Protecting the human point.

FORCEPOINT Supply Chain Solutions Mapping Guide

The Department of Commerce, National Institute of Standards and Technology (NIST), released a NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.

NIST 800-171 lists 109 controls across 14 different control families. The following represents the different categories and the three components involved in meeting the requirements they spell out.

The following document maps the specific controls to technology from Forcepoint and GigaCloud that accompanies with the proper configuration, policies and procedures can satisfy the NIST technology requirements.

The NIST SP 800 -171 Control Families

CONTROL FAMILY	POLICY	TECHNOLOGY	IT PRACTICES
Access Control	•	•	•
Awareness and Training	•		
Audit and Accountability	•	•	•
Configuration Management			
Identification and Authentication		•	•
Incident Response	•		
Maintenance	•	•	•
Media Protection	•	•	•
Personnel Security	•		•
Physical Protection	•	•	•
Risk Assessment	•	•	•
Security Assessment	•	•	•
Systems and Communication Protection	•	•	•
System and Information Integrity	•	•	•

800-171 SECURITY REQUIREMENT IDENTIFIER	NIST SP 800-171 SECURITY REQUIREMENT	ENDPOINT DLP	NGFW	GIGACLOUD	COMPLETE\PARTIAL	EXTERNAL REQUIREMENTS
3.1 Access Control						
3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Endpoint DLP can restrict access to certain functions that might result in the loss of CUI/CDI.	The NGFW User Authentication feature limits information systems access to users. User Authentication can maintain separation of internal networks that have different security levels when the confidentiality of the information that is accessed does not need to be strictly enforced. For example, user authentication can provide an extra access control measure for applications that already exchange information securely.	The certification and credentialing process in GigaCloud insures that only the authorized user can open a protected email or document.	Partial	Local access to the system will need to be completed by system owner.
3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Endpoint DLP can restrict access to certain functions that might result in the loss of CUI/CDI. User based policies are supported.	The NGFW SSH Proxy allows restriction of the types of traffic and the commands that can be used with SSH connections. For example, the SSH Proxy can be used to block port forwarding or to restrict the commands allowed in file transfers using the SSH protocol. The NGFW Proxies may be used to enforce encryption strength for the connections. In the Protocol Parameters, rules can be created to separately specify the key type and key length for each side of the connection. The Client Advanced Settings define settings for connections between the SSH Proxy and the client. The Server Advanced Settings define settings for connections between the SSH Proxy and the server. The NGFW HTTP Proxy allows you to enforce strict HTTP protocol standards, log URLs in requests, validate HTTP requests, and block some types of content in requests. For example, you can use NGFW Proxies to block actions in requests, such as HTTP POST. The NGFW TLS Inspection allows you to decrypt TLS traffic so that it can be inspected. After decrypting the traffic, normal HTTP inspection and optionally malware scanning (requires separate license) are applied. If the traffic is allowed to continue, it is re-encrypted before it is forwarded.	GigaCloud administrators have control the creation and distribution of policies that govern controlled access to protected information.	Partial	Local access to the system will need to be completed by system owner.
3.1.3	Control the flow of CUI in accordance with approved authorizations.	Endpoint DLP can implement policies that help control the flow of CUI in accordance with approved authorizations.	Once communications protocols and authorized users with access to transmit CUI data have been identified in the CUI Security Domain, the NGFW Access Control Policies can be written to allow access for permitted users.	Protected content is only accessible by identified and authorized personnel.	Complete	Implementation of document tagging needs to be in place

800-171 SECURITY REQUIREMENT IDENTIFIER	NIST SP 800-171 SECURITY REQUIREMENT	ENDPOINT DLP	NGFW	GIGACLOUD	COMPLETE\PARTIAL	EXTERNAL REQUIREMENTS
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Endpoint DLP can restrict access to certain functions that might result in the loss of CUI/CDI. User based policies are supported.	By separating administration for the CUI Security Domain from any existing firewall controls, fewer individuals will have access to change policy on the CUI NGFW.	Administrative capabilities for policy creation, distribution and enforcement can be separated and assigned to different individuals to prevent abuse of power.	Partial - These controls are internal to the individual solutions (DLP and NGFW) and do not have an effect on other enterprise applications.	This requirement will be addressed by enterprise security policy and procedure.
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Endpoint DLP can restrict access to certain functions that might result in the loss of CUI/CDI. User based policies are supported.	By separating administration for the CUI Security Domain from any existing firewall controls, fewer individuals will have access to change policy on the CUI NGFW.		Partial - These controls are internal to the individual solutions (DLP and NGFW) and do not have an effect on other enterprise applications.	This requirement will be addressed by enterprise security policy and procedure.
3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.	Endpoint DLP does not require the use of privileged accounts to access nonsecurity functions.	The NGFW Solution SMC Administration accounts can utilize an internal LDAP server to the NGFW Solution; or contact and external LDAP to aid segregation of non-privileges accounts from logging in to the NGFW Solution SMC with Administrator privileges.		Partial - These controls are internal to the individual solutions (DLP and NGFW) and do not have an effect on other enterprise applications.	This requirement will be addressed by enterprise security policy and procedure.
3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	Endpoint DLP can restrict access to certain functions that might result in the loss of CUI/CDI. User based policies are supported.	The NGFW Solution SMC has audit capabilities for tracking changes SMC Administrators execute.	Complete audit trail is maintained to track all administrative actions taken.	Partial - These controls are internal to the individual solutions (DLP and NGFW) and do not have an effect on other enterprise applications.	This requirement will be addressed by enterprise security policy and procedure.
3.1.8	Limit unsuccessful logon attempts.	Endpoint DLP administrative tools can enforce a limitation on failed logon attempts.	The NGFW Solution SMC can restrict Administrator failed logon attempts		Partial - This is an Active directory function and is enforced on the TRITON manager when configured to use Network Accounts.	

800-171 SECURITY REQUIREMENT IDENTIFIER	NIST SP 800-171 SECURITY REQUIREMENT	ENDPOINT DLP	NGFW	GIGACLOUD	COMPLETE\PARTIAL	EXTERNAL REQUIREMENTS
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	Endpoint DLP provides direct notification to users when possible CUI/CDI related DLP policies are being violated.	The NGFW Solution SMC can present Administrators with a logon banner.		Partial	Additional controls may be required at the OS level
3.1.11	Terminate (automatically) a user session after a defined condition.		The NGFW Solution can terminate a user session by idle timeout.		Partial	Additional controls may be required at the OS level
3.1.12	Monitor and control remote access sessions.		The NGFW Solution Client VPN feature allows remote access for authorized users, with control and monitoring capabilities.	Protections to email and documents can preclude offline access.	Complete	
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.		The NGFW Solution Client VPN feature uses cryptographic mechanisms to protect the confidentiality of remote access sessions.	All protected content is encrypted intransit and at rest and in use on mobile devices	Complete	
3.1.14	Route remote access via managed access control points.		The NGFW Solution Client VPN feature can terminate VPN connections on the firewall engine itself.		Complete	
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.		The NGFW Solution Client VPN feature can utilize the SSH, HTTP, and TLS proxies to limit privileges commands and remote access.		Complete	
3.1.16	Authorize wireless access prior to allowing such connections.		The NGFW Solution Engine has wireless capabilities supporting WPA Enterprise (802.1x) for authentication, which can be used to limit access.		Partial	Requires Network Access Control (NAC) or 802.1x infrastructure
3.1.17	Protect wireless access using authentication and encryption.		Certain hardware models of the NGFW Solution Engine have wireless capabilities supporting WPA Enterprise (802.1x) for authentication and encryption.	All protected content is encrypted intransit and at rest on mobile devices.	Partial	Requires Network Access Control (NAC) or 802.1x infrastructure and for the wireless infrastructure with access points to be configured correctly.

800-171 SECURITY REQUIREMENT IDENTIFIER	NIST SP 800-171 SECURITY REQUIREMENT	ENDPOINT DLP	NGFW	GIGACLOUD	COMPLETE\PARTIAL	EXTERNAL REQUIREMENTS
3.1.18	Control connection of mobile devices.		The NGFW Solution Client VPN capabilities can be used to allow authorized, controlled access of mobile devices to the CUI Security Domain.	Mobile device access can be authorized or denied.	Partial	Requires an MDM solution, such as Air Watch
3.1.20	Verify and control/limit connections to and use of external information systems.	DLP policy can be set to allow data transfer only to trusted domains.	The NGFW Solution Engine can verify and control/limit connections to and use of external information systems with Access Policy.	Mobile device access can be authorized or denied.	Complete	
3.1.21	Limit use of organizational portable storage devices on external information systems.	Endpoint DLP can implement controls on portable devices as well as on data being written to said devices.		Content remains protected no matter where it goes and requires communication with authentication and certificate server to gain access. This communication can be blocked or denied or revoked in response to specific conditions.	Complete	
3.1.22	Control information posted or processed on publicly accessible information systems.	Endpoint DLP policies can prevent sensitive information from being posted to remote HTTP/S based services including specific high risk web sites that may contain malicious code.	The NGFW Solution SSH, HTTP, and TLS proxies can control information posted TO publicly accessible information systems.	Protected content remains protected no matter where it is located.	Partial	This requirement will be addressed by enterprise security awareness education and training program.

800-171 SECURITY REQUIREMENT IDENTIFIER	NIST SP 800-171 SECURITY REQUIREMENT	ENDPOINT DLP	NGFW	GIGACLOUD	COMPLETE\PARTIAL	EXTERNAL REQUIREMENTS
3.2 Awareness & Training						
3.2.1	Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.	Endpoint DLP provides direct notification to users and managers when possible CUI/CDI related DLP policies are being violated. Triton Management Console provides insight into the analysis of high risk activities and can also be configured to provide email notifications of policy exceptions.		GigaCloud administrative console provides Alerts, Reports and Tracking data on all Protected content. Delegated administration is provided in order to maintain a separation of duties for the creation, distribution and management of security policies.	Partial	This requirement will be addressed by enterprise security awareness education and training program.
3.3 Audit & Accountability						
3.3.1	Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.	Triton Management Console provides insight into the analysis of high risk activities and can also be configured to provide email notifications of policy exceptions.	The NGFW Solution SMC holds systems audit records.	GigaCloud administrative console provides Alerts, Reports and Tracking data on all Protected content.	Complete	
3.3.2	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	Endpoint DLP policy exceptions can be traced back to individual users through event analysis.	The NGFW Solution SMC Administrator accounts have audit/log capabilities	GigaCloud administrative console provides Alerts, Reports and Tracking data on all Protected content.	Partial	Enterprise security policy and procedures requiring unique accounts, and safeguarding of credentials, is critical to accurate accountability.

800-171 SECURITY REQUIREMENT IDENTIFIER	NIST SP 800-171 SECURITY REQUIREMENT	ENDPOINT DLP	NGFW	GIGACLOUD	COMPLETE\PARTIAL	EXTERNAL REQUIREMENTS
3.3.5	Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	Triton Management Console provides insight into the analysis of high risk activities and can also be configured to provide email notifications of policy exceptions. These capabilities are automated.	NGFW is able to consume external log data for rudimentary correlation.		Complete	Mechanisms are available to provide rudimentary correlation and reporting. More complex environments may require additional technologies to provide more detailed reporting
3.3.9	Limit management of audit functionality to a subset of privileged users.	Triton Management Console implements access controls requiring the use of privileged user accounts to administer audit facilities.	The NGFW Solution SMC limits access to audit functions and records by Administrator roles/permissions.	All administrative roles can be assigned, revoked and their actions tracked.	Complete	
3.4 Configuration Management						
3.4.6	Employ the principle of least functionality by configuring the information system to provide only essential capabilities.	DLP solution will only perform DLP functions.	The NGFW Solution enables the principal of least functionality by offering the ability to configure the information system to provide essential capability.	Rights of access to protected content can be scoped by individuals or groups. This allows for the assigned of greater levels of access based on specific roles within the organization.	Partial	Relies on proper configuration of ALL information systems in the security domain to be properly configured based on enterprise security policy and procedures.
3.4.7	Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.	Endpoint DLP can restrict access to certain functions that might result in the loss of CUI/CDI.	The NGFW Solution can restrict ports, protocols, and services into and out of the CUI Security Domain		Complete	

800-171 SECURITY REQUIREMENT IDENTIFIER	NIST SP 800-171 SECURITY REQUIREMENT	ENDPOINT DLP	NGFW	GIGACLOUD	COMPLETE\PARTIAL	EXTERNAL REQUIREMENTS
3.4.8	Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny- all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	Endpoint DLP agent can monitor applications and only allow access of protected data by specifically authorized applications.	The NGFW Solution can restrict software from communicating in/out of the CUI Security domain	GigaCloud provides blacklist protection against the use of over 200 screen scraping and screen sharing applications to prevent the extraction of information from Protected content.	Complete	
3.5 Identification & Authentication						
3.5.1	Identify information system users, processes acting on behalf of users, or devices.	Endpoint DLP manager employs AD identifying and authenticating administrator login. Additionally, DLP policy is applied to end users based on AD credentials.	NGFW can help to address this control	The GigaCloud can comply with this requirement.	Partial	3rd Party Identification and authentication solution required
3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	Endpoint DLP manager employs AD identifying and authenticating administrator login. Additionally, DLP policy is applied to end users based on AD credentials.	NGFW can help to address this control	All users of GigaCloud are authenticated via PKI technology	Partial	3rd Party Identification and authentication solution required
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	Endpoint DLP servers support MFA for administrator login.	NGFW can help to address this control		Partial	Enterprise MFA solution required
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non- privileged accounts.	Endpoint DLP can help to address this control	NGFW can help to address this control		Partial	Systems policy and local technical controls will need to be in place for this control to be fully met.

800-171 SECURITY REQUIREMENT IDENTIFIER	NIST SP 800-171 SECURITY REQUIREMENT	ENDPOINT DLP	NGFW	GIGACLOUD	COMPLETE\PARTIAL	EXTERNAL REQUIREMENTS
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	Endpoint DLP can help to address this control	NGFW can help to address this control		Partial	Systems policy and local technical controls will need to be in place for this control to be fully met.
3.5.8	Prohibit password reuse for a specified number of generations.	Endpoint DLP can help to address this control	NGFW can help to address this control		Partial	Systems policy and local technical controls will need to be in place for this control to be fully met.
3.5.10	Store and transmit only encrypted representation of passwords.	Endpoint DLP can help to address this control	NGFW can help to address this control		Partial	Systems policy and local technical controls will need to be in place for this control to be fully met.
3.5.11	Obscure feedback of authentication information.	Endpoint DLP can help to address this control	NGFW can help to address this control		Partial- Enforcement outside of the Forcepoint management consoles is reliant on network policy.	Systems policy and local technical controls will need to be in place for this control to be fully met.
3.6 Incident Response						
3.7 Maintenance						
3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	Multifactor authentication can be implemented on the web based administrative interface for Endpoint DLP.	The NGFW Solution Windows Client VPN supports external smart cards.		Partial	Requires 3rd party tool

800-171 SECURITY REQUIREMENT IDENTIFIER	NIST SP 800-171 SECURITY REQUIREMENT	ENDPOINT DLP	NGFW	GIGACLOUD	COMPLETE\PARTIAL	EXTERNAL REQUIREMENTS
3.8 Media Protection						
3.8.2	Limit access to CUI on information system media to authorized users.	Endpoint DLP can protect the confidentiality of CUI/CDI by encrypting information that only authorized users are able to decrypt.		Protected content remains protected no matter where it is located.	Partial	
3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	Endpoint DLP policies can force CDI/CUI data to be encrypted when being written to digital media.		Protected content remains protected/ encrypted no matter where it is located.	Complete	
3.8.7	Control the use of removable media on information system components.	Endpoint DLP policies can enforce restrictions on the specific types of removable media devices to which CDI/CUI can be written to.	.		Complete	
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	Endpoint DLP policies can enforce restrictions on the specific types of removable media devices to which CDI/CUI can be written to.			Complete	

800-171 SECURITY REQUIREMENT IDENTIFIER	NIST SP 800-171 SECURITY REQUIREMENT	ENDPOINT DLP	NGFW	GIGACLOUD	COMPLETE\PARTIAL	EXTERNAL REQUIREMENTS
3.9 Personnel Security						
3.9.2	Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.	Endpoint DLP policies can be implemented based on user identity.		GigaCloud's integration with Active Directory allows for the revocation of access to Protected content based on change in security group membership or termination	Partial	Policies and procedures also need to be in place for recovering or revoking physical access to the system.
3.10 Physical Protection						
3.11 Risk Assessment						
3.12 Security Assessment						
3.13 System & Communications Protection						
3.13.1	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.		The NGFW Solution can monitor/control/protect at the external boundaries of the CUI Security Domain		Complete	
3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	Endpoint DLP policies can be applied to information transfer and work to prevent both unauthorized and unintended transfer.			Complete	
3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.		The NGFW Solution can have DMZ-type network for all publicly accessible system components.		Complete	

800-171 SECURITY REQUIREMENT IDENTIFIER	NIST SP 800-171 SECURITY REQUIREMENT	ENDPOINT DLP	NGFW	GIGACLOUD	COMPLETE\PARTIAL	EXTERNAL REQUIREMENTS
3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).		The NGFW Solution can deny network communication by default and allow network communication by exception		Complete	
3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.		The NGFW Solution Client VPN feature has a full tunnel (as opposed to split tunnel) option to send all traffic to external resources to the NGFW Solution for Access Policy enforcement.		Complete	
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	Endpoint DLP policies can force CDI/CUI data to be encrypted when being written to digital media and enforce restrictions on the types of removable devices that this data can be written to.	The NGFW Solution offers both site to site and Client VPN capabilities to obscure, via cryptographic mechanisms, unauthorized disclosure of CUI during transmission outside of the CUI Security Domain.	Protected content remains protected no matter where it is located.	Complete	
3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.		The NGFW Solution can terminate connections by idle timeout value.		Complete	
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.		NGFW Crypto module is FIPS validated.	The encryption scheme used in GigaCloud has been FIPS - validated	Complete	
3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.		The NGFW Solution can identify and control VoIP communications		Partial	Detailed controls and monitoring should be available within the VoIP manager

800-171 SECURITY REQUIREMENT IDENTIFIER	NIST SP 800-171 SECURITY REQUIREMENT	ENDPOINT DLP	NGFW	GIGACLOUD	COMPLETE\PARTIAL	EXTERNAL REQUIREMENTS
3.13.15	Protect the authenticity of communications sessions.		The NGFW Solution can comply with this requirement		Complete	
3.13.16	Protect the confidentiality of CUI at rest.			Protected content remains protected no matter where it is located.	Complete	
3.14 System & Information Integrity						
3.14.6	Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.		The NGFW Solution SMC has log analysis capabilities to analyze and assist in detection of potential attacks.		Complete	
3.14.7	Identify unauthorized use of the information system.		The audit capabilities in the NGFW Solution can assist in complying with this requirement for the NGFW information system.		Partial	

The mappings cover 53 of the 109 controls either completely or partially. All of the 109 controls need to be met to be compliant. Several of the controls listed as complete are dependent on a number of the remaining controls being implemented.

CONTACT
NIST800-171@forcepoint.com

[FP-DATASHEET-SUPPLYCHAIN SOLUTIONS MAPPING GUIDE_EN_HORIZONTAL] 100033.083017