliminating human error, and making the entire network more secure.

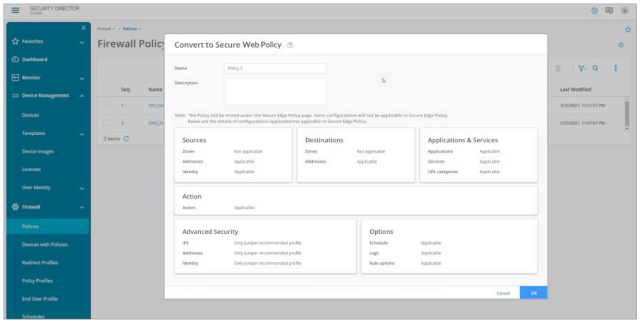

Figure 2: Unified management coupled with a single policy framework ensures security policies created for physical or virtual firewall deployments can easily and automatically apply to sites where Secure Edge delivers those same policies as a service.

Leverage Existing Investments

Transitioning to a cloud-based security architecture shouldn't mean abandoning existing IT investments. Secure Edge allows organizations to transition to a Secure Access Service Edge (SASE) architecture at their own pace and doesn't force administrators to toggle between separate management platforms for on-premises and cloud-delivered security. All deployment, configuration, and management are done through Security Director Cloud—the same management platform that manages all SRX Series firewalls.

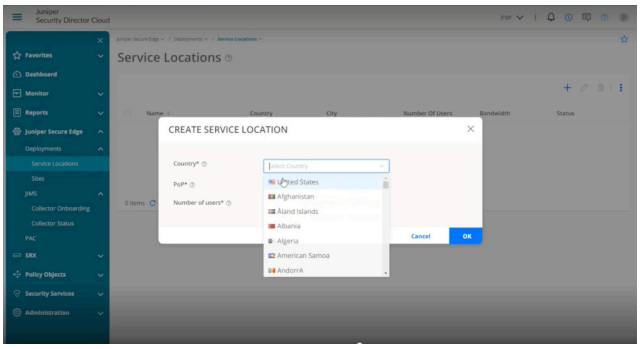

Figure 3: Easily manage site deployment and configuration, user authentication, and policies from anywhere through an easy-to-use Web interface.

In addition, organizations that love their existing identity solutions don't need to rip and replace them. Secure Edge works with all leading identity providers, such as Microsoft Azure Active Directory and Okta. It works through Security Association Markup Language (SAML) 2.0 support and any router that supports generic routing encapsulation (GRE) or IPsec.

Security Assurance

Whether it's a rule for a traditional firewall policy or a policy delivered as a service, it's important that rules are placed in the proper order, so they're effective when needed. However, rules can quickly add up, leading to outdated, shadowed, and therefore ineffective rules. Also, duplicates require hours from administrators who must sort through hundreds or even thousands of rules before they can confidently make changes.

Because Secure Edge is managed through Security Director Cloud, duplicate and shadowed rules are automatically surfaced before they're committed. Rule hit counts are highlighted so administrators can quickly make changes, ensuring that new and existing policies are effective for the intended users at the intended time.

Proven Security Effectiveness

It's not enough that a cloud-delivered FWaaS, SWG, CASB, DLP, and advanced threat prevention are easy to use. The security services controlling traffic and user access and inspecting threats must also be effective. The threat prevention features delivered as-a-service by Secure Edge are the same threat prevention features delivered on the physical, virtual, and containerized SRX Series firewalls. These features, including intrusion prevention, anti-malware, advanced threat prevention via Juniper Advanced Threat Prevention Cloud and Encrypted Traffic Insights, have been proven over 98.9% effective against server- and client-side exploits and 100% effective against malware by multiple third-party tests.

Delivering Best-in-class SSE

Juniper Secure Edge delivers best-in-class SSE as part of a full-stack SASE solution that empowers organizations to transition to a SASE architecture regardless of where they are on their SASE journey.

Juniper offers full-stack WAN edge and SSE that leverage the power of the cloud to optimize both the network and security experience.

Dynamic policies can be created to center around a user or group of users, or device or group of devices, so that access and threat protection rules are applied consistently regardless of geographic or network location. Administrators do not need to duplicate or recreate rule sets, helping increase operational efficiency and furthering Zero Trust initiatives within organizations.

Table 1: Secure Edge Features and Benefits

Feature	Benefit
Application visibility and control	Facilitates instant recognition and control of application access, including Software as a Service (SaaS) applications: the application name, description of the service, and inherent level of risk, regardless of port, protocol, or encryption method.
Secure Web Gateway	Ensures Web traffic remains free of web-borne threats and provides direct Internet access to users wherever they're located through a Secure Web Gateway functionality with SSL/TLS proxy and inspection capabilities.
Cloud Access Security Broker	Provides visibility into SaaS applications and granular controls to ensure authorized access, threat prevention, and compliance. Secures SaaS applications from unauthorized or inadvertent access, malware delivery and distribution, and data exfiltration.
URL filtering	Provides Web traffic categorizations that can be incorporated into application and security policy to automatically protect users from web-borne threats, such as drive-by malware downloads, phishing sites, and exploit kits. Secure Edge URL filtering also helps organizations maintain compliance by controlling Web access and preventing unwanted browsing activity.
Content filtering	Inspects e-mail, webpages, and files for unwanted and malicious content. Administrators can granularly control what content is allowed, restricted, or blocked within security policies.
SaaS Security	Provides greater visibility and control over SaaS applications, including data, usage, compliance, threat prevention and access, monitors and controls user behavior, and minimizes potential risks associated with use of unsanctioned apps, or "shadow IT."
Data Loss Prevention	Monitors and protects sensitive data as it transits between networks, users, and services, and at rest within SaaS applications. Prevents data leakage and excessive data exposure anywhere regulated data moves and resides, and in accordance with compliance requirements. Supports structured and unstructured data, data classification, Exact Data Match (EDM), Optical Character Recognition (OCR).
User identity	Integrates with identity services, such as Azure AD and Okta, to define policies and application use based on individual users or user groups. Provides visibility into application usage at the user level rather than IP address, providing powerful insights into application traffic traversing the network.
Dynamic user segmentation	Helps to limit third-party access as an attack vector with follow-the-user policies. Policies can be created to apply to users wherever they go, on or off the corporate network, providing automated access control to employees and third-party contractors.
Intrusion detection and prevention services (IDS/IPS)	Mitigates network and application exploits and protects against a range of attacks with signatures proven effective by multiple third-party tests. Juniper intrusion detection and prevention (IDP) constantly monitors new exploits against recently discovered vulnerabilities, keeping network protection up to date against the latest cyberattacks and stopping them at the exploit stage before they gain a foothold inside the network.
Anti-malware	Uses a constantly updated global threat database augmented by research from threat-sharing communities such as Cyber Threat Alliance, to protect the edge. Through in-line inspection and blocking, Secure Edge prevents known malware from installing on endpoints and blocks malicious outbound (C2) communications resulting from malware infections.
Domain Name System (DNS) filtering	Identifies domains with high-risk reputations, typically those associated with attack campaigns or containing unwanted content, and blocks communications to and from both the domain and associated IP address.
DNS security	Analyzes DNS queries for threat activity, such as tunneling, C2 communications, and domain generation algorithms, identifying compromise attempts and preventing additional infection. Identifies signs of DNS misuse that attackers employ to circumvent security controls.
Advanced threat protection	Leverages Juniper ATP Cloud, Juniper's global threat intelligence hub, for advanced threat protection to uncover and mitigate zero-day malware quickly and improve threat response times by taking real-time threat information and pushing it out to all points across the network. Juniper ATP Cloud has been proven effective against new and commodity malware by multiple third-party tests.

Feature	Benefit
Encrypted Traffic Insights	Restores threat visibility lost due to encryption, without the heavy burden of full TLS/SSL decryption. Secure Edge collects relevant SSL/TLS connection data, including certificates used, cipher suites negotiated, and connection behavior. This information is processed using network behavioral analysis and machine learning to determine whether the connection is benign or malicious. Malicious traffic can then be dropped, stopping threats such as botnets in their tracks.
Adaptive threat profiling	Leverages existing infrastructure to create security intelligence feeds based on real-time events occurring on the network. These feeds, unique to each organization, can be configured based on security policies and utilized by other enforcement points on the network to detect threats and update their infrastructure in real time, blocking potential attacks.
Compromised host isolation	Identifies compromised devices, which can be added to a quarantine list either manually or automatically, stopping those devices from accessing sensitive data and preventing the malware from spreading laterally.
Agentless on-ramp	Protects users with security policies through agentless functionality. Users log in through single sign-on (SSO) to securely access the applications and data they need.
SaaS Security Posture Management	Performs an automated assessment of your SaaS landscape against well-defined security guidelines, reducing the operational complexity in managing multiple apps, preventing data loss from misconfigurations, and ensuring compliance in a multi-cloud environment. Uses a prebuilt compliance libraries of common standards or best practices such as CIS Foundations Benchmarks, SOC 2, PCI, NIST 800-53, or HIPAA. Provides visibility and insights into third-party applications connecting to your SaaS applications.
Cloud Data Discovery	Performs periodic or ad-hoc deep assessments of data in cloud apps using DLP templates to identify security blind spots, detect open shares and address many global regulations — PCI, HIPAA, GDPR, GLBA, etc.

Product Options

Secure Edge can be purchased as a subscription license based on the number of users. Licensing for 1-and 3-year terms are available for both standard and advanced tiers.

Feature	Standard	Advanced
TLS/SSL inspection	Yes	Yes
Secure Web Gateway	Yes	Yes
URL filtering	Yes	Yes
Content filtering	Yes	Yes
Application visibility	Yes	Yes
User awareness and segmentation	Yes	Yes
Standard threat prevention (threat intelligence feeds, DNS filtering, anti-malware, compromised host isolation)	Yes	Yes
Advanced Threat Prevention (DNS security, zero-day malware prevention, Encrypted Traffic Insights, adaptive threat profiling)	No	Yes
Intrusion detection and prevention services (IDS/IPS)	No	Yes
Out-of-band CASB-DLP-SSPM	Add-On	Add-On

Add-Ons to WAN Assurance

Customers can add out-of-band CASB-DLP to their active WAN Assurance (SD-WAN) or Secure Edge licenses.

Out-of-band CASB-DLP*	Standard	Advanced
CASB	Yes	Yes
DLP	Yes	Yes
SaaS Security Posture Management	No	Yes
Additional Cloud Data Discovery (per TB)	Add-On	Add-On

*Out-of-band CASB-DLP licenses must be tied to an active base license for Juniper Secure Edge or Juniper WAN Assurance/SD-WAN.

Specifications

	Standard	Advanced
Traffic forwarding	Protected access credential (PAC), GRE, IPsec	PAC, GRE, IPsec
Authentication	Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Juniper Identity Management Service (JIMS)	SAML, LDAP, JIMS

Juniper Security Director Cloud

Security Director Cloud is Juniper's cloud-based centralized management platform for all security policies, regardless of form factor. Security Director Cloud enables organizations to manage security anywhere and everywhere, on-premises, in the cloud, and from the cloud, with unified policy management that follows users, devices, and applications wherever they go. Policies can be created once and applied anywhere.

Security Director Cloud provides extensive security policy management and control through a centralized interface. It enforces policies across physical, virtual, and containerized firewalls on-premises and across multiple clouds simultaneously, as well as for Secure Edge FWaaS, SWG, CASB, DLP, and advanced threat policies. Administrators can quickly manage all phases of the security policy life cycle, including zero-touch provisioning, configuration, rule placement, and effectiveness, while gaining insight into sources of risk across the network.

Organizations can use Security Director Cloud and on-premises instances of Security Director simultaneously to transition to a SASE architecture securely.

Ordering Information

To order Juniper Secure Edge and access software licensing information, please visit the How to Buy page at https://www.juniper.net/us/en/how-to-buy/form.html.

Files uploaded to the cloud for processing are destroyed afterward to ensure privacy. The Juniper Networks privacy policy can be found on the product Web portal at https://www.juniper.net/us/en/privacy-policy.html.

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit https://www.juniper.net/us/en/products.html.

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security, and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability, and equality.

Corporate and Sales Headquarters

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089 USA

Phone: 888.JUNIPER (888.586.4737)

or +1.408.745.2000

www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240 1119 PZ Schiphol-Rijk

Amsterdam, The Netherlands

Phone: +31.207.125.700

Juniper Networks | Driven by Experience™