Security Service Edge (SSE)

Request for Proposal Evaluation Questions

**How to use this document?**

This template is meant to serve as a comprehensive Request for Proposal (RFP) for Security Service Edge (SSE) solutions covering the most critical functions that SSE vendors should provide. Before sending this RFP to vendors, it is recommended to consider your own requirements and brand the document in accordance with your branding guidelines.

Table of Contents

[Schedule of Events 4](#_Toc143177620)

[**Section 1 | Company, Solution Management, Architecture, Analyst Evaluation, and Portfolio Vision Requirements** 6](#_Toc143177621)

[**Section 2 | Secure Web Access** 8](#_Toc143177622)

[**Section 3 | Data Protection and CASB** 17](#_Toc143177623)

[**Section 4 | Private Access / ZTNA** 24](#_Toc143177624)

[**Section 5 | CSPM & SSPM** 28](#_Toc143177625)

[**Section 6 | SSE Platform and Cloud Governance** 30](#_Toc143177626)

[**Section 7 | Services and Support** 34](#_Toc143177627)

[**Pricing & Licensing** 36](#_Toc143177628)

[**Terms & Conditions** 36](#_Toc143177629)

# Schedule of Events

|  |  |
| --- | --- |
| **Task** | **Date** |
| RFP Distribution | XX/XX/XX |
| Deadline for Vendor Questions | XX/XX/XX |
| Answers to Vendor Questions | XX/XX/XX |
| Deadline for RFP Submission | XX/XX/XX |
| Vendor Notification of short-listed vendors | XX/XX/XX |
| Vendor Presentations | XX/XX/XX |
| Vendor Selection | XX/XX/XX |

**What is Security Service Edge**

Security service edge (SSE) secures access to the web, cloud services, and private applications. Capabilities include access control, threat protection, data security, security monitoring, and acceptable use control enforced by network-based and API-based integration. SSE is primarily delivered as a cloud-based service and may include on-premises or agent-based components.

**Section 1 | Company, Solution Management, Architecture, Analyst Evaluation, and Portfolio Vision Requirements**

Components: Company Information, Gartner & 3rd Party Reviews

|  |  |
| --- | --- |
| **Requirement** | **Response** |
| Provide the name and version of your SSE solution? Include all components and products. |  |
| Describe the vision and direction of your SSE solution? |  |
| Briefly describe competitive differentiators compared to other SSE vendors? |  |
| What are the Key Portfolio / Growth Products for your company? |  |
| How is your solution rated in the 2023 Gartner Magic Quadrant for Security Service Edge? |  |
| How is your SSE solution rated in other analyst evaluations? |  |
| How many engineers are dedicated to the SSE solution? |  |
| Provide an architectural diagram(s) for your SSE solution? |  |
| Describe your high-availability SSE architecture? |  |
| Does your SSE solution support single sign-on? |  |
| What are the SLA(s) associated with your solution? |  |
| Who are your key integration partners? What functions do they serve? |  |
| Describe your channel engagement model? |  |
| Is your SSE solution managed through one console? |  |
| In the past 3 years, how has your company made it easier to use your SSE solution? What are key enhancements in this area? |  |
| How long has your SSE solution been available in the marketplace? |  |

**Section 2 | Secure Web Access**

Components: Web Protection, Threat Protection, Anti-malware, Shadow IT, Tenant Restrictions, Routing, FWaaS, Web Access performance

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Response** | |
| Describe at a high-level how your solution supports secure web and cloud usage |  | |
| Describe any hybrid deployment options |  | |
| Describe how the solution can allow for blocking of malicious sites by URL? |  | |
| How does your SSE solution protect roaming users from zero-day malware? |  | |
| How do you protect roaming users from browser exploits such as HTML smuggling? |  | |
| Apply SSL inspection for both on-premise and roaming users? |  | |
| Describe how your solution deals with untrusted certificates, such as allowing or blocking such sites. |  | |
| What modes do you support to steer traffic to your proxy? |  | |
| Describe the ability of your solution to access databases of known-good and known malicious URLs. Also, describe what options you offer for actions such as SSL Intercept, block, trace of hostname/IP address, etc., based on the value of the risk score. |  | |
| How many URL categories are provided/supported in your SSE solution? How many categories can a URL be categorized into? Describe how many policy decisions are made for a URL that fits both allow and deny actions based on different categories? |  | |
| Do customers have the ability to apply their own classification(s) to specific websites? |  | |
| Does your SWG have a programmable language or API that can be used for advanced policy creation beyond what is available in the UI? |  | |
| SWG should support traffic decryption. With over 80% of global internet traffic encrypted using SSL/Transport Layer Security (TLS), including a great deal of traffic that is largely undesirable. |  | |
| Are external URL filtering lists supported in your product? |  | |
| Describe the ability of your solution to set policies per (1) pre-defined and custom categories such as File Sharing or Gambling and (2) or by blacklisting or whitelisting individual URLs. Specify whether you maintain specific categories for security & malicious sites that would include: Known botnets, Known command and control servers, Compromised/malicious sites, Crypto mining, Hacking sites, Malware call-Home, Malware distribution point, Phishing/Fraud, Ad Fraud, Spam sites, Spyware & questionable software, Peer to peer, Dynamic DNS, DNS tunneling VPN |  | |
| Describe what reporting functions your solution provides to report on traffic distribution and bandwidth statistics for traffic running through the SWG, including specific information on user or group usage patterns. |  | |
| What protocols are supported and what are limitations/constraints with the level of support (ex’s. TLS1.3, HTTP/3, DoH, IPv6)? |  | |
| Is the traffic between the client and the proxy encrypted? |  | |
| Does the solution utilize signature-based malware detection? |  | |
| List the sandbox vendors that you integrate with? |  | |
| Do you own the SSL technology, or is it licensed from an OEM provider? |  | |
| At a high-level, outline how your solution can monitor and/or control access and usage to shadow cloud services. |  | |
| Describe how your service identifies and controls rogue or shadow IT cloud usage without requiring a “forklift” of existing proxy/firewall solutions. |  |
| Does your cloud solution have a registry of cloud services along with their risk assessment? How many cloud services are tracked in the 'registry/knowledge base'? |  |
| Provide details on what metadata is made available by your service on any cloud service that would be accessed by all our users. For example: (1) Functional categories (e.g., social media, file sharing, content sharing) (2) Location of cloud service provider's datacenter (3) Legal jurisdiction of the cloud service (4) Account termination policy of the cloud service (5) Compliance certifications (6) Known last compromises / data breaches of each cloud services (7) Known vulnerabilities of each cloud service (8) Encryption policies for data stored in the cloud service (9) Cryptographic protocols used to transmit data for the cloud service (10) Risk score calculated based on the risk attributes of the cloud service |  |
| What compliance certifications are being tracked for cloud services within the registry? Can it assess a cloud service against GDPR, PCI, ISO, CSA, HIPAA, and other industry regulations? |  |
| Describe your threat intelligence capabilities including: (1) Overall built-in functionality (2) Whether you use and/or collaborate with third-party/partner feeds (3) Ability to add custom feeds. |  |
| In the event of a security breach at a cloud service provider, does your solution provide a report with breach details and information on employees’ usage of the cloud service? |  |
| Can the customer see the scores for individual attributes (encryption, certification, breaches etc.) that go into calculating the risk score for a cloud service? |  |
| How is the cloud registry kept up to date for new cloud services? |  |
| Does your solution require an agent for DLP functionality? If an agent is offered/optional, what features are not available without an agent installed? |  |
| Can your SSE solution take input on false positives or negatives and use this information to tune the threat protection engine? |  |
| Can the solution create a watch list to monitor selected users who are showing suspicious behaviors? |  |
| Can you customize block pages for the enterprise? What branding options are possible? |  |
| Are usage logs sent off-premises for analysis? If so, how do you protect sensitive data (usernames and IP addresses etc.) within the logs? |  |
| Is Remote browser isolation (RBI) part of your SSE solution? Do you OEM your RBI solution? |  | |
| Can your RBI solution enable isolation for all traffic for a particular user or group of users? |  |
| Do you offer various versions or licenses of Remote Browser isolation? If so, how do they differ? |  |
| If your browser isolation capability native to your secure web gateway or does it use a separate console or next-hop proxy? |  |
| Can you enforce policy for isolated traffic? |  |
| Can your RBI solution perform threat scanning on traffic within the RBI session? |  |
| Can your RBI solution be configured to prevent credentials from being phished and posted in web forms? |  |
| How long does it take on average to scan (not download) a 20 MB pptx file for zero-days threats? |  |
| Ability to print pages from the Remote Browser Isolation session? |  |
| Ability for users to view document files in browser. A user can view a document file such as an excel, word or PDF file as a safe rendering in the browser, rather than downloaded to the local host. |  |
| Can the solution automatically assign cloud services to service groups based on individual attributes? |  |
| Does your SSE solution enforce policies while endpoints are offline? |  |
| Tenant Restrictions - Support both personal and corporate credentials with appropriate policies. Must be able to configure and apply policies appropriately depending on whether a given user is using corporate or personal credentials on a managed device. |  | |
| Does your SSE solution offer FWaaS |  | |

**Section 3 | Data Protection and CASB**

Components: CASB, DLP Endpoint, Holistic Data Protection

|  |  |
| --- | --- |
| **Requirement** | **Response** |
| DLP supports fingerprinting with similarity matching (Exact and partial) |  |
| What types of files can your product identify and perform DLP functions on? |  |
| Provide policy simulation. Prior to implementing a policy should provide a mechanism to "test" what the result of implementing the policy would do in the environment. |  |
| Does your solution provide cloud email DLP capabilities? If yes, which cloud email services do you support (Exchange Online, Gmail, etc.). |  |
| Can the solution scan content already available in the cloud service (data at rest) based on selected DLP policies to detect violations? |  |
| Describe your ability to scan existing Data at Rest for DLP policy compliance |  |
| Describe your ability to scan new data being added (or changed) in the cloud to ensure that it complies with DLP policy. |  |
| Does your solution integrate with common IAM services? Must integrate with existing corporate security infrastructure that supports user identity - whether internally or cloud based. This includes Single Sign-On (SSO) and federated identity management for user provisioning. |  |
| Does your product support country specific access control policies? It must be configurable for country specific access control requirements, such as allowing access to Salesforce.com from the US, Canada and the EU, but blocking access from other countries |  |
| Can the solution support inline DLP for Exchange Online? Does this require agents to be installed at endpoints? |  |
| Provide encryption or tokenize data in-motion and at-rest |  |
| Which ciphers does your company use for order and function preserving encryption when encrypting selected fields within cloud providers such as Salesforce and ServiceNow? |  |
| Can the solution encrypt selected fields within cloud providers such as Salesforce and ServiceNow? |  |
| Collaboration controls – can your SSE solution detect data being exfiltrated directly from sanctioned cloud services? If yes, please describe including automated countermeasure that can be taken against data exfiltration threats. |  |
| Collaboration Control for Microsoft Teams |  |
| Can your solution remediate violations in sharing policies by the following? |  |
| Can the SSE solution enforce cloud DLP policies through API integrations? |  |
| Can your solution integrate with data classification and tagging solutions such as Titus, Boldon James, and other natively available tagging features in cloud services such as Box and Office365? |  |
| Does your solution include smart data identifiers for SSN and credit cards that does not use simple regex? E.g. distinguishing SSN’s in the pre-2010 and post-2010 standard; performing LUHN check to detect credit card numbers. |  |
| My organization is interested in leveraging third party applications that are available in the respective cloud service marketplaces (e.g. Microsoft AppSource Marketplace). Does your solution provide a way to allow or block our employees from allowing these applications from accessing our corporate information stored within our cloud tenant? |  |
| Can your solution detect compromised credentials based on information such as multiple login attempts, impossible cross-region access, and untrusted location access? |  |
| Does your solution offer pre-built templates to identify selected personally identifiable information (driver’s license, credit cards, SSN) and personal health information? How many templates do you provide out-of-the-box? |  |
| Does your solution provide pre-built templates for IT teams to enforce policies required for compliance with GDPR, PCI DSS, HIPAA, HITECH, GLBA, SOX, CIPA, FISMA, and FERPA? |  |
| Does your solution provide policy simulation capabilities? I.e. Prior to implementing a policy, a mechanism to "test" the result of implementing the policy would do in the environment should be provided. |  |
| Can your solution detect DLP violations or data leakage in image file formats using technologies like OCR? |  |
| What methods does your solution support to detect managed vs unmanaged devices? |  |
| Can your solution enforce granular device-based controls such as restricting read-only access to unmanaged or personal devices? |  |
| How can the solution scan data in private cloud environments that are not accessible by the SaaS Service? |  |
| My enterprise uses or may potentially use Microsoft Dynamics 365, does your solution provide security controls for sensitive data that may be stored within that system? |  |
| Can you set policies based on Active Directory attributes? For example, enforce policies on a specific team or department within the company. |  |
| Can your solution provide a reverse proxy deployment to secure custom applications? Describe how. |  |
| Can your solution enforce access controls on custom apps based on contextual parameters such as device, location, user, activity? |  |
| Can your solution detect data exfiltration attempts? If yes, please describe how? |  |
| Describe any unique features that your solution provides to implement CASB policies against Office 365 applications to provide enhanced performance as well as smooth and complete integration. |  |
| Can the solution discover all sites within SharePoint based on author and other metadata parameters? |  |
| Describe at a high-level how you control data on endpoints? |  |
| Can DLP policies be applied from the SSE console for printing? |  |
| Can DLP policies and device control be applied for removable media? Can you block enterprise usage of removable storage devices completely? |  |
| Provide integration with on-premise DLP solutions? |  |

**Section 4 | Private Access / ZTNA**

Components: ZTNA, Private Application Protection

|  |  |
| --- | --- |
| **Requirement** | **Response** |
| Describe at a high-level how your ZTNA solution enables enterprises to connect and secure remote workers? |  |
| Is your ZTNA solution natively integrated into the proposed SSE solution? Who are your ZTNA partners? |  |
| Describe how your SSE solution supports key ZTNA principles? |  |
| How does your SSE and ZTNA solution replace network-level VPN access with application-level, context-aware, identity-based access ZTNA (Zero Trust Network Access)> |  |
| Describe at a high-level how your SSE solution supports adaptive access control in an enterprise? |  |
| Explain how your ZTNA solution can enrich activity reporting? |  |
| Provide bullet points that demonstrate how your ZTNA solution improves the experience for an organization employee? |  |
| In terms of enterprise architecture, can your ZTNA solution potentially reduce IT and networking costs? |  |
| How is your ZTNA solution deployed? |  |
| Does your ZTNA offering require a separate console and/or agent to be used? |  |
| What differentiates your ZTNA solution from the competition? |  |
| How can DLP policies be applied from the SSE console for ZTNA traffic? |  |
| How can threat protection be applied to ZNTA traffic? |  |
| Describe the level of granularity that can be achieved in your ZTNA policies. |  |
| Does your ZTNA solution provide a wrapper around private web applications using technologies like RBI or WAF to reduce the attack surface of vulnerable services? |  |
| How does your solution assess device posture? Are there options for integrations with 3rd party XDR vendors (e.g., Crowdstrike)? |  |
| The solution should optimize routing, peering and latency. Please explain how this is achieved. |  |
| What is the preferred approach for supporting off-network systems including Windows, Mac, Linux, iOS, and Android? |  |
| What capabilities does your SSE solution have around geolocation of sources and destinations? Can you define rules/policies around geolocation information? |  |
| Please provide details of the SAAS services or Cloud Service Providers which you have peering arrangements with for optimization of traffic |  |
| The SSE solution must integrate with SD-WAN technologies. Please detail which vendors are available for integrations. |  |
| What authentication methods are supported by the solution. |  |
| How does the solution encrypt unencrypted protocols on the wire? |  |

**Section 5 | CSPM & SSPM**

|  |  |
| --- | --- |
| **Requirement** | **Response** |
| Cloud Security Posture Management (CSPM) for IaaS? |  |
| Can your solution also provide Cloud Native Application Protection for workloads in AWS, GCP, and AWS? |  |
| Can your CSPM capability be used to assess our 3rd parties cloud infrastructure to ensure it is compliant to our standards? |  |
| Does your CSPM have the ability to score or represent incidents based on CSP accounts or CSP tag information (e.g. AWS tags)? |  |
| Which IaaS template format do you support for CSPM scanning? (Terraform, CloudFormation, ResourceManager) |  |
| Describe the ability to monitor, secure, and audit IaaS / PaaS environments? |  |
| How does your solution perform functions of SaaS Security Posture Management (SSPM) |  |

**Section 6 | SSE Platform and Cloud Governance**

Components: Integration with SOC tools, Single Console Management

|  |  |
| --- | --- |
| **Requirement** | **Response** |
| Integration with SIEMs |  |
| Does your solution offer a way for SOC teams or administrators to effectively understand and articulate the severity of an event that your product identifies within our cloud service providers? I.e. Mapping to MITRE ATT&CK |  |
| Does your solution provide a way to ensure my enterprise has leveraged all the controls offered by your solution to ensure our organization has extracted all the value your solution provides? |  |
| Identify location data for users of cloud services. Must be able to detect and display locational information, geographic and IP, from which access is taking place. |  |
| Provide unnoticeable performance impact to applications. When users are accessing applications through the solution, in-line, the users should not notice any performance impact. |  |
| Does your company have a program to inspect and publicly certify the enterprise-readiness of cloud services? If so, please provide details. |  |
| Does the product provide different levels of access (Role Based Access Control) to the data and product capabilities based on the role assigned to the user by the admin? |  |
| Can the solution detect anomalies within cloud services and raise alerts based on the following? |  |
| If your Secure Web Gateway does not include comprehensive CASB functionality and therefore requires procuring a CASB solution from another vendor, indicate which third-party CASB product you are proposing and provide details of how this integration ensures a unified admin user experience with your SWG. |  |
| Does the management console of your SSE solution provide configuration/policy versioning? Is there an option to roll back to a specific previous version? Can you selectively rollback selected changes? |  |
| Can your SSE solution export reports? How can your SSE solution ad hoc or on-demand send reports to teams via email? |  |
| How many cloud services do you secure via API deployment mode? |  |
| The CASB service supports custom application onboarding with an SLA |  |
| Can the solution integrate with Microsoft Graph APIs and Activity APIs to monitor activity and enforce policies? |  |
| Can your solution provide visibility into all users and departments using a particular cloud service by leveraging the Active Directory integration? |  |
| Describe how your APIs are secured |  |
| Is your solution SOC 2 Type II certified? |  |
| Do you own and manage your own data centers, or do you partner with leading cloud providers (i.e. AWS, Azure)? |  |

**Section 7 | Services and Support**

|  |  |
| --- | --- |
| **Requirement** | **Response** |
| Are professional services available? |  |
| What is your implementation methodology? |  |
| Is customer support included in the pricing? Are there varying tiers of customer support that we can purchase? |  |
| Provide Customer Support days and hours of operation. Is support 24x7x365 for all customers? |  |
| Can support tickets be logged via web and phone? |  |
| Describe the methods of communication (e.g., web portal, email notifications, etc.) that you provide for real-time status of your service, product updates, scheduled maintenance, security advisories, etc. |  |
| Do you have a community support portal where customers and/or product teams can collaborate and freely discuss? |  |

# **Pricing & Licensing**

*Describe the pricing and licensing options here*

# **Terms & Conditions**

*Please provide the links to any terms and conditions documents, as well as service descriptions,*

*support, and education.*