REDSEAL

TECHNOLOGY
INTEGRATION GUIDE

INTRODUCTION

RedSeal's network modeling and risk scoring platform is the foundation for enabling hybrid data centers to be resilient to cyber events. The platform incorporates the data and configuration files of network devices to calculate a network model, enhance situational awareness, verify compliance, improve productivity, and accelerate incident investigation. RedSeal also has a line of Integration Apps that bring enhanced information into existing, familiar security applications.

REDSEAL SDN/CLOUD INTEGRATIONS

Amazon AWS
Cisco ACI 1.3(2i)
Microsoft Azure
VMware NSX up to 6.4.0

REDSEAL INTEGRATION APPS

ArcSight ESM 6.x
ForeScout CounterACT 7.1.1
Gigamon Giga VUE-FM 5.00.x
IBM QRadar Security Intelligence 7.2.8.x
Rapid7.x
Splunk Enterprise Security 4.5.x

NETWORK DEVICES AND INFRASTRUCTURE*

*Indicates Layer 2 support

Routers/Switches

MANUFACTURER	DEVICE NAME/OS	VERSIONS SUPPORTED
Alcatel-Lucent*	AOS	6.4.6
Alcatel-Lucent*	SR-OS	11.0.R4
Arista*	Arista EOS	4.7. to 4.11.4
Cisco*	IOS	11.0 to 15
Cisco*	IOS-XR	3.8 to 4.2
Cisco*	NX-OS	5.1, 6.x, 7.x
Cisco*	VPN-3000	4.x (EOL)
Cisco*	SG Series Switches	1.3.5.58

TECHNOLOGY INTEGRATION GUIDE

Dell Force10*	FTOS	8.3.3.4
Enterasys*	Layer 2 (SecureStack)	03.01.33
Enterasys	N and C Series	N: 07.21.03.0003, C: 06.42.12.0007
Ericsson (RedBack)	SmartEdge OS	SEOS-6.1.1.5p6
Extreme Networks*	ExtremeXOS	15.7
Fujitsu*	Fujitsu XG	E11L10, E15L10
HPE*	Comware (H3C)	5.20
HPE*	ProCurve	15.8
Huawei*	Virtual Routing Platform (VRP) 5	5.120
Juniper	JunOS	8.5 through 12x
Open Source	Linux Router	IP tables, routes, netstat, IP addresses

Load Balancers

MANUFACTURER	DEVICE NAME/OS	VERSIONS SUPPORTED
A10*	AX Series and Thunder Series	ACOS 2.7.1
Brocade*	IronWare OS, NOS	BigIron/FastIron 8.0 ServerIron XL 7.5 VDX Switch
Cisco	Content Services Switch (CSS)	sg0810602
Cisco*	ACE	A4 (2.1)
Citrix*	NetScaler	9.2
F5*	BIG-IP	10.2, 11, 11.3, 11.5, 11.6, 12.1
F5	Enterprise Manager	2.1.0, 2.2.0, 2.3.0
Radware*	Alteon	26.x, 28.x
Riverbed	SteelApp, Stingray	9.1, 10.3

Firewalls

MANUFACTURER	DEVICE NAME/OS	VERSIONS SUPPORTED
Check Point	Check Point File	R77.2, R77.1, R76, R75, R71, R70, R65
Check Point	Check Point OPSEC	R80, R77.2, R77.1, R76, R75, R71, R70, R65
Cisco*	PIX	6.3, 7 and 8
Cisco	ASA	8.3.1, 8.4, 9.0, 9.1, and 9.2
Cisco*	FWSM	3.x, 4.x
Fortinet*	Fortigate FortiOS	4.0, 5.x
Forcepoint	Sidewinder	7, 8.1.2, 8.2.0, 8.2.1, 8.3

TECHNOLOGY INTEGRATION GUIDE

Forcepoint	Stonesoft NGFW	5.7 5.8, 5.9, 6.1
Juniper*	ScreenOS	6.x
Juniper*	JunOS	8.5 through 12.x
Palo Alto Networks*	PAN-OS	4.x, 5.x, 6.x, 7.x, 8.x
SonicWALL	SonicOS	5.9
WatchGuard*	Fireware OS	11.10.2

Wireless Controllers

MANUFACTURER	DEVICE NAME/OS	VERSIONS SUPPORTED
Aruba*	ArubaOS	6.1.3
Cisco	Aironet IOS	11.0 - 15
Cisco	Wireless Controller	7.4

Configuration Managers**

MANUFACTURER	DEVICE NAME/OS	VERSIONS SUPPORTED
BMC Network Automation	BladeLogic	8.2.0, 8.9.0
Cisco	Prime Infrastructure	3.0, 3.1
Cisco	Security Manager	4.3.0
EMC Ionix	Voyence	4.1
F5	Enterprise Manager	2.1.0, 2.2.0, 2.3.0
HP Network Automation	Opsware	7.6, 9.0, 9.1, 10.10, 10.20
Infoblox	NetMRI	6.4.1, 6.6.3.8, 6.9, 7.1
Juniper	NetScreen Security Manager (NSM)	2010.2
Juniper	Junos Space	15.1R1.11, 15.2R2.4
SolarWinds	Orion NCM	6.0, 7.2, 7.3, 7.4
Tripwire	Tripewire Enterprise	8.0, 8.1, 8.2

** Specific device support varies with each configuration management vendor. Please refer to RedSeal's Data Import Plugins Guide available from the RedSeal Support Portal for additional considerations on integration with configuration management systems. RedSeal also supports importing device configurations that have been saved to a file. Refer to documentation from specific device vendors for additional information on using this methodology.

TECHNOLOGY INTEGRATION GUIDE

CYBERSECURITY APPLICATIONS

Vulnerability Managers

MANUFACTURER	DEVICE NAME/OS	VERSIONS SUPPORTED
Alert Logic (Critical Watch)	Fusion VM	4-2015.7.0.22
Beyond Trust	Retina CS	3.7.9, 3.8, 5.16
BeyondTrust (eEye)	Retina Network Security Scanner	3.8 & 5.16
Digital Defense, Inc.	Frontline	5.2.0.13
McAfee	Vulnerability Manager	7.0.1 & 7.5
MaxPatrol	MaxPatrol	8
Open Source	nMap	6.25
Outpost24	Outscan, HIAB	Scanning engine: 3.2.7, XML App: 4.1.133.14
Qualys	QualysGuard/Qualys Report	6.15, 7.6, 8.11
Rapid 7	InsightVM/Nexpose	4.12, 5.12, 6.4
Symantec	Vulnerability Manager (EOL)	10.0.5 (EOL)
Tenable	Nessus	4.2, 4.4, 5.0, 6.11
Tenable	Security Center	4.6.2.1, 4.8.1, 5.5
Tripwire (nCircle)	IP360	6.8.9(v1), 6.9(v2), 7.3

Security Management***

MANUFACTURER	DEVICE NAME/OS	VERSIONS SUPPORTED
ForeScout	CounterACT	7.1.1
McAfee	ePO	4.5, 5.1

Governance/Risk/Compliance***

MANUFACTURER	DEVICE NAME/OS	VERSIONS SUPPORTED
RSA	Archer	5.3
Symantec	CCS	Suite 11

Security Information and Event Management (SIEM)***

MANUFACTURER	DEVICE NAME/OS	VERSIONS SUPPORTED
HPE	ArcSight	CEF
IBM	Qradar	LEEF
McAfee	ESM (Nitro)	N/A
Splunk	Enterprise Security	N/A

*** RedSeal has a robust REST API, as well as a standard syslog event feed that can supply RedSeal intelligence to a wide range of third party solutions. Please request RedSeal integration and testing from your solution providers.

REDSEAL

940 Stewart Drive, Sunnyvale, CA 94085

888 845 8169 | redseal.net