TAG CYBER

Using RedSeal for Healthcare Security and Compliance

An Independent Assessment

A recent study by independent industry analysts at TAG Cyber concluded that the network modeling inherent in the RedSeal platform is well-suited to meet the needs of the modern healthcare organization for cyber security—specifically, cyber visibility, compliance and risk management.

Prepared by
Edward Amoroso, Katherine Teitler, and Stan Quintana, TAG Cyber
www.tag-cyber.com

March 1, 2020

COMMISSIONED BY
REDSEAL

Introduction

TAG Cyber[1] was recently engaged to independently assess the degree to which the RedSeal[2] platform supports modern healthcare security and compliance objectives. The two-month assessment, which was held in early 2020, focused on RedSeal's cyber risk modeling toward enhanced digital resilience. TAG Cyber analysts reviewed the platform, examined RedSeal compliance support, interviewed practitioners, and performed a criteria assessment.

The TAG Cyber *Healthcare Cyber Security Framework* (HCSF)[3] served as the criteria basis for the overall assessment. Results of previous security compliance framework mappings by the RedSeal team also provided insights to the overall assessment[4]. Such mappings helped to highlight the dual objectives—both *security* and —addressed by RedSeal for the typical modern healthcare organization.

Interviews held by TAG Cyber with healthcare industry practitioners provided valuable context into how cyber risk modeling platforms can be best applied to meet the cyber security and compliance needs of the healthcare industry. The discussions also offered validation of the compliance assessments, and also helped complement the assessment conclusions drawn from the TAG Cyber HCSF review of the RedSeal platform.

The primary management conclusions drawn from this independent assessment by TAG Cyber involved the following three main findings related to use of the RedSeal platform in the healthcare industry:

- Network Complexity—RedSeal addresses network complexity by increasing visibility and understanding of the growing number of different medical devices and systems that complicate modern healthcare networks.
- Security Controls—RedSeal strongly supports the identification, prioritization, and implementation of the optimal, broad cyber security controls to be applied across a healthcare organization's network.
- Compliance Risk—RedSeal enables enterprise teams to address their growing liability, risk, and compliance needs through the use of cyber mappings, summary reports, and data visualization.

The healthcare participants assumed here include the following types of organizations: (1) Healthcare facilities such as hospitals, where the device profile of the network is dynamic and changing, (2) Pharmaceutical and medical device company networks, where a mix of research, manufacturing, and business functions creates a uniquely complex environment to secure, and (3) Retail pharmaceutical networks which include many business & supply chain complexities.[5]

[1]Founded in 2016 by Dr. Edward Amoroso, TAG Cyber is a New York-based research and analyst firm that focuses on closing the trust gap between enterprise practitioners and commercial cyber security vendors.

[2]San Jose-based RedSeal uses cyber risk modeling to help organizations achieve compliance and quantify and improve digital resilience using input from network elements such as switches, routers, firewalls, and load balancers.

[3]The new TAG Cyber Healthcare Cyber Security Framework (HCSF) is available for free download and use by anyone at https://www.tag-cyber.com/.

[4]Results of RedSeal compliance mappings for NIST 800-53 rev 4, CIS, COBIT, HIPAA, HITRUST, ISO27001, and PCI-DSS are available from RedSeal upon request. The mappings produced favorable results for healthcare organizations who use these frameworks as the basis for developing a control management process.

[5]Standard definitions of what constitutes a healthcare network are not easily identified, but perhaps the unifying aspect of the types of healthcare organizations included in the review is the life-critical aspect of any risks that might emerge from cyber security attacks or incidents.

How RedSeal Works

The RedSeal platform was designed to support cyber risk and compliance objectives by enabling enterprise teams to optimize the digital resilience of their network against cyber-related events such as network interruptions. RedSeal works by producing customized models of enterprise networks, which can include traditional perimeters, hybrid cloud architectures, or any other arrangement of public and private cloud infrastructure.

The primary input for a network model comes from configuration files RedSeal ingests from switches, routers, firewalls and load balancers. RedSeal integrates with public cloud and private cloud managers to include all network environments in the model. RedSeal cyber risk modeling also imports host and vulnerability data from vulnerability scanners and other sources. This is done without agents, span ports or taps and without being in-line with production traffic.

The RedSeal platform includes direct support for many functional security and compliance objectives that are increasingly important to the healthcare industry. These include network device configuration, accurate network infrastructure mapping, finding hidden areas of the network, visualizing the network and its devices, managing patches to the network, verifying network policies and rules, and ensuring continuous change controls (see Figure 1).

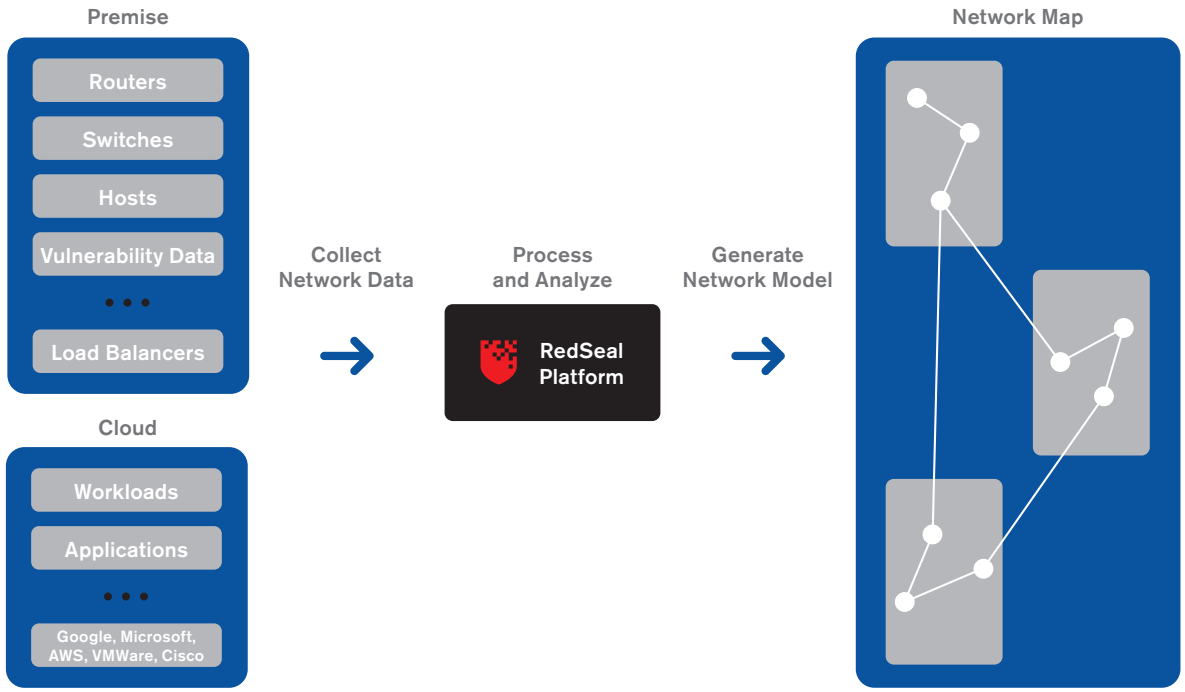

FIGURE 1. REDSEAL PLATFORM OVERVIEW

Ultimately, RedSeal calculates a Digital Resilience Score, which is a quantitative metric that supports comparison, benchmarking, and contractual requirements for an organization's network, or that of a third-party. The score, along with the cyber risk model, can also provide for validation of security posture, and can help an enterprise security team properly prioritize potential upgrades, changes, or mitigations to its network.

RedSeal Compliance Capabilities

The RedSeal platform, with its focus on network modeling and digital resilience, is uniquely suited to support the compliance needs of its customers. Specific compliance-oriented functions that help address the intense assessment scrutiny modern healthcare organizations experience include the following:

- Continuous Validation of Inventory—The on-going and continuous nature of the inventory validation support from RedSeal is especially valuable for compliance programs in healthcare. Inventory is a nagging issue in hospital facilities, for example, where new devices might be added and removed from the network. RedSeal network validation covers compliance needs in such cases.
- Continuous Validation of Secure Configurations—This function is central to how the RedSeal platform operates, since it ingests configuration information as the basis for developing a network model. This provides a suitable compliance basis for determining the security-related aspects of such configuration information from routers, switches, hosts, and other network-resident elements.
- Definition and Validation of Segmentation Policies—Healthcare networks increasingly require segmentation, either physically through network administration or logically through micro-segmentation software controls. It is well-known that many existing healthcare networks are considered flat in their design, which increases risk by making key assets visible to attackers and malware on the network.
- Quantitative Measurement of Enterprise Risk—The calculation of a digital resilience score serves as a valuable basis for quantitative benchmarking of a healthcare team's network security posture. It is possible that the compliance program might even be organized to use this value as the basis for measuring progress. (Obviously, this would need to be established with the compliance authority.)

These platform support features for compliance should be attractive to healthcare network security teams—especially ones who must submit to multiple, external reviews to maintain compliance with relevant framework controls.

Healthcare Expert Interviews

The TAG Cyber team identified and interviewed several healthcare industry practitioners to directly gauge their level of enthusiasm for the use of cyber risk modeling toward improved digital resilience and compliance. The practitioners interviewed included experienced experts from medical centers, hospitals, retail pharmacies, and medical device companies. Each was interviewed either face-to-face or using email and video conferencing.[6]

The objective in the interview process was to address three main issues: First, we wanted to understand if the healthcare expert and their organization currently use network models as the basis for making cyber security decisions. Second, we wanted to determine if they viewed such method as having merit, regardless of whether it was being done now. Third, we wanted to gauge their level of interest for using this method in the future.

[6]The practitioners and experts interviewed during the early part of 2020 for this security research agreed to provide information in a non-attributable manner for the RedSeal team. These experts are all employed in the healthcare sector and expressed concerns that any attribution might bring legal or operational risk to the organization. TAG Cyber thus agreed to maintain confidentiality of the interview discussions and to ensure anonymity of the expert and their healthcare organization.

An informal scale was used to obtain information from the experts on these issues. The results of a half-dozen interviews resulted in reasonable consensus among the experts: First, we found that 100% reported they were not currently using an automated platform for building network models as the basis for their current cyber security decision-making. This reinforces how novel the RedSeal approach is for network security.

Explicit Network Modeling Being Used Today?	**100% NOT CURRENTLY**
Explicit Network Modeling Show Merit for Healtcare?	**100% AGREE MERIT**
Interest in Network Modeling for Healthcare?	**100% INTERESTED**

Interviews were held by phone or email in February 2020 with six healthcare experts from various aspects of the sector. All requested non-attribution in their responses and involvement.

FIGURE 2. SUMMARY OF INTERVIEW RESULTS

Perhaps the most consequential result, however, was that 100% of those interviewed expressed agreement and enthusiasm that network modeling as exemplified by the RedSeal approach was both attractive and sensible. "This use of network modeling in the context of healthcare network security makes perfect sense," said one executive at a medical device company. "The approach matches up well with the needs of a healthcare organization."

100% of those interviewed expressed agreement and enthusiasm that network modeling as exemplified by the RedSeal approach was both attractive and sensible.

Another verbatim from a pharmaceutical executive was this: "Improving understanding of the assets in a healthcare network and how they are connected should be a high priority for cybersecurity teams, if only because healthcare networks are now so complex." This sentiment that network modeling is attractive to address the complexity of healthcare networks came up frequently in discussion with the experts.

Reviewing Platforms for Healthcare Security

Given the consequences of security breaches to healthcare systems, the security and compliance demands in this industry sector have grown considerably in recent years. This should come as no surprise since security incidents in healthcare could result in a loss of life. That designator—namely, whether a cyber attack could actually kill a human being—has always been a prime benchmark for determining the gravity and seriousness of a security scenario.

To address this growing need, the analysts at TAG Cyber developed a new Healthcare Cyber Security Framework (HCSF) that would serve as a compact and useful basis for supporting evaluation of whether a given platform is well-suited to meet the needs of a healthcare organization. The HCSF, in contrast to many other frameworks, is focused on commercial platform evaluation, and is also free for download and use by anyone.[7]

[7]Healthcare security evaluation criteria do exist, such as HITRUST, but these frameworks require payment-for-use, and the TAG Cyber team views this as an unreasonable burden on healthcare organizations desiring improved cyber security for their systems. Hence, the compact criteria we offer here is considered open-source and welcome for use by assessors and auditors.

The HCSF is best applied through its ten questions—referred to as the *HCSF Top Ten*—to be asked by any assessment, audit, or review professional when considering use of a given commercial platform in a healthcare setting. The HCSF Top Ten questions are as follows:

Question 1: Discovery—*Does the platform assist in identifying the unique types of devices that often arise on a healthcare network?*

Healthcare networks, especially in healthcare facilities such as hospitals, will typically involve the introduction of a diverse assortment of different medical devices. Any platform designed to reduce security risk for this sector must include explicit support for identifying unique devices and offering guidance on mitigation.

Question 2: Regulatory—*Does the platform provide assistance in meeting the myriad of regulatory and compliance demands in healthcare?*

The intensity of regulatory and compliance requirements for healthcare company participants cannot be understated. Platform support for compliance includes improved visibility, report generation, findings summaries, and risk mitigation. These capabilities streamline compliance processes for healthcare teams.

Question 3: Design—*Has the platform been built to strict design standards to reflect the importance of correct operation to prevent loss of life?*

Unlike many business sectors, successful attacks on healthcare networks could result in significant loss of life. Such gravity of consequence must be addressed in any platform for healthcare through strict design standards to ensure safe, correct operation under any set of conditions or scenarios.

Question 4: Privacy—*Does the platform include sufficient controls to properly protect the confidentiality of healthcare information?*

The cyber security industry has come to recognize recently that healthcare records have now surged ahead of credit card records in value. This implies that security platforms supporting healthcare networks must include specific controls to avoid compromise of patient and other private information.

Question 5: Interoperability—*Has the platform been designed to be easily interoperable with a growing number of automated tools supporting healthcare?*

Since the healthcare industry has emerged as one of the most popular and vibrant sectors for new technology innovations, it is imperative for any platform focused in this area to include the ability to interoperate. This is usually done via the inclusion of open application programming interfaces (APIs).

Question 6: Usage—*Has the platform been designed for ease-of-use or ease-of-interpretation by healthcare participants who are not cyber security experts?*

The healthcare industry has not been a traditional employer of cyber security experts. The sector did not develop with cyber security as a primary concern. Obviously, this has changed, so any platform focused on healthcare must be easy-to-use and produce results that are easy-to-interpret for non-experts.

Question 7: Segregation—*Does the platform support the logical or physical segregation requirements of healthcare organizations or groups?*

Many healthcare networks have developed in a so-called flat manner, with open visibility between devices scattered across the enterprise. Healthcare security teams are thus focused on segmenting their networks, so platforms supporting this sector must easily integrate with such initiatives.

Question 8: Liability and Risk—*Does the platform provide reduction in both liability and risk for the healthcare organization?*

The financial liability and potential risks associated with the healthcare industry are well-known, which implies that cyber security platforms supporting this sector must include functionality that supports liability and risk reduction. Obviously, it goes without saying that such platforms must also never increase liability or risk.

Question 9: Third-Party Review—*Does the platform support on-going review, analysis, and assessment by third-party assessment teams?*

The requirements to review, analyze, and assess healthcare networks for vulnerabilities has intensified in recent years with the growing liability and threat. Platforms supporting healthcare systems must include provisions to support the scrutiny requirements of third party auditors, assessors, testers, and regulators.

Question 10: Evolution—*Has the platform been designed to evolve with the inevitable innovations occurring in healthcare-related technologies?*

As one might expect, exciting new innovations emerge regularly for protecting healthcare networks. As a result, any commercial platform designed to interoperate with other systems on a healthcare network must be sufficiently flexible to adapt to future security and functional innovations.

As suggested above, the TAG Cyber HCSF Top Ten provide a suitable means for assessing the suitability of the RedSeal platform for use in healthcare networks (see below). An advantage of the HCSF for this effort is its focus on commercial platforms, versus the more general frameworks that address issues outside the general scope of a platform assessment (e.g., whether a healthcare team has proper staff recruiting processes, etc.)

The rubric recommended by TAG Cyber for use in assessing commercial platform suitability for healthcare networks based on the HCSF is the following:

1. Direct Coverage—This is the greatest level of coverage for a given platform with respect to any of the questions. The platform should clearly and effectively cover the HCSF question being addressed.

2. High Level of Support—This is a high level of coverage but might rely on adjacent or complementary controls or functions to clearly and effectively cover the HCSF question being addressed.

3. Complementary Support—This involves a platform offering adjacent or complementary control to other functions that are more directly addressing the HCSF question being addressed.

4. Not Applicable—This involves the platform not being deemed applicable to a given HCSF question being asked. This does not imply any negative impact, but rather just a non-applicability.

The use of the HCSF and associated rubric above require that the assessment team use their judgment to make suitable determinations. The TAG Cyber team recommends conservative estimates, which usually demand some tangible evidence of support before a platform is given credit for one of the four values included in the HCSF rubric.

TAG Cyber HCSF RedSeal Assessment

The RedSeal platform was analyzed in detail using the TAG Cyber Healthcare Security Framework (HCSF) as the basis for assessment. Each major functional component was cross-referenced with the HCSF Top Ten to determine suitability of the RedSeal platform to protect healthcare network assets. Below is a brief summary of TAG Cyber's results and justification for the HCSF questions.

Question 1: Discovery *Does the RedSeal platform assist in identifying the unique types of devices that often arise on a healthcare network?*

Result: Direct Coverage.

Justification: The ability to identify unique device types is one of the great strengths of any network modeling solution, including the type supported by the RedSeal platform. By creating a unique connectivity map with associated meta-data and information for a given healthcare network, RedSeal serves to highlight unexpected network devices that might exist.

Question 2: Regulatory *Does the RedSeal platform provide assistance in meeting the myriad of regulatory and compliance demands in healthcare?*

Result: High Level of Support.

Justification: The RedSeal platform provides highly effective network models that can complement the needs of external regulatory and compliance reviewers. Such visibility can easily ensure a successful assessment engagement with lower cost, less review time, and fewer demands on the operational healthcare network teams.

Question 3: Design *Has the RedSeal platform been built to strict design standards to reflect the importance of correct operation to prevent loss of life?*

Result: High Level of Support.

Justification: Since RedSeal is focused on digital resilience, it is specifically focused on correct operation. Its design standards appear to be word-class[8] and its focus on network modeling will result in increased assurance that a given healthcare network does not include unintended components or devices.

[8]The TAG Cyber team did not perform a detailed code or low-level software analysis of the RedSeal platform and did not perform detailed audits of RedSeal software development lifecycle processes. Instead, high-level information on these areas was collected and reviewed by the TAG Cyber team during the assessment period, and was used as the basis for the HCSF judgment.

Question 4: Privacy *Does the RedSeal platform include sufficient controls to properly protect the confidentiality of healthcare information?*

Result: Complementary Support.

Justification: Since the RedSeal platform does not store sensitive user credentials, healthcare records, or other private data, it does not include the associated burden of protection. For the data it does include, however, the system does an acceptable job of ensuring protection from unauthorized access or use.

Question 5: Interoperability *Has the RedSeal platform been designed to be easily interoperable with a growing number of automated tools supporting healthcare?*

Result: Direct Coverage.

Justification: Interoperability is directly supported in RedSeal because it creates its models easily and flexibly, regardless of changes to the underlying healthcare network. In fact, as the network changes, the power of the RedSeal solution would appear to become more obvious to security and network teams.

Question 6: Usage *Has the RedSeal platform been designed for ease-of-use or ease-of-interpretation by healthcare participants who are not cyber security experts?*

Result: High Level of Support.

Justification: Usage, administration, and interpretation by non-experts is supported by RedSeal, since the tool abstracts complex network data into more meaningful information that can be absorbed by non-experts. Reviewing network documentation might be tough for many participants in a healthcare ecosystem, but RedSeal models might make this more feasible.

Question 7: Segregation *Does the RedSeal platform support the logical or physical segregation requirements of healthcare organizations or groups?*

Result: Direct Coverage.

Justification: Logical and physical segregation require a network modeling task such as supported by RedSeal. This implies not only direct coverage for this requirement, but also necessary coverage, which suggests that RedSeal modeling is uniquely necessary for any network or workload protection redesign.

Question 8: Liability and Risk *Does the RedSeal platform provide reduction in both liability and risk for the healthcare organization?*

Result: High Level of Support.

Justification: Effectively supporting increasing liability and risk concerns in the healthcare industry demands the existence of accurate documentation on the network infrastructure supporting a given healthcare organization. RedSeal thus provides a high level of support for this liability and risk-based HCSF requirement.

Question 9: Third-Party Review *Does the RedSeal platform support on-going review, analysis, and assessment by third-party assessment teams?*

Result: High Level of Support.

Justification: On-going review, analysis, and assessment by third parties is enhanced by network maps and models along the lines of what RedSeal provides. This implies a high level of support for this HCSF requirement.

Question 10: Evolution Has the RedSeal platform been designed to evolve with the inevitable innovations occurring in healthcare-related technologies?

Result: High Level of Support.

Justification: Innovation in healthcare cyber security, networking, and application support demands that platforms provide for flexible open interfaces. The RedSeal platform works with changing healthcare network infrastructure and is hence highly supportive of innovative new capabilities for security or other functions.

HCSF Factor	Assessment
Q1: Discovery	Direct Coverage ←
Q2: Regulatory	High Level of Support
Q3: Design	High Level of Support
Q4: Privacy	Complimentary Support
Q5: Interoperability	Direct Coverage ←
Q6: Usage	High Level of Support
Q7: Segregation	Direct Coverage ←
Q8: Liability and Risk	High Level of Support
Q9: Third-Party Review	High Level of Support
Q10: Evolution	High Level of Support

FIGURE 3. SUMMARY OF REDSEAL ASSESSMENT FINDINGS

RedSeal for Healthcare: Assessment Findings Summary

This independent TAG Cyber assessment of the degree to which the commercial RedSeal platform supports modern healthcare cyber security and compliance objectives, produced the following conclusion:

Finding 1: RedSeal provides effective cyber security enhancement for healthcare networks.

This finding suggests that prevention, detection, and response to cyber threats in a healthcare network environment is assisted through use of the RedSeal platform.

RedSeal cyber modeling provides a comprehensive roadmap for healthcare organizations to address the issues targeting the sector. Healthcare organizations would thus be wise to initiate such cyber modeling to reduce risk, and to help reduce the complexity that characterizes modern healthcare networks. Specific areas where direct coverage is offered includes support for discovery, interoperability, and segregation, as determined through the HCSF assessment.

Finding 2: RedSeal supports enhanced compliance management for healthcare networks.

This finding suggests that the intense compliance needs of healthcare security and network teams are greatly assisted through use of the RedSeal platform.

RedSeal offers reporting, visibility, and metrics that are perfectly suited to address the requirements of modern healthcare compliance activities. Major framework certifications, in particular, will benefit from the deployment and use of RedSeal, as evidenced by the extensive feature mapping.

Finding 3: RedSeal supports increased digital resilience for healthcare networks.

This finding suggests that the digital resilience focus of the RedSeal platform reduces the risk of cyber threats, especially ones that might degrade healthcare network operation.

The RedSeal goal of helping enterprise teams, including in healthcare organizations, achieving digital resilience offers an excellent means to orchestrate and synthesize cyber security and compliance objectives using a common platform. This reduces the seams that often exist between security and compliance.