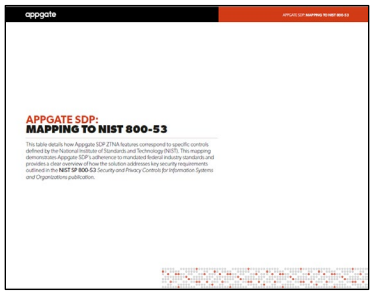
appgate

carahsoft



Appgate SDP: Mapping to NIST 800-53

Security and Privacy Controls

Thank you for downloading this Appgate resource. Carahsoft is the Master Government Aggregator® for Appgate's Cybersecurity solutions available via GSA, NCPA, NJSBA, and other contract vehicles.

To learn how to take the next step toward acquiring Appgate's solutions, please check out the following resources and information:

For additional resources:
carah.io/AppgateResources

For upcoming events:
carah.io/AppgateEvents

For additional Appgate solutions:
carah.io/AppgateSolutions

For additional Cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
Appgate@carahsoft.com
703-230-7577

To purchase, check out the contract vehicles available for procurement:
carah.io/AppgateContracts

APPGATE SDP: MAPPING TO NIST 800-53

This table details how Appgate SDP ZTNA features correspond to specific controls defined by the National Institute of Standards and Technology (NIST). This mapping demonstrates Appgate SDP's adherence to mandated federal industry standards and provides a clear overview of how the solution addresses key security requirements outlined in the **NIST SP 800-53** *Security and Privacy Controls for Information Systems and Organizations publication.*

CLASS	FAMILY	NUMBER	TITLE	IMPACT	PRIORITY	DESCRIPTION	SUPPLEMENTAL-GUIDANCE	RELEVANCE TO APPGATE SDP	DISCUSSION
Technical	Access Control	AC-03	Access Enforcement	LOW_ MODERATE_ HIGH	P1	The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.	Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to enforcing authorized access at the information-system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of an audited, explicit override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant. For classified information, the cryptography used is largely dependent on the classification level of the information and the clearances of the individuals having access to the information. Mechanisms implemented by AC-3 are configured to enforce authorizations determined by other security controls. Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SC-13, SI-9.	High	Appgate SDP supports all stated policy control paradigms, whether if be, identity-based policies, role-based policies, and attribute-based policies. The product ships with and access control list, matricies, and, where applicable, cryptographic enforcement mechanisms.
Technical	Access Control	AC-04	Information Flow Enforcement	MODERATE_ HIGH	P1	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few examples of flow control restrictions include: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on content (e.g., using key word searches or document characteristics). Mechanisms implemented by AC-4 are configured to enforce authorizations determined by other security controls. Related controls: AC-17, AC-19, AC-21, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.	High	Appgate SDP provides a highly extensible policy engine for enforcing approved authorizations for controlling the flow of information within and amongs systems. Further enhancing this, Appgate SDP ships with native integrations for the major CSPs, enabling identity context awareness and data driven policies.
Technical	Access Control	AC-05	Separation of Duties	MODERATE_ HIGH	P1	The organization: Separates duties of individuals as necessary, to prevent malevolent activity without collusion; Documents separation of duties; and Implements separation of duties through assigned information system access authorizations.	Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security); (iii) security personnel who administer access control functions do not administer audit functions; and (iv) different administrator accounts for different roles. Access authorizations defined in this control are implemented by control AC-3. Related controls: AC-3.	High	There is a non exhaustive capability to enable the separate seperation of duties in any manner an organization deems best. All possible permutations and combinations of the identity, role, and attributes can be used to support this.
Technical	Access Control	AC-06	Least Privilege	MODERATE_ HIGH	P1	The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	The access authorizations defined in this control are largely implemented by control AC-3. The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. Related controls: AC-2, AC-3, CM-7.	High	Appgate SDP policies are default-deny and only through explicit entitlement assignment is access facilitated.

CLASS	FAMILY	NUMBER	TITLE	IMPACT	PRIORITY	DESCRIPTION	SUPPLEMENTAL-GUIDANCE	RELEVANCE TO APPGATE SDP	DISCUSSION
Technical	Access Control	AC-07	Unsuccessful Login Attempts	LOW_ MODERATE_ HIGH	P2	The information system: Enforces a limit of [Assignment: organization-defined number] consecutive invalid login attempts by a user during a [Assignment: organization-defined time period]; and Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period] ; locks the account/node until released by an administrator; delays next login prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.	Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization. If a delay algorithm is selected, the organization may chose to employ different algorithms for different information system components based on the capabilities of those components. Response to unsuccessful login attempts may be implemented at both the operating system and the application levels. This control applies to all accesses other than those accesses explicitly identified and documented by the organization in AC-14.	High	Due to the extensible nature of Appgate SDP's policy engine, conditionalized enforcement based on Unsuccessful Login Attempts is available, so long as the enterprise SSO/IdP makes said information available.
Technical	Access Control	AC-08	System Use Notification	LOW_ MODERATE_ HIGH	P1	The information system: Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording; Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.	System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. System use notification is intended only for information system access that includes an interactive login interface with a human user and is not intended to require notification when an interactive interface does not exist.	High	Appgate SDP supports the use of system use notification messages or banners. This is available to both end-users, Appgate SDP administrators, and infrastruture teams (ssh). This can even be enanced by Appgate SDP through rich-text support in our client as well as continuous policy evaluation/ enforcement.
Technical	Access Control	AC-10	Concurrent Session Control	HIGH	P2	The information system limits the number of concurrent sessions for each system account to [Assignment: organization-defined number].	The organization may define the maximum number of concurrent sessions for an information system account globally, by account type, by account, or a combination. This control addresses concurrent sessions for a given information system account and does not address concurrent sessions by a single user via multiple system accounts	High	If that information is made available, Appgate SDP supports restricting sessions based on a maximum allowed number of concurrent sessionf for an information system

CLASS	FAMILY	NUMBER	TITLE	IMPACT	PRIORITY	DESCRIPTION	SUPPLEMENTAL-GUIDANCE	RELEVANCE TO APPGATE SDP	DISCUSSION
Technical	Access Control	AC-17	Remote Access	LOW_ MODERATE_ HIGH	P1	The organization: Documents allowed methods of remote access to the information system; Establishes usage restrictions and implementation guidance for each allowed remote access method; Monitors for unauthorized remote access to the information system; Authorizes remote access to the information system prior to connection; and Enforces requirements for remote connections to the information system.	This control requires explicit authorization prior to allowing remote access to an information system without specifying a specific format for that authorization. For example, while the organization may deem it appropriate to use a system interconnection agreement to authorize a given remote access, such agreements are not required by this control. Remote access is any access to an organizational information system by a user (or process acting on behalf of a user) communicating through an external network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless (see AC-18 for wireless access). A virtual private network when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the organization establishes a network connection between organization-controlled endpoints in a manner that does not require the organization to depend on external networks to protect the confidentiality or integrity of information transmitted across the network). Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. Enforcing access restrictions associated with remote connections is accomplished by control AC-3. Related controls: AC-3, AC-18, AC-20, IA-2, IA-3, IA-8, MA-4.	High	Appgate SDP not only monitors and logs unauthorized access attempts, but fundamentally discourages/impedes such attempts through the use of Single Packet Authorization.
Technical	Access Control	AC-19	Access Control for Mobile Devices	LOW_ MODERATE_ HIGH	P1	The organization: Establishes usage restrictions and implementation guidance for organization-controlled mobile devices; Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems; Monitors for unauthorized connections of mobile devices to organizational information systems; Enforces requirements for the connection of mobile devices to organizational information systems; Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction; Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and Applies [Assignment: organization-defined inspection and preventative measures] to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.	Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Organization-controlled mobile devices include those devices for which the organization has the authority to specify and the ability to enforce specific security requirements. Usage restrictions and implementation guidance related to mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Examples of information system functionality that provide the capability for automatic execution of code are AutoRun and AutoPlay. Organizational policies and procedures for mobile devices used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific measures to the device after travel is completed. Specially configured mobile devices include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family. Related controls: MP-4, MP-5.	High	In addition to AC-17, where Appgate SDP not only monitors and logs unauthorized access attempts, but fundamentally discourages/impedes such attempts through the use of Single Packet Authorization. Appgate SDP supports mobile OS, which when coupled with our extensible policy engine, allows for a non-exhaustive set of policy permutations and combinations to be implemented. Even for mobile.

CLASS	FAMILY	NUMBER	TITLE	IMPACT	PRIORITY	DESCRIPTION	SUPPLEMENTAL-GUIDANCE	RELEVANCE TO APPGATE SDP	DISCUSSION
Technical	Access Control	AC-20	Use of External Information Systems	LOW_ MODERATE_ HIGH	P1	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: Access the information system from the external information systems; and Process, store, and/or transmit organization-controlled information using the external information systems.	External information systems are information systems or components of information systems that are outside of the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to: (i) personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of the organization. For some external systems, in particular those systems operated by other federal agencies, including organizations subordinate to those agencies, the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. In effect, the information systems of these organizations would not be considered external. These situations typically occur when, for example, there is some pre-existing sharing or trust agreement (either implicit or explicit) established between federal agencies and/or organizations subordinate to those agencies, or such trust agreements are specified by applicable laws, Executive Orders, directives, or policies. Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system and over which the organization has the authority to impose rules of behavior with regard to system access. The restrictions that an organization imposes on authorized individuals need not be uniform, as those restrictions are likely to vary depending upon the trust relationships between organizations. Thus, an organization might impose more stringent security restrictions on a contractor than on a state, local, or tribal government. This control does not apply to the use of external information systems to access public interfaces to organizational information systems and information (e.g., individuals accessing federal information through www.usa.gov). The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the organizational information system from the external information system; and (ii) the maximum security categorization of information that can be processed, stored, and transmitted on the external information system. This control defines access authorizations enforced by AC-3, rules of behavior requirements enforced by PL-4, and session establishment rules enforced by AC-17. Related controls: AC-3, AC-17, PL-4.	High	While the entirety of this control is typically not met with Appgate SDP, such terms and conditions can either be applied if said external system allows for "conditional access" or by enforcing mechanisms and policies to assist other tools in doing so. For example, applying and enforcing a Proxy Auth Configuration (PAC) file.
Technical	Audit and Accountability	AU-02	Auditable Events	LOW_ MODERATE_ HIGH	P1	The organization: Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [Assignment: organization-defined list of auditable events]; Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event].	The purpose of this control is for the organization to identify events which need to be auditable as significant and relevant to the security of the information system; giving an overall system requirement in order to meet ongoing and specific audit needs. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are to be audited at a given point in time. For example, the organization may determine that the information system must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the extreme burden on system performance. In addition, audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Related control: AU-3.	High	Appgate SDP suppots high fidelity logging of any and all network behavior through our systems. This supports the Audit and Accountability goals.

Appgate SDP: Mapping to NIST SP 800-53

CLASS	FAMILY	NUMBER	TITLE	IMPACT	PRIORITY	DESCRIPTION	SUPPLEMENTAL-GUIDANCE	RELEVANCE TO APPGATE SDP	DISCUSSION
Technical	Audit and Accountability	AU-03	Content of Audit Records	LOW_ MODERATE_ HIGH	P1	The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.	Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Related controls: AU-2, AU-8.	High	The logging within Appgate SDP is quite verbose, and can even be configured to log NAT mappings if there is a desire for NAT'd session ID.
Technical	Audit and Accountability	AU-08	Time Stamps	LOW_ MODERATE_ HIGH	P1	The information system uses internal system clocks to generate time stamps for audit records.	Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts).	High	Appgate SDP provides a mechanism to accumulate user actions.
Technical	Access Control	AU-14	Session Audit	NONE	P0	The information system provides the capability to: Capture/record and log all content related to a user session; and Remotely view/hear all content related to an established user session in real time.	Session auditing activities are developed, integrated, and used in consultation with legal counsel in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.	High	Appgate SDP provides and implements a capability to provide session auditing.
Technical	Identification and Authentication	IA-02	Identification and Authentication (Organizational Users)	LOW_ MODERATE_ HIGH	P1	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations). Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in AC-14. Unique identification of individuals in group accounts (e.g., shared privilege accounts) may need to be considered for detailed accountability of activity. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. Access to organizational information systems is defined as either local or network. Local access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network. Network access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection. Remote access is a type of network access which involves communication through an external network (e.g., the Internet). Internal networks include local area networks, wide area networks, and virtual private networks that are under the control of the organization. For a virtual private network (VPN), the VPN is considered an internal network if the organization establishes the VPN connection between organization-controlled endpoints in a manner that does not require the organization to depend on any external networks across which the VPN transits to protect the confidentiality and integrity of information transmitted. Identification and authentication requirements for information system access by other than organizational users are described in IA-8. The identification and authentication requirements in this control are satisfied by complying with Homeland Security Presidential Directive 12 consistent with organization-specific implementation plans provided to OMB. In addition to identifying and authenticating users at the information-system level (i.e., at logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Related controls: AC-14, AC-17, AC-18, IA-4, IA-5.	High	Appgate SDP uniquely identify and authenticates organizational users on a device + account + identiy provider level. At login they receive a a certificate that is then used for mutual TLS amongst the system. This is a system wide, hard coded behavior, and has been a core part of the product since the beginning.
Technical	Identification and Authentication	IA-03	Device Identification and Authentication	MODERATE_ HIGH	P1	The information system uniquely identifies and authenticates [Assignment: organization-defined list of specific and/or types of devices] before establishing a connection.	The devices requiring unique identification and authentication may be defined by type, by specific device, or by a combination of type and device as deemed appropriate by the organization. The information system typically uses either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for identification or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the security categorization of the information system.	High	Appgate SDP uniquely identify and authenticates organizational users on a device + account + identiy provider level, prior to any session establishment.

CLASS	FAMILY	NUMBER	TITLE	IMPACT	PRIORITY	DESCRIPTION	SUPPLEMENTAL-GUIDANCE	RELEVANCE TO APPGATE SDP	DISCUSSION
Technical	Identification and Authentication	IA-04	Identifier Management	LOW_ MODERATE_ HIGH	P1	The organization manages information system identifiers for users and devices by: Receiving authorization from a designated organizational official to assign a user or device identifier; Selecting an identifier that uniquely identifies an individual or device; Assigning the user identifier to the intended party or the device identifier to the intended device; Preventing reuse of user or device identifiers for [Assignment: organization-defined time period]; and Disabling the user identifier after [Assignment: organization-defined time period of inactivity].	Common device identifiers include media access control (MAC) or Internet protocol (IP) addresses, or device-unique token identifiers. Management of user identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). It is commonly the case that a user identifier is the name of an information system account associated with an individual. In such instances, identifier management is largely addressed by the account management activities of AC-2. IA-4 also covers user identifiers not necessarily associated with an information system account (e.g., the identifier used in a physical security control database accessed by a badge reader system for access to the information system). Related control: AC-2, IA-2.	High	Appgate SDP can suport the ability to integrate with workflow provisioning tools to enable designated organizational officers to authorize users/devices.
Technical	Identification and Authentication	IA-05	Authenticator Management	LOW_ MODERATE_ HIGH	P1	The organization manages information system authenticators for users and devices by: Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator; Establishing initial authenticator content for authenticators defined by the organization; Ensuring that authenticators have sufficient strength of mechanism for their intended use; Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; Changing default content of authenticators upon information system installation; Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type]; Protecting authenticator content from unauthorized disclosure and modification; and Requiring users to take, and having devices implement, specific measures to safeguard authenticators.	User authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). Many information system components are shipped with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, present a significant security risk, and therefore, are changed upon installation. The requirement to protect user authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of users and by controls AC-3, AC-6, and SC-28 for authenticators stored within the information system (e.g., passwords stored in a hashed or encrypted format, files containing encrypted or hashed passwords accessible only with super user privileges). The information system supports user authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one time tokens, and number of allowed rejections during verification stage of biometric authentication. Measures to safeguard user authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, IA-2, PL-4, PS-6.	High	Appgate SDP supports this by means of making outbound API calls to the organizations information system.
Technical	Identification and Authentication	IA-06	Authenticator Feedback	LOW_ MODERATE_ HIGH	P1	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password, is an example of obscuring feedback of authentication information.	High	Appgate SDP adequately obsfucates authentication information when implemented and also provides native integrations with federated identity providers, thus incorporating the additional security benefits they provide as well.
Technical	Identification and Authentication	IA-07	Cryptographic Module Authentication	LOW_ MODERATE_ HIGH	P1	The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	None.	High	Appgate SDP is FIPS 140-2 compliant, and has achieved common criteria certification numerous times. Additionally, Appgate SDP implements mutual TLS and strong PKI standards across the ecosystem.

Appgate SDP: Mapping to NIST SP 800-53

CLASS	FAMILY	NUMBER	TITLE	IMPACT	PRIORITY	DESCRIPTION	SUPPLEMENTAL-GUIDANCE	RELEVANCE TO APPGATE SDP	DISCUSSION
Technical	Identification and Authentication	IA-08	Identification and Authentication (Non-organizational Users)	LOW_ MODERATE_ HIGH	P1	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	Non-organizational users include all information system users other than organizational users explicitly covered by IA-2. Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance with AC-14. In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Accordingly, a risk assessment is used in determining the authentication needs of the organization. Scalability, practicality, and security are simultaneously considered in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk to organizational operations, organizational assets, individuals, other organizations, and the Nation. Identification and authentication requirements for information system access by organizational users are described in IA-2. Related controls: AC-14, AC-17, AC-18, MA-4.	High	Authentication and authorization within Appgate SDP can incorporate both end users and non person entities such as processes acting on behalf of non-organizational users. The Appgate SDP workflow identifies each and every session uniquely and provides means to audit permissions, access, and prior behavior.
Operational	Maintenance	MA-05	Maintenance Personnel	LOW_ MODERATE_ HIGH	P1	The organization: Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.	Individuals not previously identified in the information system, such as vendor personnel and consultants, may legitimately require privileged access to the system, for example, when required to conduct maintenance or diagnostic activities with little or no notice. Based on a prior assessment of risk, the organization may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for a very limited time period. Related controls: IA-8, MA-5.	High	While this falls outside of something that Appgate SDP provides, it does allow for the implementation of almost all conceivable methods for establishing personnel authorization for internal maintenance through the use of our data-centric, context aware, and continuously evaluated policies.
Management	Planning	PL-04	Rules of Behavior	LOW_ MODERATE_ HIGH	P1	The organization: Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.	The organization considers different sets of rules based on user roles and responsibilities, for example, differentiating between the rules that apply to privileged users and rules that apply to general users. Electronic signatures are acceptable for use in acknowledging rules of behavior. Related control: PS-6.	High	Appgate SDP allows for individualized messages to all users, both admins and end users, that can describe their roles, responsibilities, and expected behavior with regard to information and information system usage. An end user action is required to confirm said message before allowing access to information systems.
Management	Program Management	PM-07	Enterprise Architecture	LOW_ MODERATE_ HIGH	P1	The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.	The enterprise architecture developed by the organization is aligned with the Federal Enterprise Architecture. The integration of information security requirements and associated security controls into the organizations enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organizations mission/business processes. This also embeds into the enterprise architecture, an integral security architecture consistent with organizational risk management and information security strategies. Security requirements and control integration are most effectively accomplished through the application of the Risk Management Framework and supporting security standards and guidelines. The Federal Segment Architecture Methodology provides guidance on integrating information security requirements and security controls into enterprise architectures. Related controls: PL-2, PM-11, RA-2.	High	The data driven nature of Appgate SDP's policies allow for the integration and/or consideration of information security and subsequent risks on a per user, per session, per entitlement basis.
Management	System and Services Acquisition	SA-10	Developer Configuration Management	MODERATE_ HIGH	P1	The organization requires that information system developers/integrators: Perform configuration management during information system design, development, implementation, and operation; Manage and control changes to the information system; Implement only organization-approved changes; Document approved changes to the information system; and Track security flaws and flaw resolution.	Related controls: CM-3, CM-4, CM-9.	High	Appgate SDP allows for role and entitiy specific administration privledges to facilitate the management and control of changes to itsself. All CRUD actions are audited and logged, even attempts.

Appgate SDP: Mapping to NIST SP 800-53

CLASS	FAMILY	NUMBER	TITLE	IMPACT	PRIORITY	DESCRIPTION	SUPPLEMENTAL-GUIDANCE	RELEVANCE TO APPGATE SDP	DISCUSSION
Management	System and Services Acquisition	SA-11	Developer Security Testing	MODERATE_ HIGH	P2	The organization requires that information system developers/ integrators, in consultation with associated security personnel (including security engineers): Create and implement a security test and evaluation plan; Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and Document the results of the security testing/ evaluation and flaw remediation processes.	Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security-relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security authorization process for the delivered information system. Related control: CA-2, SI-2.	High	Appgate SDP's data centric polices allow organizations to automatically realize the results of security tests and can even build remediation actions into policy to compensate for the unexpected/anticipated.
Management	System and Services Acquisition	SA-13	Trustworthiness	HIGH	P1	The organization requires that the information system meets [Assignment: organization-defined level of trustworthiness].	The intent of this control is to ensure that organizations recognize the importance of trustworthiness and making explicit trustworthiness decisions when designing, developing, and implementing organizational information systems. Trustworthiness is a characteristic or property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system. Trustworthy information systems are systems that are capable of being trusted to operate within defined levels of risk despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation. Two factors affecting the trustworthiness of an information system include: (i) security functionality (i.e., the security features or functions employed within the system); and (ii) security assurance (i.e., the grounds for confidence that the security functionality is effective in its application). Appropriate security functionality for the information system can be obtained by using the Risk Management Framework (Steps 1, 2, and 3) to select and implement the necessary management, operational, and technical security controls necessary to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. Appropriate security assurance can be obtained by: (i) the actions taken by developers and implementers of security controls with regard to the design, development, implementation, and operation of those controls; and (ii) the actions taken by assessors to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. Developers and implementers can increase the assurance in security controls by employing well-defined security policy models, structured, disciplined, and rigorous hardware and software development techniques, and sound system/security engineering principles. Assurance is also based on the assessment of evidence produced during the initiation, acquisition/development, implementation, and operations/maintenance phases of the system development life cycle. For example, developmental evidence may include the techniques and methods used to design and develop security functionality. Operational evidence may include flaw reporting and remediation, the results of security incident reporting, and the results of the ongoing monitoring of security controls. Independent assessments by qualified assessors may include analyses of the evidence as well as testing, inspections, and audits. Minimum assurance requirements are described in Appendix E. Explicit trustworthiness decisions highlight situations where achieving the information system resilience and security capability necessary to withstand cyber attacks from adversaries with certain threat capabilities may require adjusting the risk management strategy, the design of mission/business processes with regard to automation, the selection and implementation rigor of management and operational protections, or the selection of information technology components with higher levels of trustworthiness. Trustworthiness may be defined on a component-by-component, subsystem-by-subsystem, or function-by-function basis. It is noted, however, that typically functions, subsystems, and components are highly interrelated, making separation by trustworthiness perhaps problematic and at a minimum, something that likely requires careful attention in order to achieve practically useful results. Related controls: RA-2, SA-4, SA-8, SC-3.	High	Appgate SDP's allows for auditing of policies, conditions, and entitlements in a non-disruptive way that enables organizations to quantatively define and report on trustworthiness levels.
Technical	System and Communications Protection	SC-02	Application Partitioning	MODERATE_ HIGH	P1	The information system separates user functionality (including user interface services) from information system management functionality.	Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical and is accomplished by using different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate. An example of this type of separation is observed in web administrative interfaces that use separate authentication methods for users of any other information system resources. This may include isolating the administrative interface on a different domain and with additional access controls.	High	The end user data and Appgate SDP management functionality are distinct and seperate functions within Appgate SDP. There is never a need for end user traffic and management traffic to rely and transit the same network infrastructure when adequatly deployed/architected.

CLASS	FAMILY	NUMBER	TITLE	IMPACT	PRIORITY	DESCRIPTION	SUPPLEMENTAL-GUIDANCE	RELEVANCE TO APPGATE SDP	DISCUSSION
Technical	System and Communications Protection	SC-03	Security Function Isolation	HIGH	P1	The information system isolates security functions from nonsecurity functions.	The information system isolates security functions from nonsecurity functions by means of an isolation boundary (implemented via partitions and domains) that controls access to and protects the integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process. Related control: SA-13.	High	Appgate SDP clearly defines when and where security functions get evaluated and applied through the use of criteria and conditions and intuitively allows for that seperation to be uniform and consistant across an Apppgate collective.
Technical	System and Communications Protection	SC-04	Information In Shared Resources	MODERATE_ HIGH	P1	The information system prevents unauthorized and unintended information transfer via shared system resources.	The purpose of this control is to prevent information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. Control of information in shared resources is also referred to as object reuse. This control does not address: (i) information remanence which refers to residual representation of data that has been in some way nominally erased or removed; (ii) covert channels where shared resources are manipulated to achieve a violation of information flow restrictions; or (iii) components in the information system for which there is only a single user/role.	High	Within Appgate SDP, unauthorized information transfer is all but impossible due to a default-deny approach to policy authorization.Unintended information transfer via shared system resources can also be handled by Appgate SDP through the use of url filtersing and http verb filtering.
Technical	System and Communications Protection	SC-05	Denial of Service Protection	LOW_ MODERATE_ HIGH	P1	The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list].	A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organizations internal network from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may reduce the susceptibility to some denial of service attacks. Related control: SC-7.	High	The use of Single packet authorization (SPA), by its very nature precludes Appgate SDP from DDoS attacks and other common DoS attacks. SPA achieves this by not allowing it to become a target in the first place by effectively being undiscoverable to adversaries but also highly available to authorized users.
Technical	System and Communications Protection	SC-06	Resource Priority	NONE	P0	The information system prevents unauthorized and unintended information transfer via shared system resources.	The information system limits the use of resources by priority.	High	One example of Appgate SDP limiting the use of resources by priority, is how Appgate SDP is designed to be cloud scalable to take advantage of the automated provisioning and deprovisioning that most cloud service providers provide.
Technical	System and Communications Protection	SC-07	Boundary Protection	LOW_ MODERATE_ HIGH	P1	The information system: Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	Restricting external web traffic only to organizational web servers within managed interfaces and prohibiting external traffic that appears to be spoofing an internal address as the source are examples of restricting and prohibiting communications. Managed interfaces employing boundary protection devices include, for example, proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in an effective security architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). The organization considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third-party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-4, IR-4, SC-5.	High	Appgate SDP as a software defined perimiter, compliant with Cloud Security Alliance specifications, monitors and controls communications at all external boundaries. The distributed nature of Appgate SDP allows the traditional architectures that require internal boundaries and external connections to increase segmentation and thus control between networks by making the resources available as their own site within Appgate SDP. The multi-tunnel capabilities of the Appgate SDP client, enable that all authorized resources can be accessed, with the added benefit of reducing complexity and increasing security.
Technical	System and Communications Protection	SC-08	Transmission Integrity	MODERATE_ HIGH	P1	The information system protects the integrity of transmitted information.	This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-17, PE-4.	High	Appgate SDP implements mutual TLS which by and large provides the highest level of protections to the integrity and confidentiality of transmitted information.

CLASS	FAMILY	NUMBER	TITLE	IMPACT	PRIORITY	DESCRIPTION	SUPPLEMENTAL-GUIDANCE	RELEVANCE TO APPGATE SDP	DISCUSSION
Technical	System and Communications Protection	SC-09	Transmission Confidentiality	MODERATE_ HIGH	P1	The information system protects the confidentiality of transmitted information.	This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-17, PE-4.	High	Appgate SDP implements mutual TLS which by and large provides the highest level of protections to the integrity and confidentiality of transmitted information.
Technical	System and Communications Protection	SC-10	Network Disconnect	MODERATE_ HIGH	P2	The information system terminates the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.	This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating-system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. The time period of inactivity may, as the organization deems necessary, be a set of time periods by type of network access or for specific accesses.	High	Appgate SDP continuously evaluates sessions against (a) set(s) of conditions. The failure of which, results in the termination of any sessions that were allowed by any entitlements that utilized said condition.
Technical	System and Communications Protection	SC-11	Trusted Path	NONE	P0	The information system establishes a trusted communications path between the user and the following security functions of the system: [Assignment: organization-defined security functions to include at a minimum, information system authentication and reauthentication].	A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login).	High	The workflow that Appgate SDP implements for high-confidence connections can be configured to require trusted communications (i.e. LDAPS vs LDAP, HTTPS vs HTTP).
Technical	System and Communications Protection	SC-13	Use of Cryptography	LOW_ MODERATE_ HIGH	P1	The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	None.	High	Appgate SDP uses wolfcrypt crypto modules, implemenets tls 1.3, and it FIPS 140-2 compliant.
Technical	System and Communications Protection	SC-14	Public Access Protections	LOW_ MODERATE_ HIGH	P1	The information system protects the integrity and availability of publicly available information and applications.	The purpose of this control is to ensure that organizations explicitly address the protection needs for public information and applications with such protection likely being implemented as part of other security controls.	High	Appgate SDP can overlay on those those publically available information systems and applications to provide all of the same integrity that any other resource would enjoy. The "publically available" deployments can still be accessed in a similiar manner without an Appgate SDP client via an Appgate SDP Clientless Portal, but the actual application server/services would become enshrined in Appgate SDP policies and protections.
Technical	System and Communications Protection	SC-16	Transmission of Security Attributes	NONE	P0	The information system associates security attributes with information exchanged between information systems.	Security attributes may be explicitly or implicitly associated with the information contained within the information system. Related control: AC-16.	High	Appgate SDP's context awareness allows itself to participate in security attributes exchanges among and between other information systems. This also enables policy makers to integrate and use those security attributes directly, as an intuitive part of policy.

CLASS	FAMILY	NUMBER	TITLE	IMPACT	PRIORITY	DESCRIPTION	SUPPLEMENTAL-GUIDANCE	RELEVANCE TO APPGATE SDP	DISCUSSION
Technical	System and Communications Protection	SC-21	Secure Name / Address Resolution Service (Recursive Or Caching Resolver)	HIGH	P1	The information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.	A recursive resolving or caching domain name system (DNS) server is an example of an information system that provides name/address resolution service for local clients. Authoritative DNS servers are examples of authoritative sources. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data.	High	Appgate SDP provides numerous ways to manage and use DNS within an organization. One such example, is our DNS forwarder, which allows for dynamic routing of traffic to occur based on DNS resolution requests. Appgate SDP's resolver functionality extends well beyond DNS to include native integrations with all major CSP's and hypervisors to enable the use of metadata (tags/labels/security groups) as a means of defining resources. API calls are made directly to the relevant hosting solutions, which in turn gives Appgate SDP an authoritative response as to what resources are currently available and continuously updates this information which subsequently get reflected in real-time to the client.
Technical	System and Communications Protection	SC-22	Architecture and Provisioning for Name / Address Resolution Service	MODERATE_ HIGH	P1	The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.	A domain name system (DNS) server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. Additionally, the two servers are commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility). With regard to role separation, DNS servers with an internal role, only process name/address resolution requests from within the organization (i.e., internal clients). DNS servers with an external role only process name/address resolution information requests from clients external to the organization (i.e., on the external networks including the Internet). The set of clients that can access an authoritative DNS server in a particular role is specified by the organization (e.g., by address ranges, explicit lists).	High	Appgate SDP provides administrators with the ability to define any number of nameservers to query with optional domain restrictions, so that fault-tolerance and role seperation parity is on par with those very nameservers.
Technical	System and Communications Protection	SC-23	Session Authenticity	MODERATE_ HIGH	P1	The information system provides mechanisms to protect the authenticity of communications sessions.	This control focuses on communications protection at the session, versus packet, level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted. For example, this control addresses man-in-the-middle attacks including session hijacking or insertion of false information into a session. This control is only implemented where deemed necessary by the organization (e.g., sessions in service-oriented architectures providing web-based services).	High	Appgate SDP SDP uses a multi-layer authorization model to provide real-time, context-aware control over all user access attempts. This includes Single Packet Authorization (SPA) which cloaks the Appgate SDP SDP system itself and only allows Clients to open a communications channel, as well as Multi-Factor Authentication (MFA) at sign-in which registers a user's device, turning it into a second (trusted) authentication factor.
Technical	System and Communications Protection	SC-24	Fail In Known State	HIGH	P1	The information system fails to a [Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures] preserving [Assignment: organization-defined system state information] in failure.	Failure in a known state can address safety or security in accordance with the mission/ business needs of the organization. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system. Failure in a known safe state helps prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving information system state information facilitates system restart and return to the operational mode of the organization with less disruption of mission/business processes.	High	Appgate SDP fails closed. The individual appliances that make up an Appgate SDP collective are booted as a read-only OS, such that a failure of one would only require a reboot. The read-only OS aspect ensures that unintended changes or unanticipated events are not persistant across reboots.
Technical	System and Communications Protection	SC-25	Thin Nodes	NONE	P0	The information system employs processing components that have minimal functionality and information storage.	The deployment of information system components with minimal functionality (e.g., diskless nodes and thin client technologies) reduces the need to secure every user endpoint, and may reduce the exposure of information, information systems, and services to a successful attack. Related control: SC-30.	High	An Appgate SDP collective only consists of Appgate SDP appliances and Appgate SDP clients. The applianes are all deployed from a common Appgate SDP image which is a highly modified and lean Ubuntu instance with only required systems and services.

CLASS	FAMILY	NUMBER	TITLE	IMPACT	PRIORITY	DESCRIPTION	SUPPLEMENTAL-GUIDANCE	RELEVANCE TO APPGATE SDP	DISCUSSION
Technical	System and Communications Protection	SC-27	Operating System-independent Applications	NONE	P0	The information system includes: [Assignment: organization-defined operating system-independent applications].	Operating system-independent applications are applications that can run on multiple operating systems. Such applications promote portability and reconstitution on different platform architectures, increasing the availability for critical functionality within an organization while information systems with a given operating system are under attack.	High	An Appgate SDP collective only consists of Appgate SDP appliances and Appgate SDP clients. Clients are published for all of the major Operating systems as well as phone OS's. Further, Appgate SDP also has a clientless portal option for those organizations that wish not to install anything on end user devices.
Technical	System and Communications Protection	SC-28	Protection of Information At Rest	MODERATE_ HIGH	P1	The information system protects the confidentiality and integrity of information at rest.	This control is intended to address the confidentiality and integrity of information at rest in nonmobile devices and covers user information and system information. Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system. Configurations and/or rule sets for firewalls, gateways, intrusion detection/prevention systems, and filtering routers and authenticator content are examples of system information likely requiring protection. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate.	High	Appgate SDP provides administrators with the ability to define any number of nameservers to query with optional domain restrictions, so that fault-tolerance and role seperation parity is on par with those very nameservers.
Technical	System and Communications Protection	SC-29	Heterogeneity	NONE	P0	The organization employs diverse information technologies in the implementation of the information system.	Increasing the diversity of information technologies within the information system reduces the impact of the exploitation of a specific technology. Organizations that select this control should consider that an increase in diversity may add complexity and management overhead, both of which have the potential to lead to mistakes and misconfigurations which could increase overall risk.	High	Appgate SDP's Zero Trust platform and built-in risk engine quickly and dynamically integrates third party technologies so enterprises can create cohesive, dynamic Zero Trust architectures. Additionally, the Zero Trust Platform acts as a nerve center so you can quickly build and easily maintain any number of Collectives to accelerate Zero Trust adoption
Technical	System and Communications Protection	SC-30	Virtualization Techniques	NONE	P0	The organization employs virtualization techniques to present information system components as other types of components, or components with differing configurations.	Virtualization techniques provide organizations with the ability to disguise information systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms.	High	An Appgate SDP appliance is only the operating system. This allows Appgate SDP to be virtualized, or deployed on bare metal.