REDSEAL

CIS TOP 20 CONTROLS

with RedSeal

THE FOUNDATION FOR RESILIENCE

CYBERSECURITY BEST PRACTICES

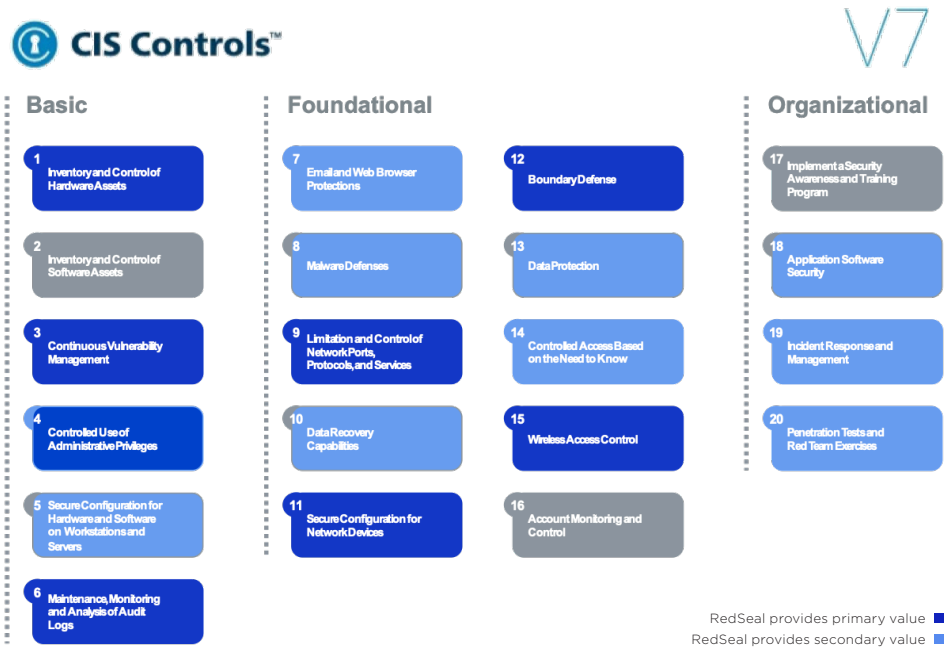
The Center for Internet Security's Critical Security Controls (CIS Controls) represent global industry best practices for cybersecurity. They are a prioritized and focused set of just 20 recommended cybersecurity actions. These 20 controls provide the highest pay off to protect against the most common attacks. They fall into three categories:

- **Basic** Six basic controls that every organization should address first. Implementation of solutions in these 6 areas forms the foundation of every cybersecurity program.
- **Foundational** Ten additional controls that build upon the foundational elements. Think of these as secondary initiatives once your organization has established a good foundation.
- **Organizational** Four additional controls that address organizational processes around your cybersecurity program.

While no one product can help with all 20 controls, RedSeal's platform can help you implement aspects of 17 of the 20. RedSeal's unique ability to model your network and understand all access paths is the foundation for a strong CIS Top 20-based security program.

To help you map RedSeal capabilities to each control group, we've identified the specific control areas where RedSeal provides primary value and those where it provides secondary value. RedSeal can support the implementation of other controls, as well.

What follows is a description of how RedSeal maps to each of the CIS Top 20 controls.



CIS TOP 20 CONTROLS WITH REDSEAL

CONTENTS

CIS TOP 20 CONTROLS WITH REDSEAL

THE CENTER FOR INTERNET SECURITY
Critical Security Controls Version 7

Basic CIS Control #1: Inventory and Control of Hardware Assets		
SUB-CONTROL	**CONTROL TITLE**	**REDSEAL CAPABILITY**
1.1	Utilize an Active Discovery Tool	RedSeal's assisted modeling capability actively discovers network devices and determines how they are connected. From there, RedSeal computes a network model, uncovering previously unknown subnets and devices.
1.2	Use a Passive Asset Discovery Tool	RedSeal can passively and automatically detect new network devices by signaling when anyone modifies existing network configurations. RedSeal also works with vulnerability scanners and endpoint data sources to put new hosts in the correct network context.
1.5	Maintain Asset Inventory Information	RedSeal can produce network device inventory reports that can be compared with existing inventory to validate these assets. Using RedSeal's active and passive discovery processes, you can maintain a complete list of these network devices. For endpoints (hosts), RedSeal can ingest host data from multiple endpoint sources and place them into the context of the deployed network. You can identify gaps where there is no end host data and maintain an inventory of endpoints.
1.6	Address Unauthorized Assets	Gap analysis will identify these unauthorized assets, so appropriate steps can be taken to remove or quarantine these assets -- or update inventory control systems.
1.7	Deploy Port Level Access Control	RedSeal's configuration checks will show you that 802.1X is enabled at the management plane and which interfaces (example, user interfaces) are permitted, and report on violations of this policy.

CIS TOP 20 CONTROLS WITH REDSEAL

Basic CIS Control #3: Continuous Vulnerability Management		
SUB-CONTROL	**CONTROL TITLE**	**REDSEAL CAPABILITY**
3.1	Run Automated Vulnerability Scanning Tools	RedSeal ingests vulnerability scan data from SCAP compliant and other scanners and adds network context information to the scanner priorities. In addition, RedSeal identifies areas of the network that aren't being scanned.
3.5	Deploy Automated Software Patch Management Tools	RedSeal can validate that automated patch management tools have the appropriate access to end host subnets to effectively execute patching operations.
3.6	Compare Back-to-back Vulnerability Scans	RedSeal can compare back-to-back scanning results to verify that vulnerabilities were addressed—by patching, implementing a compensating control or documenting an exception created by vulnerability suppression feature. RedSeal's known attack surface report shows changes in the known attack surface over time.
3.7	Utilize a Risk-rating Process	RedSeal allows you to segment assets by groups based on topology, asset type, or other criteria. It provides a number of vulnerability prioritization reports. RedSeal adds the context of location and accessibility to a specific system and vulnerability.

CIS TOP 20 CONTROLS WITH REDSEAL

Basic CIS Control #4: Controlled Use of Administrative Privileges		
SUB-CONTROL	**CONTROL TITLE**	**REDSEAL CAPABILITY**
4.1	Maintain Inventory of Administrative Accounts	For network devices, RedSeal can audit the number of local administrative accounts with admin rights. Custom checks can further ensure that devices are using remote access, authorization, and accounting (AAA) services (such as TACACs), and that configurations are aligned with your organization's standard.
4.2	Change Default Passwords	RedSeal automatically checks network device configurations for the presence of default passwords—and identifies them for administrators to change.
4.6	Use of Dedicated Machines for All Administrative Tasks	This requirement is most often met by dedicating a network segment to machines with administrative access. This zone has specialized access inside the network and no internet access. RedSeal's zones and policy feature can assess whether this has been done correctly.
4.8	Log and Alert on Changes to Administrative Group Membership	RedSeal has a configuration check to verify login security settings. This is routine practice for customers using a standard secure template.
4.9	Log and Alert on Unsuccessful Administrative Account Login	A RedSeal custom configuration check can validate that network devices are appropriately configured for this type of log event to be issued.

Basic CIS Control #5: Secure Configuration for Hardware and Software on Workstations and Servers		
SUB-CONTROL	**CONTROL TITLE**	**REDSEAL CAPABILITY**
5.4	Deploy System Configuration Management Tools	RedSeal can validate that management and monitoring tools have the appropriate access to all systems under management.
5.5	Implement Automated Configuration Monitoring Systems	See Sub-Control 5.4

CIS TOP 20 CONTROLS WITH REDSEAL

Basic CIS Control #6: Maintenance, Monitoring and Analysis of Audit Logs		
SUB-CONTROL	**CONTROL TITLE**	**REDSEAL CAPABILITY**
6.1	Utilize Three Synchronized Time Sources	RedSeal can validate that your network devices have specified three time sources in the configuration of each network device.
6.2	Activate audit logging	RedSeal can ensure that the audit log settings on each network device are consistent with your organization's policies.
6.3	Enable Detailed Logging	See Sub-Control 6.2
6.6	Deploy SIEM or Log Analytic tool	RedSeal can validate that SIEM and/or log analytic tools have the appropriate access to capture logging information from network devices and servers.

Foundational CIS Control #7: Email and Web Browser Protections		
SUB-CONTROL	**CONTROL TITLE**	**REDSEAL CAPABILITY**
7.4	Maintain and Enforce Network-Based URL Filters	RedSeal can monitor zone segmentation to ensure that web traffic traverses web proxies. It will highlight or send an alert if it detects any access policy violation.
7.9	Block Unnecessary File Types	Similar to Sub-Control 7.4, RedSeal can ensure that proxy and other devices are "in path" and no access exists that would defeat a monitoring device.

CIS TOP 20 CONTROLS WITH REDSEAL

Foundational CIS Control #8: Malware Defenses		
SUB-CONTROL	**CONTROL TITLE**	**REDSEAL CAPABILITY**
8.1	Utilize Centrally Managed Anti-Malware Software	RedSeal validates that anti-malware tools have the appropriate network access to communicate with end systems.
8.6	Centralize Anti-malware Logging	See Sub-control 8.1
8.7	Enable DNS Query Logging	RedSeal can ensure that network objects support a standard configuration profile, including settings for DNS.

Foundational CIS Control #9: Limitation and Control of Network Ports, Protocols, and Services		
SUB-CONTROL	**CONTROL TITLE**	**REDSEAL CAPABILITY**
9.2	Ensure Only Approved Ports, Protocols and Services Are Running	The RedSeal model identifies all access paths by port and protocol. It allows users to query any path based on source, destination, port and protocol. The RedSeal zones and policy feature allows users to create network segmentation and access policies to define, alert, and enforce any access violations of this policy.
9.3	Perform Regular Automated Port Scans	RedSeal can monitor for newly provisioned access to key assets. An increase in network access generates both a policy violation report and an email to a distribution list. This network access analysis is more accurate than an active network port scan, which can miss spots not visible from the scan's location or access opened to an unresponsive service.
9.5	Implement Application Firewalls	RedSeal can validate that network-based application firewalls (such as WAFs) are implemented in the correct network location to control access to servers. For organizations that have deployed next-generation firewalls with application support, RedSeal can: • Group internal systems by the services they are running and build a segmentation policy. Customers can include a rule to ensure that a firewall exists between one zone and another and that the appropriate application rules are deployed. • Ensure that the firewalls are provisioned with the correct options for application filtering (Layer 7).

CIS TOP 20 CONTROLS WITH REDSEAL

Foundational CIS Control #10: Data Recovery Capabilities		
SUB-CONTROL	**CONTROL TITLE**	**REDSEAL CAPABILITY**
10.1	Ensure Regular Automated Back Ups	When network devices support automated backup, a RedSeal custom configuration check can ensure compliance with the mandate.

Foundational CIS Control #11: Secure Configuration for Network Devices		
SUB-CONTROL	**CONTROL TITLE**	**REDSEAL CAPABILITY**
11.1	Maintain Standard Security Configurations for Network Devices	RedSeal conducts configuration checks on routers, firewalls and switches. These checks include pre-defined best practices, STIGs, CIS Benchmarks, and customized checks. The results of each check are fully documented.
11.3	Use Automated Tools to Verify Standard Device Configurations and Detect Changes	RedSeal's configuration checks allow you to define baseline configurations and automatically detect deviations. Deviations can be sent to the appropriate groups for remediation.
11.5	Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions	• RedSeal custom configuration checks (and STIG checks) can validate that the configuration for an AAA server, such as TACACs, is enabled. The two-factor configuration is on the AAA server. • RedSeal can also alert to devices using non-secure protocols such as TELNET or SNMPv1.
11.6	Use Dedicated Machines for All Network Administrative Tasks	RedSeal can validate that a management segment doesn't have excess access or access to the internet.
11.7	Manage Network Infrastructure Through a Dedicated Network	RedSeal can validate that the management network infrastructure across network connections is separated from business use of that network.

CIS TOP 20 CONTROLS WITH REDSEAL

Foundational CIS Control #12: Boundary Defense		
SUB-CONTROL	**CONTROL TITLE**	**REDSEAL CAPABILITY**
12.1	Maintain an Inventory of Network Boundaries	The RedSeal model maintains an up-to-date listing of ingress and egress points to the network.
12.2	Scan for Unauthorized Connections across Trusted Network Boundaries	With RedSeal's zones and policies feature, you can establish a segmentation policy that validates and identifies deviations across trusted network boundaries.
12.3	Deny Communications with Known Malicious IP Addresses	RedSeal's zones and policy feature can maintain a list of all blacklisted IP addresses and validate that they do not have access to the network. Since the list of bogon addresses changes over time, organizations can choose to separate this process into three steps: • First, making sure that perimeter devices enforce a filter for bogons (via a custom configuration check), • Second, making sure the bogon content is up to date (either via custom check, or manually), and third, making sure no exit pathways have been missed. • The third step is best done as an access query from internal subnets out to the edges. This is much more thorough than injecting sample bits of traffic into the live traffic, which can only cover a tiny fraction of the possible pathways.
12.4	Deny Communication over Unauthorized Ports	See Sub-Control 12.2
12.6	Deploy Network-based IDS Sensor	RedSeal can ensure that network devices are properly configured to support deployed sensors. This includes determining if commands for SPAN ports and/or NetFlow (or other flow sampling) are configured.
12.7	Deploy Network-Based Intrusion Prevention Systems	See Sub-Control 12.6
12.8	Deploy NetFlow Collection on Networking Boundary Devices	RedSeal can ensure that network devices are properly configured to support NetFlow or other flow sampling techniques.
12.9	Deploy Application Layer Filtering Proxy Server	RedSeal can monitor zone segmentation to ensure that application traffic traverses proxies. It will send an alert if it finds access that violates the policy.

CIS TOP 20 CONTROLS WITH REDSEAL

Foundational CIS Control #13: Data Protection		
SUB-CONTROL	**CONTROL TITLE**	**REDSEAL CAPABILITY**
13.4	Only Allow Access to Authorized Cloud Storage or Email Providers	• If the control is a network ACL with known addresses, RedSeal can do a tracked access query from internal networks to a list of specific addresses. Changes in the query results can trigger an event. • Additionally, if there is a configuration command on a network device (e.g. firewall) that implements a block list, RedSeal can determine if this control is accurately configured on the device.

CIS TOP 20 CONTROLS WITH REDSEAL

Foundational CIS Control #14: Controlled Access Based on the Need to Know		
SUB-CONTROL	**CONTROL TITLE**	**REDSEAL CAPABILITY**
14.1	Segment the Network Based on Sensitivity	• You can use RedSeal's zone segmentation to specify controls and verify that your network is enforcing the intended controls. • RedSeal identifies variations in the controls and paths that are in violation (devices, ACLs, routes that circumvent the rule) for remediation.
14.2	Enable Firewall Filtering Between VLANs	RedSeal custom configuration checks can verify that firewall filtering between VLANs is enabled and correctly configured.
14.6	Protect Information through Access Control Lists	RedSeal's policy function allows an organization to create a segmentation policy that monitors compliance with this control.

Foundational CIS Control #15: Wireless Access Control		
SUB-CONTROL	**CONTROL TITLE**	**REDSEAL CAPABILITY**
15.1	Maintain an Inventory of Authorized Wireless Access Points	RedSeal's modeling features allow an organization to maintain a list of deployed access points and where these access points are connected within the network.
15.2	Detect Wireless Access Points Connected to the Wired Network	RedSeal's assisted modeling function can discover and identify unauthorized access points.
15.7	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	RedSeal can verify the configuration of access points and determine if they: • Have AES or better encryption specified • Don't have unencrypted options provisioned
15.10	Create Separate Wireless Network for Personal and Untrusted Devices	RedSeal's network model can validate that virtual local networks for BYOD exist and the VLAN goes through the same border routing as corporate traffic.

CIS TOP 20 CONTROLS WITH REDSEAL

Organizational CIS Control #18: Application Software Security		
SUB-CONTROL	**CONTROL TITLE**	**REDSEAL CAPABILITY**
18.9	Separate Production and Non-Production Systems	With RedSeal, you can model your segmentation to validate that network security controls prohibit developers from accessing production systems.
18.10	Deploy Web Application Firewalls (WAFs)	RedSeal can validate that no path around WAFs exists.

Organizational CIS Control #19: Incident Response and Management		
SUB-CONTROL	**CONTROL TITLE**	**REDSEAL CAPABILITY**
19.1	Document Incident Response Procedures	• For the incident investigation phase, RedSeal can provide network context for IoCs and show you potential exposure impact to other systems. • For the containment option development phase, RedSeal can: - Identify where compensating controls can be configured in the network. - Identify the switch port where the IoC is connected, so you can remove a device from the network.

CIS TOP 20 CONTROLS WITH REDSEAL

Organizational CIS Control #20: Penetration Tests and Red Team Exercises		
SUB-CONTROL	**CONTROL TITLE**	**REDSEAL CAPABILITY**
20.2	Conduct Regular External and Internal Penetration Tests	• You can use RedSeal's network model to conduct virtual penetration testing from both external and internal sources. • RedSeal also identifies attack vectors that can be used to exploit enterprise systems.
20.5	Create Test Bed for Elements Not Typically Tested in Production	A secondary RedSeal server provides a non-production environment for this activity. This secondary environment can mimic the production environment so you can simulate changes to network devices.
20.6	Use Vulnerability Scanning and Penetration Testing Tools in Concert	• By combining RedSeal data with vulnerability data, RedSeal can help Red Teams focus their efforts on vulnerable assets that are accessible from an outside network. • RedSeal also helps direct Red Teams by identifying all access and vulnerabilities on all systems from any point inside the network.
20.7	Ensure Results from Penetration Test are Documented Using Open, Machine-Readable Standards	• RedSeal comes pre-configured with tracked queries that run and are logged with each analysis. You can create additional tracked queries to evaluate access over a given portion of the network. • RedSeal includes known and potential attack surface queries, along with prepackaged historical trending reports. These allow you to track how changes to network controls impact access from external networks to internal networks and hosts within the RedSeal model. An increase in attack surface doesn't immediately correspond to an increase in risk but is something that warrants investigation. • This information is not in a standard format, such as SCAP, but is exportable in standard formats (CSV, XML, etc.) to be incorporated into other systems.