U.S. General Services Administration

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

Version 3.0

September 2023

Last Updated: 10/26/2023

Table of Contents

DOCUMENT CHANGE RECORD

Version Number	Date	Description
1.0	6/28/2023	Initial Document
2.0	9/27/2023	Revised Document

1 Executive Summary

Security as a Service (SECaaS) is a cloud based service model that allows an Agency to outsource their cybersecurity needs. SECaaS is a flexible, scalable, subscription based solution that allows an Agency to avoid the overhead costs for security personnel and infrastructure while maintaining access to the latest in cyber security technologies. SECaaS allows an Agency to maintain protection from the latest threats while reducing costs and improving efficiencies.

Federal Agencies are currently modernizing information technology (IT) services, infrastructure, and improving the security and efficiency of their networks through the adoption of cloud based services such as SECaaS. Outsourcing its security needs allows an Agency to focus on its mission while addressing the growing need for network security and protecting agency network assets.

2 Introduction

This paper will discuss SECaaS, as a comprehensive security solution that helps Agencies address any security issue without relying on its own dedicated security staff and infrastructure. Federal Agencies are moving toward as a service solutions and new innovative technologies to transform and modernize their IT infrastructure. SECaaS is a cloud-based security delivery model that offers organizations a flexible and scalable way to protect their systems and data without the need for extensive in-house infrastructure and management. It can be a valuable option for Agencies looking to enhance their security posture while reducing operational overhead. SECaaS solutions can be Agency specific and can include services such as: Encryption, Web Security, Email Security, Data Loss Prevention, Identify Management, Access Management, Security Assessments, and Disaster Recovery.

The Cloud Security Alliance (CSA)[1] defines the following categories of SECaaS tools:

- Identity and Access Management
- Data Loss Prevention
- Web Security
- Email Security
- Security Assessments
- Intrusion Management
- Security, Information and Event Management
- Encryption
- Business Continuity Disaster Recovery and Disaster Recovery as a Service
- Network Security

[1] https://cloudsecurityalliance.org/research/topics/security-as-a-service/

SECaaS solutions typically have the following characteristics:

- Self-service on-demand provisioning – users can rapidly turn up and turn down services as needed with a zero-touch deployment
- Fast automated updating of the security stack for achieve maximum protection
- Rapid Elasticity – immediately scale up or down based on user/network needs, changing security postures while managing risks
- Consumption pricing model – “pay by the drink”
- Universal access to various devices such as mobile phones, tablets, laptops, and desktops.
- Single dashboard for operations and management (single-pane-of-glass monitoring) for day to day management
- Ease of integration with other Software as a Service (SaaS) applications
- SECaaS solutions are a natural fit for a comprehensive modernization strategy along with Software Defined Wide Area Network (SD-WAN), Trusted Internet Connection (TIC) 3.0, Zero Trust Architecture, Internet Protocol Version 6 (IPv6) and other modern technologies.

3 Federal Guidance and Efforts Supporting SECaaS

The Federal Government recognizes the potential benefits of SECaaS technology and has taken several steps to promote its adoption and use. By leveraging the capabilities of SECaaS, Federal Agencies can improve security, scalability and increase the cost-effectiveness of their network infrastructure. The Federal Government is supporting the development and deployment of SECaaS through multiple efforts, including:

- GSA’s Technology Modernization Fund (TMF) which was authorized through the Modernizing Government Technology Act (MGT) provides funds to Agencies for implementing new modern IT systems including cloud-based security framework such SECaaS.
- The Cloud Smart Strategy- launched in 2018, aims to modernize the Federal Agencies IT infrastructure and accelerate the adoption of cloud-based technologies, including SD-WAN.
- The Federal Risk and Authorization Management Program (FedRAMP) offers a standardized approach to authorization, security assessment, and continuous monitoring for cloud-based technologies, including SECaaS solutions.
- The National Institute of Standards and Technologies (NIST) Cybersecurity Framework – This framework provides guidance and best practices for improving cybersecurity risk, including the adoption of SECaaS solutions.
- The Federal Information Technology Acquisition Reform Act (FITARA) was passed in 2014 to promote modern secure, cost-effective IT solutions across the Federal Government. Agencies are encouraged to deploy cloud-based solutions, including SECaaS, as part of their IT modernization efforts.

4 The Emerging SECaaS Landscape

SECaaS and general Cybersecurity requirements are changing rapidly due to a number of reasons including global/geopolitical conflicts, social media weaponization, evolving threat paths, new and challenging attacks, and others. [2] Emerging trends in SECaaS include:

- Security Requirements for the distributed workforce - post pandemic many Agencies need to adapt security policies and infrastructure to support the hybrid workforce.[3]
- Operational Technology (OT) and the Internet of Things (IoT) - new technologies including OT and IoT devices have resulted in new security threats. Recent attacks have revealed that many OT/IoT networks are not properly protected.[4]
- Rise in Cloud Adoption- The pandemic rapidly accelerated cloud adoption as Agencies swiftly reacted to a challenging situation. The increase in cloud deployments comes with an increase in cloud security incidents. The 2022 IBM Cost of a Data Breach Report found that 45% of breaches occurred in cloud environments. [5]

5 Advantages of Cloud-Delivered Security as a Service (SECaaS)

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.

Agencies should consider implementing SECaaS as part of their comprehensive modernization and virtualization strategy with integrated with other components such as SD-WAN, ZTA, TIC 3.0, and IPv6. The Agency's security posture and risk tolerance should be factored into the overall SECaaS approach.

6 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] Gartner Top Security and Risk Trends in 2022

[3] https://www.forbes.com/sites/forbestechcouncil/2023/01/09/top-four-cybersecurity-trends-for-2023/?sh=78fdb2532a4c

[4] Microsoft Digital Defense Report 2022.pdf

[5] Cost of a data breach 2023 | IBM

6.1 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.

6.2 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.

6.3 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.

6.4 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.

7 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.

Agencies should consider implementing SECaaS as part of a larger comprehensive network modernization strategy with other components such as Software Defined, TIC 3.0, Cloud, Shared Services, and Zero Trust

Agencies should review CISA's TIC 3.0 Core Guidance Documents including CISA’s Program Guidebook, Reference Architecture and Security Capabilities Catalog along with the updates regarding the Policy Enforcement Points (PEP) Security Capabilities Catalog, Branch Office Use Case, Remote User Use Case.[6] CISA's Core Guidance can provide guidance to an Agency on how to protect their environments and comply with their risk management strategy along with the security considerations for the applicability and rigor of security capabilities all based on agency risk tolerance.

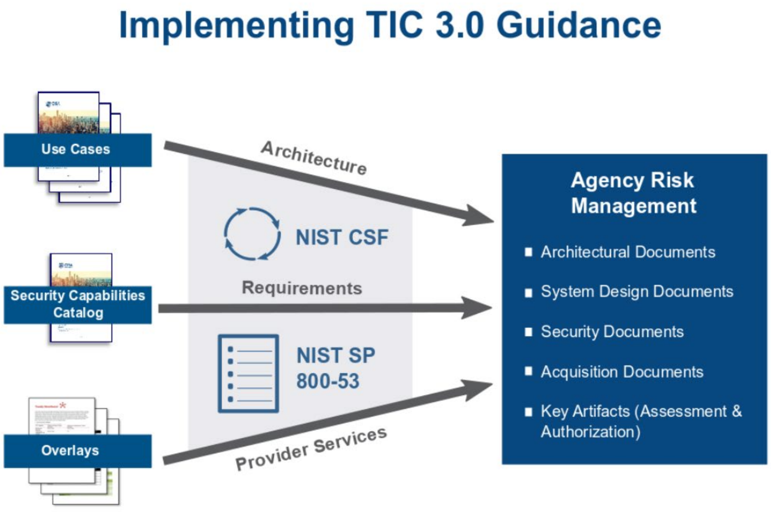


Figure 1 Integrate TIC into an Agency Risk Management Plan

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.[7]

[6] Trusted Internet Connections (TIC) 3.0 Core Guidance Documents | CISA

[7] CISA%20TIC%203.0%20Program%20Guidebook%20v1.1.pdf

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.

8 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.

EIS SaaS 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.

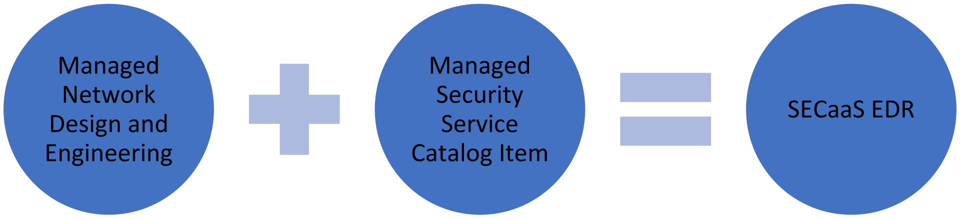
9 SECaaS Implementation Scenarios

9.1 Example 1 Endpoint Detection and Response (EDR)

For this example, an agency wants to procure an 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


Managed Network Design and Engineering
Managed Security Service Catalog Item
SECaaS EDR

MN00001	Managed Network Design and Engineering	Device

MS90001	NRC	Managed Security Service Catalog Item
MS90002	MRC	Managed Security Service Catalog Item
MS90003	Usage	Managed Security Service Catalog Item

Figure 2- EDR

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.

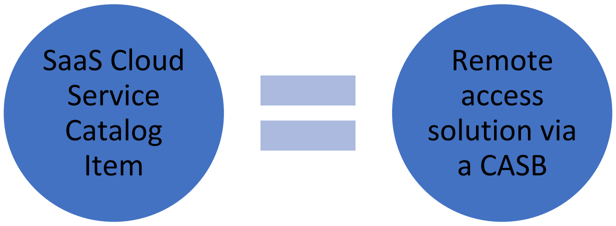
9.2 Example 2: Remote Access through Cloud Access Security Broker (CASB)

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.


SaaS Cloud Service Catalog Item
Remote access solution via a CASB

SS90001	NRC	SaaS Cloud Service Catalog Item
SS90002	MRC	SaaS Cloud Service Catalog Item
SS90003	Usage	SaaS Cloud Service Catalog Item

Figure 3 - Remote Access - CASB

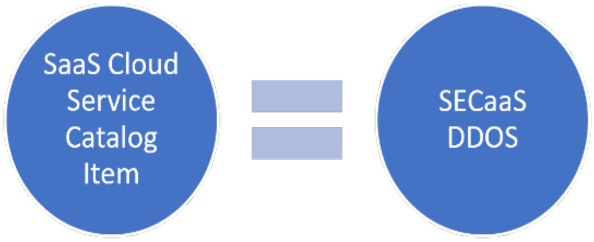
9.3 Example 3: DDoS Protection/Mitigation

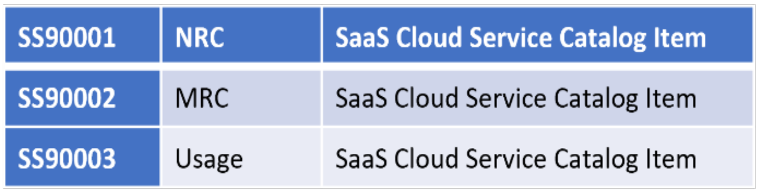
For this example, an agency wants to procure a DDoS Protection/Mitigation solution as a service to improve its security posture for Internet Protocol Service (IPS) and/or the Broadband Internet Service (BIS).

The agency's SECaaS DDoS Protection/Mitigation requirements include:

- Implement volume-based DDoS mitigation with enough bandwidth to exceed the volume 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.





SS90001	NRC	SaaS Cloud Service Catalog Item
SS90002	MRC	SaaS Cloud Service Catalog Item
SS90003	Usage	SaaS Cloud Service Catalog Item

Figure 4 DDoS Protection/Mitigation

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

10 GSA Is Here to Help

For more information on the topics covered in this paper, please reach out to your designated GSA representative - a/k/a EIS Solution Broker - at https://gsa.gov/nspsupport or call 855-482-4348 to get in touch. GSA has multiple offerings for products, services, and solutions to support your planning, implementation, and continued support of the components of your SECaaS. Thank you for reading!

11 Contributors

General Services Administration
JPI