Secure Cloud Business Applications (SCuBA)
Technical Reference Architecture (TRA)

Secure Cloud Business Applications (SCuBA) Technical Reference Architecture (TRA)

Request for Comment Draft
Publication: April 2022

Contents

Figures

Tables

1. Introduction

1.1 Background

The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and reduce cyber risks, including by serving as the operational lead for Federal Civilian Executive Branch (FCEB) cybersecurity by providing cybersecurity tools, incident response services, and assessment capabilities. Recent cyberattacks provide ample evidence that the FCEB information technology (IT) enterprise requires continued focused efforts to protect against sophisticated attacks by nation-state actors.

CISA established the Secure Cloud Business Applications (SCuBA) project per its authorities granted in the American Rescue Plan Act of 2021 and the FY21 National Defense Authorization Act, P.L. 116-283. [1] [2] Under the SCuBA project, CISA will establish and configure environments for Microsoft 365 (M365) and Google Workspace (GWS). CISA will design cybersecurity architectures for M365 and GWS services by leveraging vendor native capacities as well as third-party solutions as necessary. Establishing the visibility of cloud service offerings and standing up test environments to enable selection, configuration, and testing of security capabilities affords CISA the opportunity to: (a) expand its cloud security expertise to benefit both government and critical infrastructure partners; (b) expand utilization of available cloud security related data across existing and planned security programs; (c) improve program requirements and services; (d) share the knowledge gained and lessons learned with FCEB agencies; and (e) help secure cloud business application environments across the federal enterprise.

The SCuBA project will address cybersecurity and visibility gaps in business applications hosted in the cloud and provide guidance to secure FCEB implementations. These gaps impact each agency's ability to manage cyber risk for its IT enterprise and CISA's ability to adequately understand and manage cyber risk for the federal enterprise. The SCuBA project will provide architecture and security configurations that offer fundamental protections for cloud business applications and give FCEB agencies and CISA the visibility necessary to identify and detect adversarial activity in their cloud environments.

1.2 Purpose

The purpose of the SCuBA Technical Reference Architecture (TRA) is to provide context, standard views, and terminology that incorporate and align all SCuBA efforts. The SCuBA TRA is product and vendor agnostic and is consistent with other federal, DHS, and CISA reference architectures (RAs). The SCuBA TRA is based upon the Cloud Security TRA published by CISA, the United States Digital Service, and the Federal Risk and Authorization Management Program (FedRAMP). [3] Development of the SCuBA TRA will require interagency coordination and consultation with the major Cloud Service Providers (CSPs). The SCuBA TRA should be used to inform product-specific RAs, implementation architectures, and configuration guidelines that will be developed by other SCuBA efforts.

A secure cloud-based business application (e.g., M365 or GWS) deployment requires a combination of application configuration, security services (provided natively with the application or by a third party), integration with existing enterprise systems, and robust operational practices. When fully developed, the SCuBA TRA will provide threat-based guidance to create a secure implementation architecture.

CISA will engage with FCEB agencies to facilitate data acquisition of cloud logs and telemetry for analysis and—when needed—facilitate incident response and threat-hunting activities. Simultaneously, CISA will consult with cloud vendors to identify opportunities to develop and improve solutions that provide enhanced security and support for cloud business applications used by FCEB agencies. Cloud vendors occupy a unique vantage point in the SCuBA TRA because they can identify trends and threat activities across sectors and service offerings. They can also respond to threats that may be undetectable to their tenants, and they can update their offerings to mitigate vulnerabilities and adversarial campaigns. CISA will work with agencies to address risks and maximize benefits associated with their use of cloud services.

For SCuBA to be consistent with Office of Management and Budget (OMB) M-21-31, [4] agencies must work with CISA to implement comprehensive logging and information-sharing capabilities. This coordination includes agencies sharing telemetry and logs from their cloud business applications with CISA. Such information is necessary for CISA to have the visibility and capacity to respond to evolving cloud threats and perform effective monitoring, threat hunting, and incident response activities. In turn, CISA will share information that will allow

agencies to collect, process, and analyze telemetry to fulfill their own internal security requirements, enhance their visibility, and meet mission needs.

1.3 Scope

The scope of the SCuBA TRA is cloud business applications, delivered through a Software-as-a-Service (SaaS) model to users, and the security services used to secure and monitor these applications. Figure 1-1 shows that agencies are responsible for securely configuring their cloud business applications and collecting the associated logs and telemetry to meet their security needs.

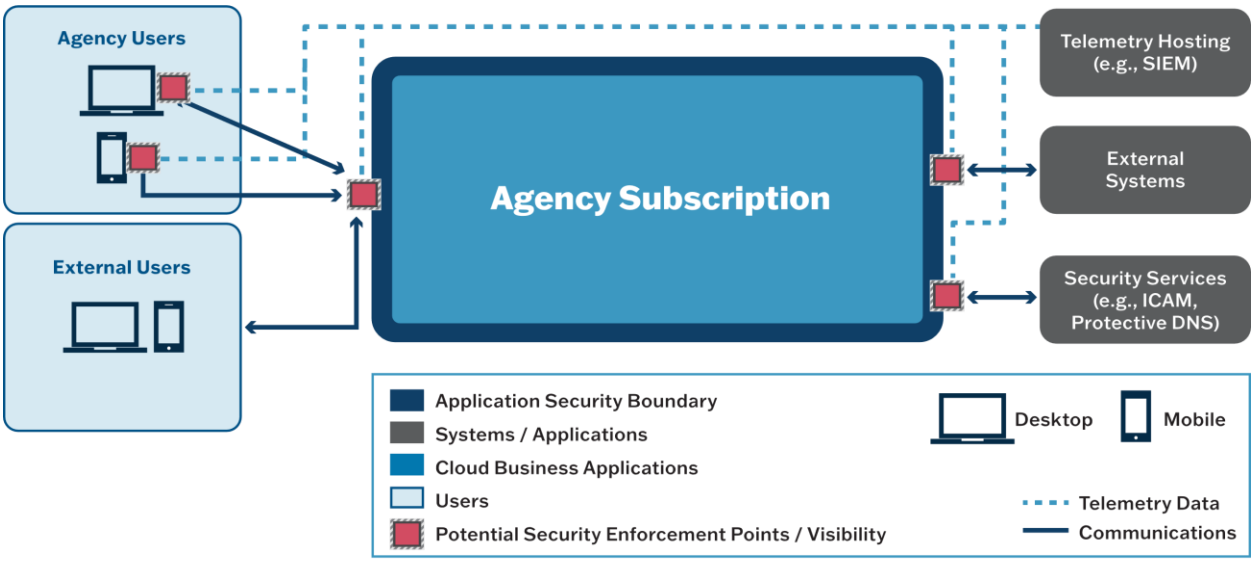

Figure 1-1. SCuBA System View

Agency Users:

- The scope of the SCuBA TRA includes connections from campus and internet sources. Agency strategies for adopting Zero Trust (ZT) will define any changes or merging of campus and internet access.
- Agency user access is through agency endpoints. The management and security of the endpoints are outside the scope of the SCuBA TRA. Additionally, Bring Your Own Device (BYOD) is not in scope of the SCuBA TRA.
- Dedicated telephony devices, such as desktop phones using Voice over Internet Protocol or Time Division Multiplex signaling, are not in scope of the SCuBA TRA.

External Users:

- External users include both trusted business partners and the public, who use the collaboration tools for voice and video as well as document/content sharing.

Agency Subscribed Cloud Business Applications:

- The initial set of cloud business capabilities are scoped to M365 and GWS. These capabilities—which currently include Productivity, Messaging, Content Management, Collaboration, and Voice—may expand in the future. See Section 3 for more details on the scope of the cloud business capabilities.

2. Development

Initially, the SCuBA TRA comprises input from across CISA (e.g., National Cybersecurity Protection System [NCPS], Vulnerability Management, and Continuous Diagnostics and Mitigation [CDM]), analysis and identification of cloud security guidance, applicable supporting documents (Section 4), identification of cybersecurity threats (Section 5), and necessary security capabilities to harden cloud business applications (Section 6).

SCuBA TRA updates will be based on lessons learned from other SCuBA efforts, such as product-specific testing, configuration guidance, capabilities, and instance architectures. Updates will also be informed by input from FCEB agencies; collaborations with CSPs and commercial organizations with mature cloud implementations; and cloud threat assessments, testing, and input from cloud application and infrastructure security Subject Matter Experts (SMEs). Figure 2-1 shows the SCuBA iterative approach.

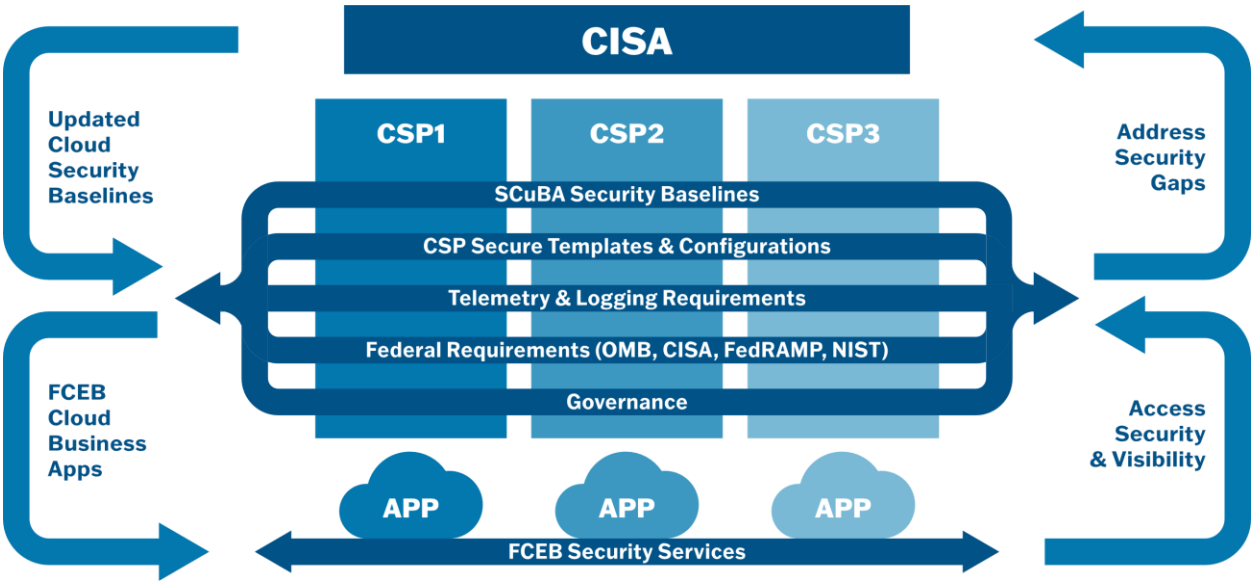

Figure 2-1. SCuBA Iterative Approach

The SCuBA TRA supports CISA's objective to keep pace with evolving technologies and capabilities. It accomplishes this objective through the following iterative approach:

- **Building on Existing Knowledge:** CISA will build on current knowledge of CSP and SaaS offerings to provide guidance based on understanding threats and related efforts. CISA will collaborate with the CSPs to improve the SaaS offerings and how these interface with security services.
- **CISA Cloud Security and SCuBA Baselines:** CISA will first gather and assess feedback and lessons learned from implementing within its own divisions, then it will deploy baselines in response to increasingly complex mission needs. Applying SCuBA security solutions to a wide range of agencies will require iterating on existing technologies and testing new capabilities.
- **Enabling a Feedback Loop:** As agencies deploy cloud solutions to meet mission needs, threats evolve to leverage new tactics, techniques, and procedures (TTPs), and SaaS offerings change to reflect market demands. A feedback loop is required to continue refinement of engineering solutions and improved guidance on configuring SaaS offerings.

3. Definition of Cloud Business Applications

For the initial version of the SCuBA TRA, cloud business applications are defined as including the business capabilities shown in Figure 3-1.

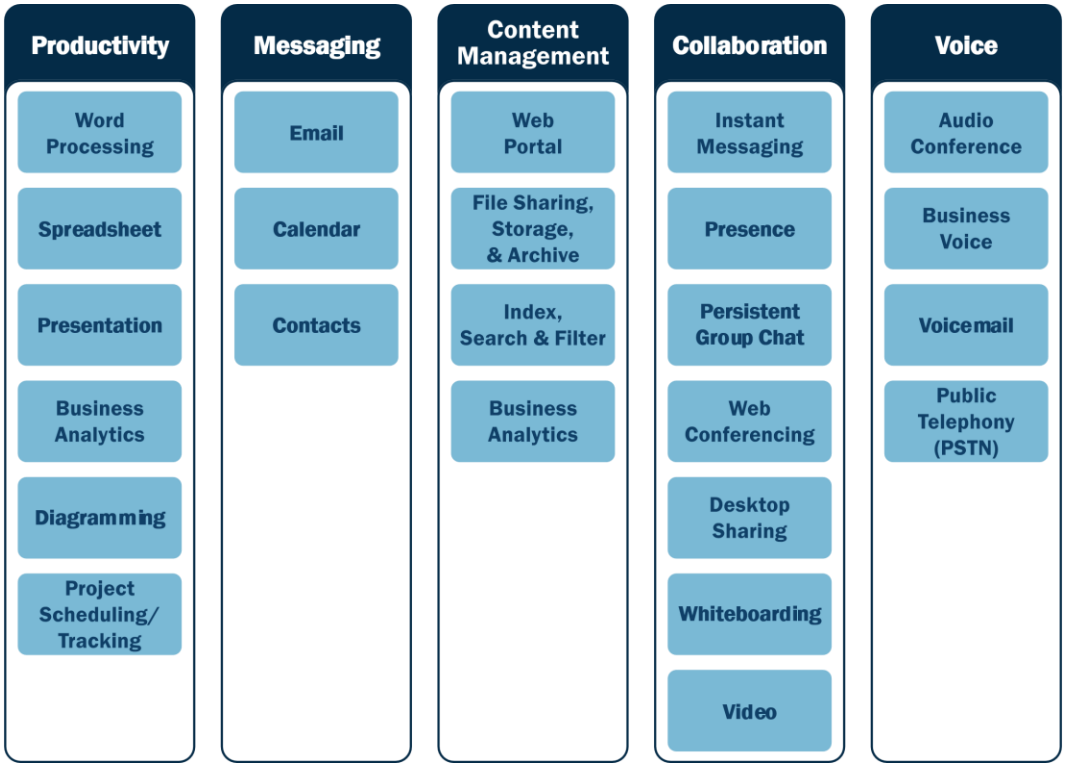

Figure 3-1. Cloud Business Capabilities

Figure 3-1 groups the capabilities into categories using vendor-agnostic terms (Productivity, Messaging, etc.) based on their functions. The examples under each category are not exhaustive, but they are representative of the scope of the functions. Each category may have similar threats and security controls, and agencies can assess the threats and security controls necessary to protect their enterprise and provide CISA the required visibility.

The categories are:

- **Productivity:** Capabilities that allow users to perform business analytics and produce documents, graphs, spreadsheets, presentations, diagrams, project schedules, and trackers. These capabilities produce objects that are human readable and can be shared by Messaging or Content Management capabilities.
- **Messaging:** Capabilities focused on email, calendaring, and contact management.
- **Content Management**: Capabilities for website hosting, file storage and sharing, searching, and workflows.
- **Collaboration**: Capabilities that allow for real-time text, video, and desktop sharing. Productivity capabilities can be used as an integrated function of the Collaboration capabilities.
- **Voice:** Capabilities focused on telephone-based functions, either initiated from a phone (mobile or wired) or to connect to the Public Switched Telephone Network (PSTN).

4. Cloud Security Guidance

The following subsections list cloud security guidance documents that informed the development of the SCuBA TRA.

4.1 CISA Cloud Security Guidance

CISA Cloud Security Technical Reference Architecture

The CISA Cloud Security TRA is a guide for agencies to adopt cloud technology for cloud deployment, adaptable solutions, secure architecture, agile development, and ZT. [3] The guide discusses shared services, cloud migration, and cloud security posture management. Various sections of the SCuBA TRA correspond to the CISA

Cloud Security TRA including Identity, Credential, and Access Management (ICAM); Logging; Monitoring; and Shared Services.

CISA NCPS Cloud Interface Reference Architecture Volumes 1 and 2

The NCPS Cloud Interface Reference Architecture is a two-volume set that explains how agencies can create reporting patterns to describe their process for providing cloud-generated security information to CISA's Cloud Log Aggregation Warehouse. Volume 1 defines general reporting patterns. [5] Volume 2 is a catalog of reporting patterns that are typical of how agencies can send telemetry from a single CSP or from multiple providers. [6] Together these two documents describe multiple options for sharing cloud telemetry with CISA but do not define specific requirements for what cloud telemetry is shared. The extensible Visibility Reference Framework (eVRF), described later in this section, will be used as a framework for CISA to define telemetry requirements.

CISA Trusted Internet Connections 3.0 Core Guidance and Use Cases

The Trusted Internet Connections (TIC) 3.0 core guidance comprises the *Program Guidebook*, the *Reference Architecture*, the *Security Capabilities Catalog*, the *Use Case Handbook*, and the *Overlay Handbook*. [7] Together, these five documents can be used by agencies to develop and deploy modern architectures:

- The *Program Guidebook* outlines the TIC program and explains its history.
- The *Reference Architecture* defines the key technical concepts used to define TIC 3.0 architectures.
- The *Security Capabilities Catalog* is a library of security capabilities that will be used in TIC 3.0 use cases.
- The *Use Case Handbook* describes how agencies can create and use TIC use cases, in general.
- The *Overlay Handbook* defines how vendors can map their products and services to the TIC security capabilities.

Additionally, TIC 3.0 use cases contain guidance on the secure implementation and/or configuration of specific platforms, services, and environments. In accordance with OMB M-19-26, CISA has published the following use cases: (1) Traditional TIC Use Case, (2) Branch Office Use Case, (3) Remote User Use Case, and (4) Cloud Use Case (Draft). These publications contain specific guidance for agency IaaS, PaaS, SaaS, and EaaS deployments. Each TIC use case contains a conceptual architecture, risk and deployment considerations, one or more security pattern options, and security capability implementation guidance for a common agency computing scenario. Agencies can combine use cases to modernize their enterprise.

Continuous Diagnostics and Mitigation

The SCuBA TRA will draw insight and guidance from the CISA CDM Program to provide a dynamic approach to fortifying government network and system cybersecurity. [8] The CDM Program will continue to deliver cybersecurity tools, integration services, and dashboards that help participating agencies improve their security posture. Additionally, the CDM Program is continuing to develop guidance for agencies focused on the integration of cloud platforms into CDM dashboards.

CISA Zero Trust Maturity Model

CISA's *Zero Trust Maturity Model* is one of many roadmaps that agencies may reference as they transition toward a ZT architecture. [9] The maturity model's goal is to assist agencies in developing their ZT strategies and implementation plans. The model also presents ways in which various CISA cybersecurity programs can support ZT solutions across agencies.

extensible Visibility Reference Framework Guidebook

The purpose of eVRF is to define the concepts, requirements, and mechanisms for CISA, FCEB agencies, and other partners to identify, collect, and evaluate cyber visibility to mitigate threats. [10] The *eVRF Guidebook* is an instruction manual for eVRF; it defines and describes key concepts, roles and responsibilities, and workflows. It identifies the demand for visibility as a unique characteristic of cybersecurity, with a structure and workflow that defines visibility for different portions of a digital environment. An eVRF workbook defines specific visibility surfaces and can be implemented with an Excel spreadsheet or a software application. The implementation of eVRF workbooks will continue to evolve over time.

4.2 Federal Cloud Security Guidance

Federal Risk and Authorization Management Program

FedRAMP provides a standardized approach to security authorizations for cloud service offerings. [11] This program provides cloud service offerings to the federal government, adopts innovative cloud services to meet agency mission needs, and acts as a third party to perform initial and periodic security assessments. The cloud business application will follow the FedRAMP authorization process to properly authorize the cloud service offering.

OMB Memorandum: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

The OMB Zero Trust Architecture (ZTA) strategy memorandum (M-22-09) sets forth specific cybersecurity standards and objectives for agencies to fulfill as part of their adoption of ZT architectures. [12] The SCuBA TRA aligns with these objectives and standards. Agencies should consider the actions specified in the memo and their own ZT strategies when designing and implementing security for their cloud business applications to ensure they meet ZT goals.

OMB Memorandum: Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents

The OMB memorandum (M-21-31) establishes logging, log retention, and log management requirements for agencies. [4] Although its requirements are broader than cloud environments, they do apply to cloud; thus, agencies will need to ensure they continue to fulfill these requirements in deploying and maintaining their cloud business applications.

Federal ICAM Architecture Introduction

The Federal Identity, Credential, and Access Management (FICAM) Architecture Introduction describes the basics of ICAM, the FICAM architecture, and how to use the information to facilitate enterprise ICAM practices at an agency. [13] See Section 6.1 for additional information.

5. Threats to Cloud Business Applications

As the threat landscape constantly evolves, an authoritative source for tracking, documenting, and mitigating threats is imperative. Multiple sources for characterizing threats can be used to inform an architecture to secure cloud business applications. Threat identification sources for cloud applications are either open-source or closed source (proprietary/classified). The MITRE ATT&CK® framework will be the primary open-source taxonomy for characterizing threat sources and TTPs for SCuBA.

The MITRE ATT&CK matrix for SaaS and relevant vendor-specific matrices will be used to outline security threats. The MITRE ATT&CK framework is a knowledge base and authoritative source for cyber adversary behavior. The framework outlines various phases of a cyberattack lifecycle and the targets malicious cyber actors are known to exploit. ATT&CK includes only adversarial tactics and techniques based on real-world observations as of the date of the posted matrix, reducing its ability to characterize novel or emerging adversarial activities. eVRF accounts for these emerging threats by characterizing the visibility available for cloud business applications, regardless of whether specific attacker actions have been cataloged in ATT&CK. eVRF further permits mapping of those observables to the ATT&CK techniques applicable to the business applications domain. In this way, eVRF visibility surface definitions and coverage maps can identify visibility that should be available and characterize the visibility that is available within a given system, respectively. See Section 0 for additional details.

6. Securing Cloud Business Applications

This section describes the essential components of security services and capabilities to secure and harden cloud business applications. These security services and capabilities prevent and mitigate vulnerabilities and threats from affecting the cloud business applications during implementation, configuration, and administration.

In addition, once in place, these security services and capabilities harden the system to improve the security of the cloud business applications and the platform where the applications are hosted.

The set of configurations and security services is based on the previously identified business capabilities, threats to those capabilities, and related CISA efforts. Agency-specific implementations of these services should adhere to their specific risk profiles and tolerances. Also, these security configurations, when monitored in real time, serve as a proactive security approach to identify potential cybersecurity threats and help safeguard the environment.

Figure 6-1 illustrates the security and visibility points for SCuBA. Each of the points maps to one or more sections of the SCuBA TRA, as shown in Table 6-1. Additionally, from a ZT perspective, while the security of these applications intersects with each of the pillars described in the ZT Maturity Model, the application security boundary most closely aligns with the application workload pillar.

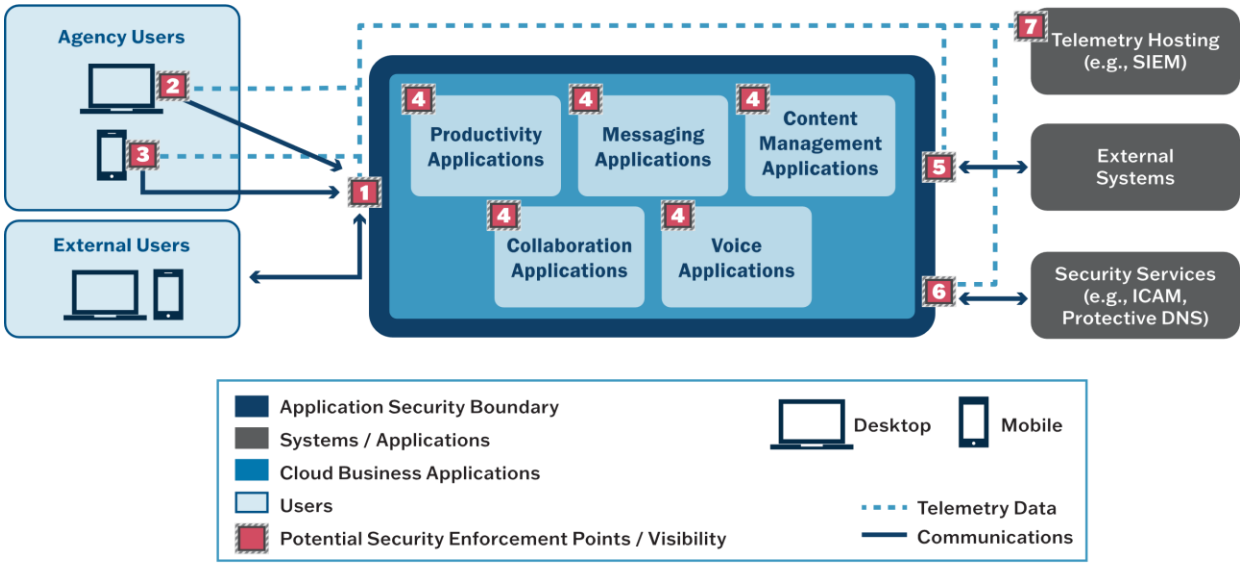

Figure 6-1. SCuBA Security and Visibility View

Table 6-1 maps the numbered security and visibility points to the sections below that cover them .

Table 6-1. Security and Visibility Mapping to Sections

Security Enforcement Point/Visibility	Relevant Sections
1	Section 6.2 Secure Cloud Access from Any Location
2	Section 6.5.1 Desktop Endpoint Security
3	Section 6.5.2 Mobile Endpoint Security
4	Section 6.6 Application Security Configuration
5	Section 6.3 External Email Protections Section 6.6.1 Data Sharing and Exfiltration Protection
6	Section 6.1 Identity, Credential, and Access Management Section 6.4 Protective Domain Name System
7	Section 6.7 Cyber Visibility and the eVRF Analytical Framework Section 6.8 Telemetry Generation and Processing
All	Section 6.7 Cyber Visibility and the eVRF Analytical Framework Section 6.8 Telemetry Generation and Processing Section 6.9 Shared Responsibility Model

6.1 Identity, Credential, and Access Management

ICAM is a core tenet of ZT, and it facilitates cybersecurity risk management decisions. ICAM is the set of tools, policies, and systems that an agency uses to enable the right individual to access the right resource, at the right

time, and for the right reason, in support of federal business objectives. Government Services Administration (GSA) provides guidance on establishing an ICAM program through the implementation of FICAM architecture and the National Institute of Standards and Technology (NIST) Special Publication 800-63-3, *Digital Identity Guidelines*. The FICAM architecture provides the overarching architecture for establishing requirements and guidelines for an ICAM program. NIST's Special Publication 800-63-3 provides the mandatory guidelines to be used to determine various levels of identity proofing, registration, authenticators, authentication protocols, and federation for agencies implementing digital identity services. [14]

Typically, agencies have a pre-existing ICAM program such as the one shown in Figure 6-2. This infrastructure provides central management of identities, issues logical credentials (typically personal identity verification [PIV] cards or derived PIV credentials), and, in some advanced cases, provides central management of roles or entitlements.

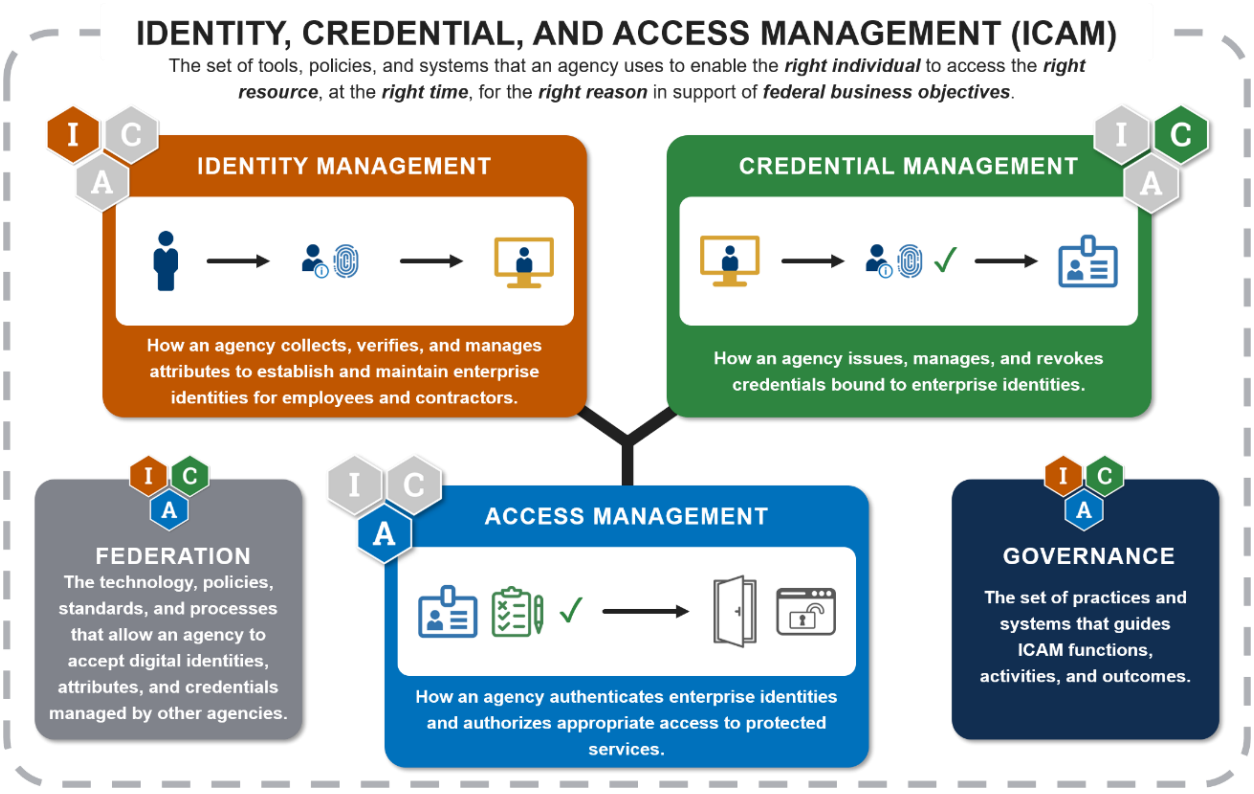

Figure 6-2. ICAM Practice Areas and Supporting Elements [13]

A common deployment of business applications is to federate the pre-existing ICAM infrastructure (e.g., through Microsoft Active Directory Federated Services) with the business applications. (Various configurations are possible, but the details are out of scope of this document.) However, because such a deployment reuses pre-existing infrastructure, certain cybersecurity compromises of on-premises infrastructure could also pose risks to the cloud. The FICAM architecture provides guidance to the Federal Government to design, plan, and execute common ICAM processes. [13] FICAM recommends that only end-user accounts should be federated, and OMB ZTA strategy (M-22-09) states administrative accounts should be authenticated using phishing-resistant multifactor authentication.

An alternative architecture that is becoming more prevalent for agencies leverages a cloud-based Identity as a Service (IDaaS) provider for authentication directly in the cloud (e.g., using a PIV-based credential). Such an architecture adopts a shared responsibility model in which the IDaaS provider assumes responsibility for security of key components of the platform (e.g., cryptographic material required for federation protocols) while the agency remains responsible for secure configuration. Some responsibilities, such as monitoring for threats, are shared between the agency, the vendor, and CISA in this model.

CISA recommends that agencies explore, in detail, the tradeoffs between these two models as relevant to their existing environment and mission goals.

ICAM is critical to securing a cloud application. Many parts of ICAM should be managed enterprise-wide (identity lifecycle, issuance of root credentials, and privilege role assignment, etc.). However, some parts of access management are configured specifically within the cloud business applications. This is especially true with respect to managing end-user access. One important aspect is strong administrative controls and least privilege. Policies—such as Conditional Access in M365 or Context Aware Access in GWS—enable limiting access only to authorized and up-to-date devices. Such policies should be enabled to tie together the Secure Cloud Access (SCA) and endpoint protection technologies. These policies "close the loop" by ensuring that agency data is only accessible by devices that follow the agency's desired security posture. CISA is developing secure configuration baselines specific to cloud-native identity and access management services for M365 [10] and GWS to support these identity- and access-focused considerations.

6.2 Secure Cloud Access from Any Location

With the growth of mobile, telework, and cloud applications, traditional approaches to secure cloud access no longer meet the needs of the FCEB. The TIC program recognizes this and articulates a new model for securing access to cloud applications. The SCuBA TRA uses the TIC 3.0 guidance as the foundation for securing user access to business applications; this capability is called, "secure cloud access" or "SCA." SCA solutions should be part of agencies' cloud business application deployment. In the broader cloud market, vendors use terms such as Zero Trust Network Access, Cloud Access Security Broker (CASB), Secure Email Gateway (SEG), Secure Access Service Edge, and others to refer to products and services that target different aspects of SCA. The broader market is rapidly evolving as these discrete solutions converge.

SCA solutions give users the ability to securely access the agency's business applications that reside on a CSP. These business application users may be on the enterprise network, in a branch office, on a remote device, or on a mobile device. A non-person entity[1] (NPE) may also be a user of agency business applications. The SCA solution, along with the security services embedded in the destination CSP and the source workstation or device (e.g., endpoint detection and response [EDR]) follow the TIC guidance. Different use cases and security patterns may require other technical solutions. SCA security functions may be the same as, or complement, the source workstation or device and CSP security functions. For example, SCA functions may be provided by the CSP, the source workstation or device, a third-party vendor, or all of these. See Figure 6-3 for an overview graphic of a SCA concept.

The SCuBA TRA provides only an introduction to the SCA topic. TIC 3.0 guidance documents can provide additional information on design alternatives for different SCA use cases.

[1] NPE: An entity with a digital identity that acts in cyberspace but is not a human actor. This can include organizations, hardware devices, software applications, and information artifacts. Source(s): CNSSI 4009-2015 from DHS OIG 11-121.

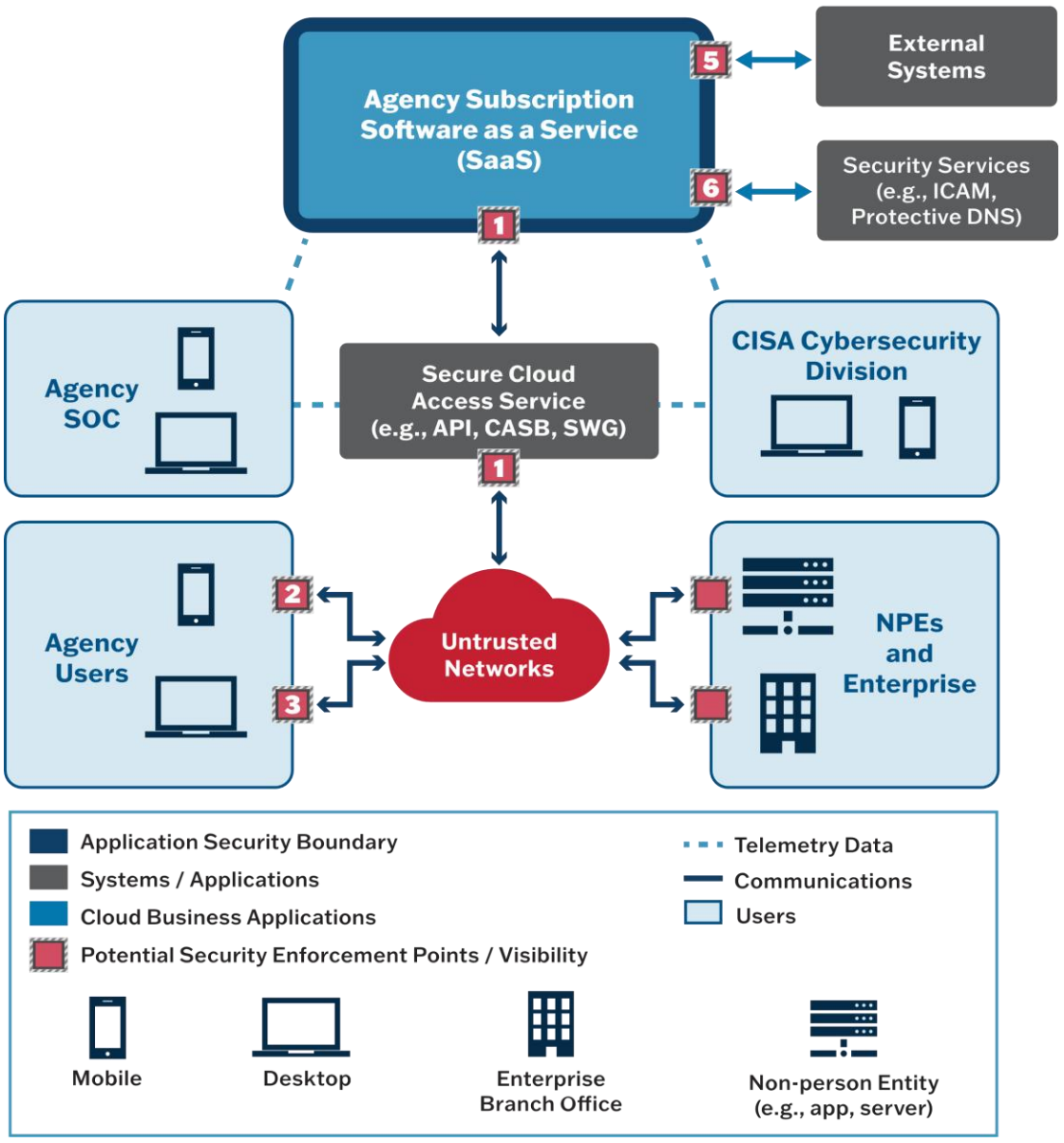

Figure 6-3. SCA Concept

6.3 External Email Protections

Email is often used as an entry point to agency environments, as shown in Figure 6-4. It is used by adversaries for delivering both phishing links and malware, as seen in recent high-visibility attacks. Email-related risks are typically addressed with a combination of native security capabilities built into the CSP's products as well as independent third-party offerings. Historically, these capabilities for federal executive branch agencies were provided by EINSTEIN 3 Accelerated (E3A), administered by CISA. Typically, email security solutions (whether provided as a native security capability in a CSP offering or as a separate product) include the following:

- **Filtering and Tagging**: Email filtering of all messages (e.g., ingress, egress, internal) for detecting malware, identifying spam, and tagging for agencies. This includes the use of both government (i.e., CISA, agency) and commercial indicators and attributes (behavioral and reputational) for malware detection, and spam identification and tagging for agencies, including the use of both government (i.e., CISA, agency) and commercial indicators and attributes (behavioral and reputational).
- **Log Visibility**: Visibility into email attributes should be provided to both CISA and agency security operations personnel.

- **Authentication and Integrity**: Modern techniques for ensuring sending and receiving email servers are mutually authenticated and messages are not manipulated in transit. This is accomplished using Domain-based Message Authentication, Reporting, and Conformance, Sender Policy Framework, and Domain Keys Identified Mail.
- **Additional Features**: Other key features in robust email security protections include automated indicator provisioning, threat intelligence, advanced analytics, reporting, cyber hunt support and incident response, sandboxing, detonation, and the ability to incorporate third-party security services.

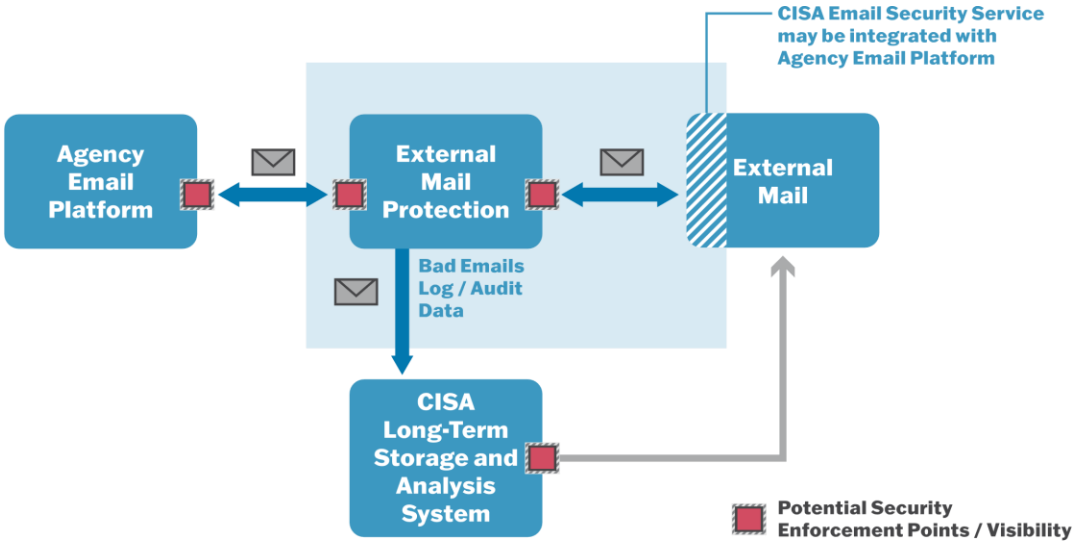

Figure 6-4. External Email Flow

CISA is also developing secure configuration baselines (see Section 6.6) that relate to email security. Identity-related configuration requirements and baselines in development also support email security. Agencies should integrate external email protections and implement secure configuration baselines for critical cloud services that affect email security, such as Exchange Online, Azure Active Directory, and Google Cloud Identity.

6.4 Protective Domain Name System

In addition to SCA solutions that apply policy to and collect telemetry from network flows between endpoints and cloud applications, domain name system (DNS) lookup provides a widely used insertion point in internet infrastructure to implement cybersecurity policy and visibility. Secure DNS solutions' key capabilities include:

- internet protocol (IP) v4 and v6 source address verification;
- query filtration by IP, domain, subdomain, or record type;
- auto-blockage of newly created domains, "look-alike" homoglyphs, nonstandard query structures, and known risky domains;
- self-monitoring heuristics to gauge percentage of correctly permitted (benign) queries, correctly blocked (malign) queries, and anomalous false positives;
- direct bypass, for use cases where crucial DNS queries must go through;
- location blocking;
- DNS over Transport Layer Security (DoT) and DNS over Hypertext Transport Protocol Secure; and
- telemetry collection for both the agency and CISA (i.e., to discover outbound Command and Control traffic).

CISA is developing a new DNS service to replace the legacy E3A domain sinkholing functionality. Agencies should deploy the CISA DNS security solution (when available) or equivalent protective DNS capabilities, including customizable DNS query filtration, such as "allow," "deny" (block), "overwrite" (rewrite) response, or "sinkhole" (suppression), based on domain parameters, encrypted DNS support, DoT support, DNS security extensions support, and compatibility with current Internet Engineering Task Force (IETF) DNS protocol extensions.

6.5 Endpoint Security Services

Managing endpoints (both mobile and desktop) is critical to securing cloud business applications and to support a ZT approach. Although mobile security is not within the scope of the SCuBA project itself, it is expected that agencies will need to deploy and configure their cloud business applications to enable access from their mobile and desktop devices.

6.5.1 Desktop Endpoint Security

SCuBA relies upon endpoint security technologies for both policy and visibility. The cloud business application access policies should be configured to limit access to agency data based on host posture assessment (see Section 6.6). In other words, the policies should enforce that all sensitive data requests come from agency-managed devices that comply with agency endpoint security policies, such as operating system version and patch level (or devices explicitly authorized by risk-based policy decisions supporting mission needs). EDR products can be used to collect the signals necessary for these policy decisions to be made and to provide critical visibility into the endpoints that enable cybersecurity response.

Agencies should leverage the CDM Program to obtain and deploy EDR technologies in their environment. Additionally, the cloud business application should be configured to leverage signals from the EDR products to govern access to private agency data.

Endpoints not managed by the agency, such as those of guests, collaborators, partners, customers, or even agency users' personal devices, will have limited opportunities for agency policy enforcement or evaluation. The breadth of access to agency data should reflect this limited insight by reducing or even prohibiting access to sensitive information.

6.5.2 Mobile Endpoint Security

Similar access policies should also be configured for agency-managed mobile endpoints. To protect and manage mobile devices and applications, the CDM Program helps agencies deploy Enterprise Mobility Management (EMM) capabilities. [15] EMM solutions enable agencies to manage device configuration and device compliance; monitor and track devices; manage allowed mobile apps; detect and address malicious mobile apps via mobile threat defense and mobile application vetting; discover and respond to network-based attacks and vulnerable configurations; and support the issuance and life cycle management of credentials provisioned on mobile devices. Agencies' cloud business applications should be configured to leverage signals from EMM solutions in access decisions.

CISA also published Capacity Enhancement Guides to help enterprises and consumers improve cybersecurity of their mobile devices. [16] To support agencies as they develop their ZT plans and roadmaps, CISA developed a whitepaper titled "Applying Zero Trust Principles to Enterprise Mobility." [17] The paper describes mobile security technologies, explains how they support ZT principles, and identifies areas requiring additional work.

6.6 Application Security Configuration

As the federal government continues to move critical services to the cloud, it is imperative to ensure consistent, effective, modern, and manageable security configurations to protect all information assets in and connections to cloud services. The objective of this initiative is to move federal cybersecurity forward by helping agencies keep pace with sophisticated and determined cyber threats. At the time of this writing, the SCuBA project is developing and testing minimum viable security baselines that can be easily and quickly adopted across the federal civilian landscape. A "Security Baseline" defines a set of basic security objectives that must be met by any given service or system. (See Figure 2-1 for a visual representation of where these artifacts sit within the iterative approach to the SCuBA TRA development.)

A key benefit of this work is that agencies using M365 and GWS can adopt these recommended cybersecurity configurations. Maintaining and updating this guidance is essential to ensuring an acceptable and consistent security posture. These efforts are led by CISA with input and support from interested federal agencies. The baselines are also developed with an eye towards automation rather than manual repetitive tasks where possible, improving consistency in application and reducing time to deployment.

The baselines cover the full scope of the security architecture for SCuBA, including ICAM, collaboration, cloud access security broker capabilities, threat intelligence, detection, mitigation, cloud storage, cloud-native email

service security, and cloud-native business applications. Additional baselines may be selected as CISA continues maturing SCuBA.

6.6.1 Data Sharing and Exfiltration Protection

Another SCuBA security concern is data sharing and data exfiltration risk. Agencies must balance the need to collaborate with other stakeholders outside the agency (and thus share content, calendars, etc.) with the need to protect agency data.. At a minimum, agencies should use cloud business applications' built in rules systems to detect cross-tenant data sharing. These rules can be used to discover exfiltration of important agency data. In some cases, agencies may also choose to block cross-tenant sharing of certain types of data (e.g., share busy/free status but not documents), depending on mission requirements.

6.7 Cyber Visibility and the eVRF Analytical Framework

Agencies will need to collect and apply cyber visibility, both operational and technical (e.g., insights into assets, users, systems, data, events, logs), to detect potentially malicious activities associated with the use of cloud business applications. These activities include the application of key eVRF concepts. The fundamental purpose of the *eVRF Guidebook* is to define the concepts, requirements, and mechanisms for CISA, FCEB agencies, and other partners to collect and apply cyber visibility to mitigate threats. In the context of SCuBA, an applicable eVRF concept is that of the visibility surface, which is defined as "a digital environment for which cyber-observable data exists or should exist." [10] The application logs, endpoint access logs, proxy logs, service logs, reports, and alerts generated with the monitoring, auditing, and alerting services are essential parts of this digital environment and will provide evidence of malicious and benign activity. Section 6.1 identifies sources for such telemetry. Analysts from agencies, CISA, and vendors each have a unique role and associated visibility demands for telemetry from these sources that are stored in the Telemetry Hosting solution. These visibility demands will need to be accommodated when deploying and configuring services to ensure coverage. Use of the eVRF workflow can assist in characterizing visibility completeness.

The *eVRF Guidebook* identifies three phases of the workflow for accomplishing cyber visibility: (1) define visibility surface, (2) produce visibility coverage maps, and (3) generate coverage comparisons for analysis and insights. Figure 6-5 describes these process phases and includes a detailed description for each. The execution steps are provided in the referenced document. [10]

Figure 6-5. eVRF Workflow

The *eVRF Guidebook* identifies roles and responsibilities for CISA, organizations (agencies), and vendors/service providers. [10] In summary, CISA has the responsibility for developing an eVRF visibility surface definition and requirements coverage map in an eVRF workbook. Agencies are to use this eVRF workbook to guide their internal policies and align with CISA's cyber visibility requirements, and vendors/service providers can work to reduce or eliminate visibility gaps in their offerings.

An eVRF workbook can be implemented as a purpose-built software application, using a spreadsheet or tables. Ultimately, a purpose-built software application would offer the most flexible way to create and edit a visibility surface definition and coverage maps.

6.8 Telemetry Generation and Processing

The quality and completeness of the visibility offered to cyber analysis is dependent upon the observation points and telemetry-generating system components. The following subsections outline what services agencies will need to use to ensure effective security visibility and management of cloud business applications. In implementing these services, agencies should comply with the logging requirements issued by OMB M-21-31 [4] and consult NIST Special Publication 800-92 [18] for additional guidance on security log management.[2] This will enable agencies to collect the logs they need for their own security operations and to provide additional visibility to CISA.

6.8.1 Logging

Agencies will need to configure their cloud services to generate logs for their applications to enable various cybersecurity outcomes: improved visibility, asset management, incident response, and more. They are also essential to fulfill many compliance requirements. By leveraging the eVRF workbook for SCuBA, agencies can determine the necessary log data that must be collected to enable these outcomes and detect different TTPs as well as what logs must be shared with CISA.

To ensure appropriate levels of visibility, logs from multiple observation points must be collected. Figure 6-6 presents an alternate SCuBA security and visibility view that emphasizes the collection of telemetry and logs.

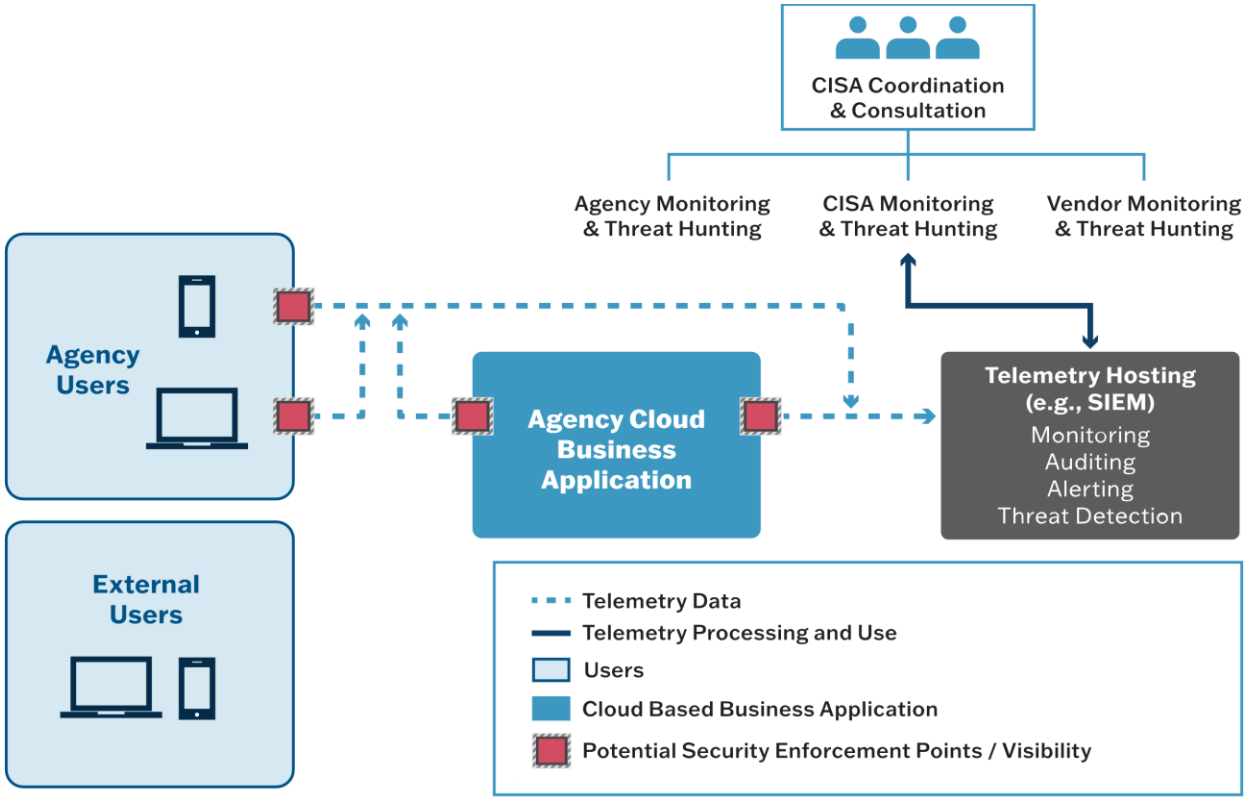

Figure 6-6. SCuBA Telemetry

[2] NIST is in the process of revising the NIST Special Publication 800-92 (https://csrc.nist.gov/Projects/log-management).

In cloud business applications, logs should be collected from each of the key building blocks previously identified:

- The SCA solution
- The endpoint solutions
- The SCuBA application platform (M365/GWS)
- The security services, such as the ICAM solution (whether on-premises or cloud-based) and the secure DNS solution

As shown in Figure 6-6, the telemetry and logs can be aggregated via the Telemetry Hosting solution to facilitate analysts' needs and internal agency monitoring, auditing, alerting, and threat detection activities. An eVRF visibility surface definition and OMB M-21-31 [4] logs should capture both key business events (e.g., send/receive email, document sharing outside of tenant) as well as configuration changes (e.g., new user creation, policy updates) as both can be indicative of cybersecurity events. Logs should be generated in an automated fashion. They can be configured to capture numerous pieces of contextual information about cloud activities, accesses, and resource states; this often includes fields or attributes such as associated user ID, resource ID, Application Programming Interface (API) name, timestamp, IP addresses, etc. Specific metadata are identified in more detail in the eVRF visibility surface definition. Agencies will need to manage issues associated with scaling, retention, access, privacy, provenance, exportability, and timeliness—among other issues—of their logs as well as ensure that the logs that must be shared with CISA in real time are properly delivered as per the NCPS Cloud Interface Reference Architecture. [5], [6]

6.8.2 Monitoring

While some logs may be stored for record keeping and compliance purposes, others will be monitored, audited, and analyzed as part of broader agency security posture management. Agencies should therefore incorporate logs from their cloud business applications into their monitoring services to update tracking metrics, conduct resource mapping, and generate security reports, which will in turn facilitate auditing, alerting, and threat detection. The same applies for new security services deployed as part of SCuBA adoption.

6.8.3 Auditing

Agencies should conduct further analysis of their application logs and security reports through security auditing. This can address various contextual questions for a potential event, such as which users, processes, services, or applications were involved; what was done; where it took place; when it occurred and over what time period; how it occurred; and the impacts. Auditing services allow agencies to better understand what is happening within (and to) their cloud environments and ensure they are operating as desired. This is a more labor-intensive process than automated monitoring and report generation, as it typically involves a human policy decision point (as opposed to a technology policy decision point). Periodic audits can further seek to discern not only whether given transactions *can* occur, but whether they *should* occur in normal operating conditions and states. The additional review of organizational visibility (i.e., the awareness of business functions, priorities, risks, and collaboration agreements) enhances auditor precision and can provide further insights to an agency.

6.8.4 Alerting

Agencies should create alerts for their business applications that automatically generate based on their monitoring and auditing data. Alerts will enable agencies to quickly identify various issues with business applications, such as misconfigurations, unauthorized access, and privilege changes, as well as other anomalous activities for review and remediation. Such alerts will represent the result of defects or heuristically derived detections and should be given preferential treatment in analysis tools and dashboards (with respect to the raw data used to generate the alerts). Agencies should integrate these alerts into their existing Security Operations Center (SOC) procedures and leverage their existing Security Information and Event Management (SIEM) and Security Automation, Orchestration, and Response (SOAR) tooling to respond to security alerts.

6.8.5 Threat Detection

Agencies can leverage a variety of tools and services to detect and mitigate potentially malicious activity taking place within or against their cloud environments through business applications. These can include threats such as denial of service, data exfiltration, malware injection, unauthorized privilege escalation and account creation, etc. Threats may be detected using automated means or manual discovery. Data visualization tools and

dashboards can assist agency analysts in detecting threats against agency cloud business applications. Agencies should review threat-detection services offered natively by their service provider as well as stand-alone and third-party offerings to incorporate anomaly detection, machine learning, threat intelligence, etc., within their threat detection capabilities for their cloud business applications. Agencies should test these services to benchmark fidelity in the alerts generated and latencies in detection. Agencies should also update their logging, monitoring, auditing, and alerting policies and procedures based on lessons learned from their threat detection capabilities (i.e., to incorporate analytics for newly discovered threats, reduce false positives, and expand visibility coverage to mitigate gaps).

6.9 Shared Responsibility Model

The SCuBA TRA relies on a shared responsibility model, as shown in Figure 6-7 and described in the following subsections, between the agency, CISA, and the selected vendors. Each plays a critical role in ensuring a robust security posture and achieving the desired security outcomes. This is true both with respect to protective security controls as well as visibility, detection, and response.

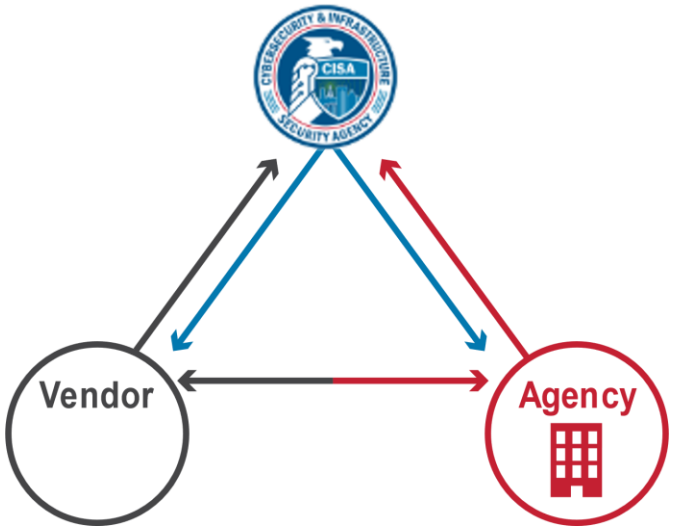

Figure 6-7. Shared Responsibility Model

6.9.1 Protective Security Controls and Services

- **Agencies**: Agencies are responsible for properly configuring their chosen cloud business application platform in accordance with the SCuBA solution architecture documents. Agencies are also responsible for ensuring that their SCuBA deployment leverages appropriate capabilities of their other security services as discussed in Sections 6.1 and 6.5.
- **Vendors**: Vendors are responsible for securing the underlying SaaS platform behind the business applications. Vendors should also offer agencies the necessary product capabilities to implement the required security controls, including integrations with independent software vendor solutions (e.g., to provide email security services or identity services) if necessary.
- **CISA**: CISA is responsible for defining the baseline security requirements, architectures, and configurations necessary to realize the SCuBA vision. CISA is also responsible for developing shared services to implement pieces of the TRA.

6.9.2 Visibility, Detection, and Response

- **Agencies**: Agencies are responsible for first-line security operations, such as alert triage and response to limited-scope incidents. Agencies collect and retain logs per OMB M-21-31 and CISA guidelines (both the CISA logging guidance as well as the eVRF CISA visibility requirements). Agencies can leverage CISA-provided shared services to enhance their logging and security monitoring operations. Agencies are also encouraged to coordinate with their vendors and/or service providers on the application of telemetry configuration and visibility coverage map generation, which may include feature requests in future product releases.

- **Vendors**: Cloud business application providers can share vulnerability and breach-related information with CISA and agencies to enhance situational awareness and facilitate response activities. Additionally, vendors can identify trends and threat activities across sectors and service offerings. They can respond to threats that are undetectable to their tenants and update their offerings to mitigate vulnerabilities and adversarial campaigns. Vendors can also share information about updates and changes to their products, share guidance on how to effectively use their offerings as engineered, and provide formal instruction and training opportunities to ensure consistent understanding of product limitations and features.
- **CISA**: CISA's duties include refining visibility requests, updating baselines, and providing response support. One of CISA's primary responsibilities is to assist agencies in threat discovery and remediation. Thus, CISA will engage with FCEB agencies to facilitate data acquisition of cloud logs and telemetry to ensure delivery aligns with CISA's preferences for timeliness, frequency, format, and other attributes, as described in the *National Cybersecurity Protection System Cloud Interface Reference Architecture Volume Two: Reporting Pattern Catalog*. [6] This telemetry will enable CISA's analysis, incident response, and threat hunting activities. CISA will engage cloud vendors to mitigate security and visibility gaps providing enhanced security for cloud business applications. CISA will also coordinate with cloud vendors to mitigate risks facing FCEB agencies' cloud services through information sharing and the deployment of security services.

7. References

[1] 117th Congress, "H.R. 1319 - American Rescue Plan Act of 2021," Senate and House of Representatives of the United States of America, Washington, D.C., 2021.

[2] 116th Congress, "H.R. 6395, National Defense Authorization Act for Fiscal Year 2021," Senate and House of Representatives of the United States of America, Washington, D.C., 2021.

[3] CISA, United States Digital Service, and Federal Risk and Authorization Management Program, "Cloud Security Technical Reference Architecture," 2021. [Online]. Available: https://www.cisa.gov/cloud-security-technical-reference-architecture.

[4] Office of Management and Budget, "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents," 27 August 2021. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf. [Accessed 15 November 2021].

[5] CISA, "CISA NCPS Cloud Interface Reference Architecture Volume 1: General Guidance," Cybersecurity and Infrastructure Security Agency, Arlington, VA, 2020.

[6] CISA, "National Cybersecurity Protection System Cloud Interface Reference Architecture Volume Two: Reporting Pattern Catalog," Cybersecurity and Infrastructure Security Agency, Arlington, VA, 2020.

[7] CISA, "Trusted Internet Connections Guidance Repository," Cybersecurity & Infrastructure Security Agency (CISA), [Online]. Available: https://www.cisa.gov/tic-guidance. [Accessed February 2022].

[8] CISA, "Continuous Diagnostics and Mitigation CDM)," CISA CDM Program Management Office, [Online]. Available: https://www.cisa.gov/cdm. [Accessed January 2022].

[9] CISA , "Zero Trust Maturity Model," June 2021. [Online]. Available: https://www.cisa.gov/zero-trust-maturity-model. [Accessed Jan 2022].

[10] CISA, "CISA Blog on SCuBA," [Online]. Available: https://www.cisa.gov/blog/2022/03/31/secure-cloud-business-applications.

[11] General Services Administration, "FedRAMP," [Online]. Available: https://www.gsa.gov/technology/government-it-initiatives/fedramp. [Accessed January 2022].

[12] Office of Management and Budget, "Moving the U.S. Government Towards Zero Trust Cybersecurity Principles," 26 January 2022. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf. [Accessed Febuary 2022].

[13] General Services Administration (GSA), "Federal ICAM Architecture Introduction," IDManagement.gov, 6 January 2021. [Online]. Available: https://playbooks.idmanagement.gov/arch/. [Accessed January 2022].

[14] P. Grassi, M. Garcia and J. Fenton, "NIST Special Publication 800-63-3, Digital Identity Guidelines," June 2017. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63-3.html. [Accessed November 2021].

[15] CISA, "Continuous Diagnostics and Mitigation Program, Technical Capabilities, Vol 2: Requirements Catalog," Cybersecurity and Infrastructure Security Agency (CISA), Arlington, VA, 2020.

[16] CISA, "CISA Releases Capacity Enhancement Guides to Enhance Mobile Device Cybersecurity for Consumers and Organizations," Cybersecurity & Infrastructure Security Agency, 24 November 2021. [Online]. Available: https://www.cisa.gov/uscert/ncas/current-activity/2021/11/24/cisa-releases-capacity-enhancement-guides-enhance-mobile-device. [Accessed December 2021].

[17] CISA, "Applying Zero Trust Principles to Enterprise Mobility. (DRAFT)," Cybersecurty & Infrastructure Security Agency, Arlington, VA, Not released to date..

[18] National Institute of Standards and Technology (NIST), "NIST Guide to Computer Security Log Management," 13 September 2006. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-92/final. [Accessed 15 November 2021].

[19] Federal Mobility Group, "International Travel Guidance for Government Mobile Devices DRAFT," Federal Mobility Group, Arlington, VA, 2021.

[20] Federal Mobility Metrics Working Group (FMMWG) , "Federal Mobility Metrics Working Group (FMMWG)," Federal Mobility Group (FMG) and Advanced Technology Academic Research Center (ATARC), Arlington, VA, 2021.

Appendix A. Glossary

Application Programming Interface (API): A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.

Cloud Service Provider (CSP): An external company that provides a platform, infrastructure, applications, and/or storage services for its clients.

Continuous Diagnostics and Mitigation (CDM): A CISA program that provides a dynamic approach to fortifying government networks and systems cybersecurity by delivering cybersecurity tools, integration services, and dashboards that help participating agencies improve their security posture.

Domain Name System (DNS): A system that stores information associated with domain names in a distributed database on networks. DNS translates IP addresses into human-understandable names.

Enterprise Mobility Management (EMM): A suite of services and technologies that enables an agency to secure the use of mobile devices (e.g., tablets, smartphones, and e-readers) per the agency's policies. Components of an EMM include mobile device management, mobile application management, and mobile identity management.

extensible Visibility Reference Framework (eVRF): Defines the concepts, requirements, and mechanisms for CISA, FCEB agencies, and other partners to collect and apply cyber visibility to mitigate threats. eVRF was created in response to Executive Order 14028, "Improving the Nation's Cybersecurity."

Federal Civilian Executive Branch (FCEB): A subset of U.S. federal departments and agencies that excludes the Department of Defense and agencies in the intelligence community.

Identity, Credential, and Access Management (ICAM): A fundamental and critical cybersecurity capability that ensures the right people and NPEs have the right access to the right resources at the right time.

Internet Engineering Task Force (IETF): A large, open, international internet standards body comprised of network designers, operators, vendors, and researchers interested in how the internet architecture evolves and the smooth operation of the internet. The IETF technical work of developing open standards through open processes is done in working groups that are organized by topic into several areas.

Mobile Application Vetting (MAV): Performs enterprise-level security analysis of managed apps and their libraries prior to deployment and throughout the lifecycle of the apps. Integration of EMM with MAV provides the ability for the EMM to apply mitigations (e.g., uninstall app or block access to enterprise resources).

Mobile Threat Defense (MTD): Helps detect the presence of malicious apps or software, malicious activity, and connections to deny-listed websites or networks. Integration of EMM with MTD provides the ability for MTD to notify the EMM of malicious apps or activity on a mobile device so that the EMM can provide mitigations.

Multifactor Authentication (MFA): An authentication system that requires more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or a combination of authenticators that provide different factors.

Secure Cloud Access (SCA): A subset of remote access solutions that provide the ability for a trusted user on a remote workstation to securely access the agency's business application on a cloud service provider.

Security Information and Event Management (SIEM): An application that is used to gather security data from across systems to facilitate monitoring, analysis, triaging, and alerting through a single interface.

Security Operations Center (SOC): A centralized operations center for monitoring, analyzing, detecting, and responding to security information and security incidents.

Security Orchestration, Automation, and Response (SOAR): A platform or collection of technologies for coordinating, defining, automating, and executing tasks to analyze and respond to security data and security incidents. This often includes threat and vulnerability management technologies, security incident response capabilities, and additional tools that enable automation across security operations.

Software-as-a-Service (SaaS): The capability provided to the consumer to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Technical Reference Architecture (TRA): A document that illustrates recommended approaches to cloud migration and data protection, as outlined in Section 3(c)(ii) of Executive Order 14028. As the federal government continues to transition to the cloud, the TRA will be a guide for agencies to leverage when migrating to the cloud securely. Additionally, the document explains considerations for shared services, cloud migration, and cloud security posture management.

Telemetry: Artifacts derived from security capabilities that provide visibility into security posture.

Zero Trust (ZT): Per Executive Order 14028, "the term ''Zero Trust Architecture'' means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. … In essence, a Zero Trust Architecture allows users full access but only to the bare minimum they need to perform their jobs. If a device is compromised, zero trust can ensure that the damage is contained. The Zero Trust Architecture security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity."

Appendix B. Abbreviations

Abbreviation	Definition
API	Application Programming Interface
ATT&CK	[MITRE] Adversarial Tactics, Techniques, and Common Knowledge
BYOD	Bring Your Own Device
CASB	Cloud Access Security Broker
CDM	Continuous Diagnostics and Mitigation
CISA	Cybersecurity and Infrastructure Security Agency
CSP	cloud service provider
DHS	Department of Homeland Security
DNS	domain name system
DoT	DNS over Transport Layer Security
E3A	EINSTEIN 3 Accelerated
EDR	endpoint detection and response
EMM	Enterprise Mobility Management
eVRF	extensible Visibility Reference Framework
FCEB	Federal Civilian Executive Branch
FedRAMP	Federal Risk and Authorization Management Program
FICAM	Federal Identity, Credential, and Access Management
GSA	Government Services Administration
GWS	Google Workspace
ICAM	Identity, Credential, and Access Management
IDaaS	Identity as a Service
IETF	Internet Engineering Task Force
IP	internet protocol
IT	information technology
M365	Microsoft 365
MAV	mobile application vetting
MFA	multi-factor authentication
MTD	Mobile Threat Defense
NCPS	National Cybersecurity Protection System
NIST	National Institute of Standards and Technology
NPE	non-person entity
OMB	Office of Management and Budget
pDNS	protective domain name system
PIV	personal identity verification
PSTN	Public Switched Telephone Network
RA	Reference Architecture
SaaS	Software-as-a-Service
SCA	Secure Cloud Access
SCuBA	Secure Cloud Business Applications

Abbreviation	Definition
SEG	Secure Email Gateway
SIEM	Security Information and Event Management
SME	subject matter experts
SOAR	Security Automation, Orchestration, and Response
SOC	Security Operations Center
TIC	Trusted Internet Connection
TRA	Technical Reference Architecture
TTPs	Tactics, Techniques, and Procedures
ZT	Zero Trust
ZTA	Zero Trust Architecture