EIS and the Implementation of Security as a Service (SECaaS)

Version 2.0

February 2022
# Table of Contents

1. Advantages of Cloud-Delivered Security as a Service (SECaaS) ........................................... 3
2. Business Value of EIS SECaaS Services .................................................................................. 3
   2.1 Characteristics: .................................................................................................................. 3
   2.2 Deployment Models: .......................................................................................................... 3
   2.3 Industry Expertise and Experience .................................................................................... 4
   2.4 Fast Consistent Security Provisioning and Updates .......................................................... 4
   2.5 Cost Savings and Cost Avoidance ..................................................................................... 4
3. Recommendations for SESaaS Implementation through EIS .................................................. 4
4. EIS Services Enabling SECaaS ............................................................................................... 5
5. SECaaS Implementation Scenarios .......................................................................................... 6
   5.1 Example 1 Endpoint Detection and Response (EDR) ......................................................... 6
   5.2 Example 2: Remote Access through Cloud Access Security Broker (CASB) ..................... 7
   5.3 Example 3: DDoS Protection/Mitigation ............................................................................. 7
6. Additional Information .............................................................................................................. 9
1 Advantages of Cloud-Delivered Security as a Service (SECaaS)

Agencies should consider moving to cloud-delivered consumption-based services, including Security as a Service (SECaaS) to:

- Address an agency’s growing needs for network security and broader cybersecurity
- Protecting agency assets and network from latest threats
- Improved efficiencies
- Cost savings and cost avoidance

Enterprise Infrastructure Solutions (EIS) offers the flexibility of using a Service Catalog under Managed Security Service (MSS) and/or Software-as-a-Service (SaaS) to meet an agency’s SECaaS requirements. This allows agencies to obtain scalable, on-demand cybersecurity services which may be customized to integrate with other existing agency solutions or leveraged to replace current capabilities. GSA’s EIS industry partners can help agencies with the planning and implementation of their requested SECaaS capabilities as part of the task order.

2 Business Value of EIS SECaaS Services

Moving to a SECaaS arrangement may benefit an agency by providing them an established strategy including industry expertise and experience, fast consistent security provisioning and updates, cost savings and cost avoidance. This allows agencies to focus on their core mission.

SECaaS allows agencies to outsource security services in a similar arrangement to other “as-a-Service” models with the following characteristics:

2.1 Characteristics:

- On Demand Self-Service – ability to select and rapidly turn up and turn down services as needed and with a zero-touch deployment
- Fast automated updating of the security stack to achieve maximum protection
- Broad Network Access – universal access to web-based/thin or thick client platforms on various devices such as mobile phones, laptops, and tablets
- Dynamic operations and management dashboards with true single-pane-of-glass monitoring
- Rapid Elasticity – ability to immediately scale up or down based on user/network needs and changing security postures while managing risks
- Consumption pricing model – ability to pay only for what is used
- Ease of integration with SaaS applications through multi-cloud architectures
- Natural fit with modernized solutions such as managed SD-WAN, the various TIC 3.0 use cases, and components of a Zero Trust Architecture
- Simplifies site access configurations by removing or reducing security hardware or software at each site

2.2 Deployment Models:
The SECaaS delivery model is similar to other SaaS models, meaning agencies leverage shared multi-tenant instances running within a public cloud infrastructure. Leveraging the SECaaS model would require no additional time or cost for agencies to own and manage their own instances or have it managed by a managed service provider.
As with other SaaS the access to the service can be either directly over the public Internet, using secure tunnels leveraging TLS or IPsec over the public Internet, or through a layer-2 or layer-3 dedicated private virtual network. Increased availability is an inherent feature of SECaaS with multiple instances running on geographically diverse data centers. For smaller sites, low-cost fixed wireless or broadband Internet connections are sufficient to achieve high availability access to SECaaS capabilities.

2.3 Industry Expertise and Experience
Agencies would benefit from the expertise and experience of an EIS industry partner that offers government clients a SECaaS solution in addition to, or in place of other EIS Managed Services. Turning over some or all of an agency’s cybersecurity operations to an industry partner who possesses a broader view of cybersecurity operations across the public and private sectors would result in agencies being relieved of the burden of retaining in house or other contracted expertise to stay current with the latest security tools, services and trends. Through SECaaS arrangements, agencies gain access to industry leading technology, tools, and expertise for a reoccurring operational expense.

2.4 Fast Consistent Security Provisioning and Updates
Agencies would benefit from SECaaS characteristics such as rapid scalability for faster provisioning and deploying security configurations or updated threat definitions without being dependent on manual actions. An additional benefit to agencies would be not having to manage disparate systems and providers, while promoting deployment standardization and reducing the administrative burden.

2.5 Cost Savings and Cost Avoidance
Agencies avoid large capital and operational costs associated with purchasing, deploying and maintaining their own security equipment and software services. This equipment and software is highly specialized and expensive to purchase, operate, and keep up to date. In addition, agencies can avoid the challenges and costs of maintaining and retaining highly specialized cybersecurity personnel.

3 Recommendations for SECaaS Implementation through EIS
Agencies should carefully consider many factors when they establish their requirements and evaluate vendor proposed solutions.

Agencies have a number of considerations when selecting a vendor. Considerations such as the vendor’s capabilities to support the requirements, the vendor must have the staffing and capabilities to be able to respond when needed, the vendor must have plans in place to recover from a disturbance or disruption, the agency may require the vendor to have a partnership or agreement with a preferred cloud infrastructure or security stack supplier, and it is critical for the vendor to have the right security expertise for the agency’s environment.

Agency requirements should specify the details of the SECaaS deployment. Agencies need to carefully define service features and capabilities they require. Agencies also need to carefully define the performance metrics and Service level Agreements (SLAs) which can cover the contractor’s time to respond to agency requests, service availability, time to restore, incident
detection and response timeframes, deployment timelines, and other agency specific requirements.

SECaaS can be combined with EIS MSS and/or SaaS for customized solutions to an agency’s specific needs and environment. Services that can be provided as SECaaS are:

- Endpoint Detection and Response (EDR)
- Extended Detection and Response (XDR)
- Security Information and Event Management (SIEM)
- Security Orchestration & Automated Response (SOAR)
- Cloud Access Security Broker (CASB)
- Secure Access Service Edge (SASE)
- Business Continuity and Disaster Recovery
- Continuous Monitoring
- Email Filtering and Security
- Identity and Access Management
- Penetration testing
- Vulnerability Scanning
- Web Security

Similar to other “as-a-Service” items, agencies may procure SECaaS through a subscription model (all you can consume) or a payment for services utilized model (pay as you go). Agencies should have a clear definition on what features are included and what features are at an additional cost.

Agencies considering requirements for an Agency-Specific Network Operations Center (NOC) and Security Operations Center (SOC) should leverage the EIS Managed Network Service (MNS) where NOC and SOC features are currently available. As these services are offered via Individual Case Basis (ICB) CLINs, agencies are encouraged to include specific performance expectations and requirements within their solicitations to ensure they receive the level and type of services expected.

4 EIS Services Enabling SECaaS

In order to deploy SECaaS an agency would need to create requirements such as the service’s technical capabilities, features, interfaces, and performance metrics (SLAs). The EIS Contract offers the services and flexibility to construct comprehensive SECaaS solutions.

The primary EIS service to leverage for SECaaS is the Managed Security Service (MSS) which uses a Service Catalog without prescribed CLINs. The Service Catalog allows the EIS Provider the flexibility to offer an array of potential services and service variations, as well as special tailored solutions with the “as-a-Service” pricing models.

SECaaS also leverages a Service Catalog instead of pre-defined CLINS.

Managed Network Service (MNS) has CLINs for Design and Engineering Support and for an Agency-Specific Security Operations Center (SOC) service leveraging Individual Case Basis (ICB) CLINs which may be customized for an agency specific solution. MNS also has Task
Order Unique CLINs (TUCs) to allow for customized agency solutions and allow the “as-a-Service” pricing models.

5 SECaaS Implementation Scenarios

5.1 Example 1 Endpoint Detection and Response (EDR)

For this example, an agency wants to procure a EDR solution that provides enterprise-wide prevention and detection as a service. The agency also wants the vendor to do design and engineering work as part of the solution for the agency’s environment.

The agency’s SECaaS EDR requirements can include capabilities such as:

- Monitoring of endpoints both the online and offline
- Increased visibility and transparency of user data
- Real-time response to threats
- Detecting stored endpoint events
- Detecting malware injections
- Creating whitelists and blacklists for applications and network traffic
- Integration with other technologies

![Figure 1- EDR](image)

<table>
<thead>
<tr>
<th>MN00001</th>
<th>Managed Network Design and Engineering</th>
<th>Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS90001</td>
<td>NRC</td>
<td>Managed Security Service Catalog Item</td>
</tr>
<tr>
<td>MS90002</td>
<td>MRC</td>
<td>Managed Security Service Catalog Item</td>
</tr>
<tr>
<td>MS90003</td>
<td>Usage</td>
<td>Managed Security Service Catalog Item</td>
</tr>
</tbody>
</table>
The EIS vendor can perform the design and engineering work under MNS CLINs and implement a solution for the EDR requirements using service catalog CLINs under MSS.

5.2 Example 2: Remote Access through Cloud Access Security Broker (CASB)

For this example, an agency wants to procure a remote access solution via a CASB as a service to improve its security posture for IPS and/or Internet Broadband services.

The agency’s remote access solution via CASB requirements can include capabilities such as:

- Remote access from user’s multiple devices
- Secure and reliable remote connectivity for internal and external applications
- Applications are not exposed to the internet
- Secure connectivity between clouds
- Enforcement of business and security policies

The EIS vendor can implement a solution for these requirements and use service catalog CLINs under SaaS.

### Figure 2 Remote Access - CASB

<table>
<thead>
<tr>
<th>SaaS Cloud Service Catalog Item</th>
<th>Remote access solution via a CASB</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS90001 NRC</td>
<td>SaaS Cloud Service Catalog Item</td>
</tr>
<tr>
<td>SS90002 MRC</td>
<td>SaaS Cloud Service Catalog Item</td>
</tr>
<tr>
<td>SS90003 Usage</td>
<td>SaaS Cloud Service Catalog Item</td>
</tr>
</tbody>
</table>

5.3 Example 3: DDoS Protection/Mitigation

For this example, an agency wants to procure a DDoS Protection/Mitigation solution as a service to improve its security posture for Internet Protocol Service (IPS) and/or the Broadband Internet Service (BIS).

The agency’s SECaaS DDoS Protection/Mitigation requirements include:
- Implement volume-based DDoS mitigation with enough bandwidth to exceed the volume of an attack
- Implement volume and application level protection
- In a multi-home environment, ensure all traffic passes through a DDoS mitigation grid.
- Accurate filtering via thorough profiling of legitimate traffic
- Have a response procedure in case legitimate traffic gets blocked
- Implement active notification
- Access to relevant monitoring, alerting, and network performance reports and metrics.
- IPv6 compliance

The EIS vendor can implement a solution for these requirements and use service catalog CLINs under SaaS.

![DDoS Protection/Mitigation](image)

<table>
<thead>
<tr>
<th>SS90001</th>
<th>NRC</th>
<th>SaaS Cloud Service Catalog Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS90002</td>
<td>MRC</td>
<td>SaaS Cloud Service Catalog Item</td>
</tr>
<tr>
<td>SS90003</td>
<td>Usage</td>
<td>SaaS Cloud Service Catalog Item</td>
</tr>
</tbody>
</table>

DDoS mitigation can be priced using different pricing models including:

- Per Internet circuit and per circuit bandwidth regardless of traffic volume or mitigation number
- Per circuit and per maximum volume of clean traffic required
- Hours of mitigation - regardless of the number of Internet circuits, bandwidth, or the number of mitigations
- Proactive vs. reactive monitoring – under proactive monitoring the provider automatically initiates filtering if they are detecting an attack
- Mitigations per month – for low-attack volume cases
6 Additional Information

For more information please contact your designated GSA representative via [www.gsa.gov/nspsupport](http://www.gsa.gov/nspsupport) or call 1-855-482-4348.

For more information on the EIS services mentioned, please review the EIS Service Guides here: [https://eis-public-pricer.eos.gsa.gov/service-guides/](https://eis-public-pricer.eos.gsa.gov/service-guides/)