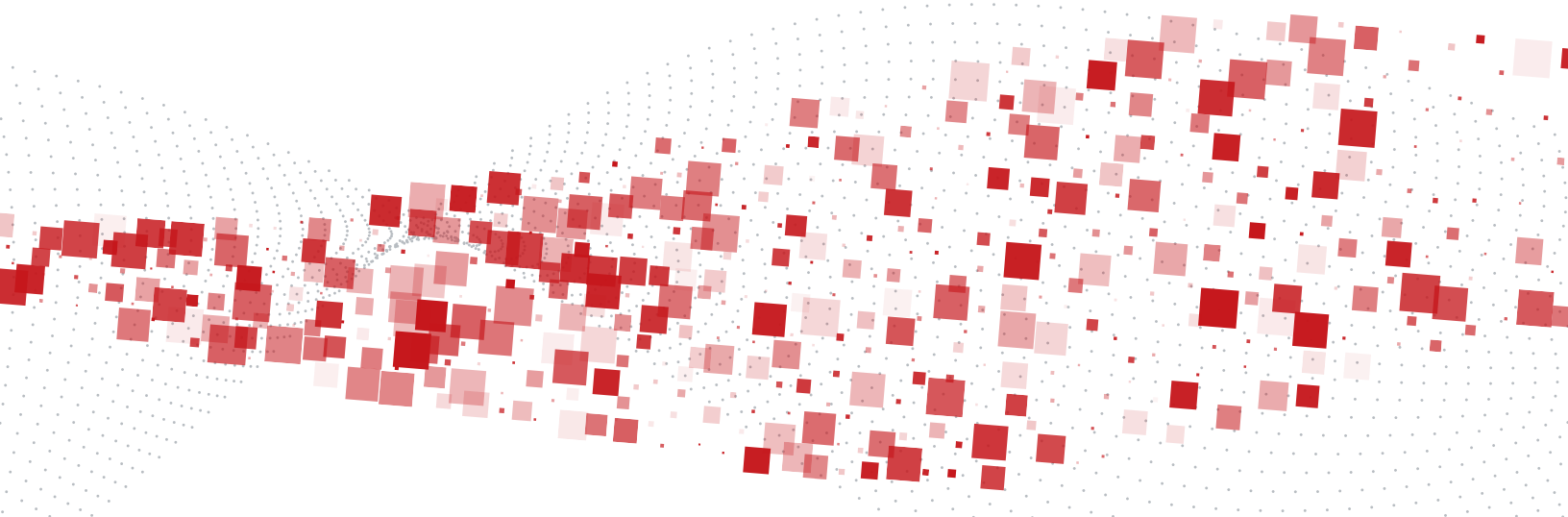
SOLUTION BRIEF

Cybersecurity

Compliance and Auditing



Executive summary

Lengthy, manual cybersecurity compliance efforts have been expensive for US government agencies—both in budget and time. The pace of network change is causing audit teams at all levels to realize the futility of trying to manually comply with cybersecurity regulations. The time gap between sampling network configurations and getting audit results inevitably means that the network has changed and the results are no longer valid. RedSeal's network mapping and analysis platform is turning this around. Compliance and audit teams are able to reduce network modeling times from weeks to less than a day. They use RedSeal's automation to visualize the current status of their as-built networks, reduce costs, and improve operational tempo—while enhancing the digital resilience of their networks.

> *"With RedSeal we are CCRI ready 90% of the time."*
>
> **– Anthony Pierce, JSOC**

Background

DISA has compliance requirements for network and security devices called Ports, Protocols and Services Management (PPSM). These are standards for the DoD Information Network (DODIN) and the Joint Information Environment (JIE) networks. PPSM is an instruction sheet on how to configure network and security devices and how to get approval for that configuration to operate on a network.

DoD conducts PPSM and other compliance and vulnerability assessments to evaluate risk and document security implementation strategies. Called Command Cyber Readiness Inspections (CCRI), these audits occur a least annually for most DoD networks. They find that network and security devices creep out of compliance over time, due to undocumented configuration changes, personnel and organizational changes, and operational cadence.

REDSEAL

Audit and compliance at DoD

At the United States Marine Corps, the cyber compliance team used to travel to each location to prep for a CCRI audit. They would start with a few sample configuration files. Checking for deficiencies in this small sample would take 3-5 days. At this point, the team would be able to propagate the list of configuration issues out to the network ops team to be remediated. This manual process of complying with DISA regulations was clearly too long—and inefficient.

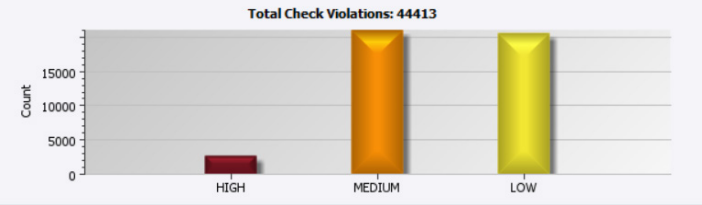


Figure 1: STIG check status

After learning from the USMC Information Assurance Range about RedSeal's ability to automatically model networks, the USMC team deployed RedSeal and completed the process in hours. Now, they use RedSeal's platform to map site infrastructure and test for compliance against DISA STIGs, and compare their documented architecture against what was actually implemented. This has not only saved the USMC hundreds of man hours, but also increased their audit coverage from a network sample to include all their network devices.

The USMC audit team now has actual information about their entire network, based on automated, continuous network monitoring. Moreover, each location's staff is no longer pulled away from daily operational needs to deal with the demands of a DISA audit. RedSeal continuously audits their networks for compliance.

In 2014, the USMC audit team shared their success in lowering costs, increasing operational tempo and improving digital resilience with another DoD command. This command's cybersecurity team was also looking for a better way to maintain compliance with DISA regulations. They struggled to create audit artifacts from normal operations. After learning about USMC's success, they deployed RedSeal and saw similar results. More importantly, the security teams realized that the vulnerabilities prioritized by RedSeal were truly the highest risk. Beyond compliance with DISA audits, RedSeal is used to increase network and cybersecurity resilience by both the NOC and SOC teams.

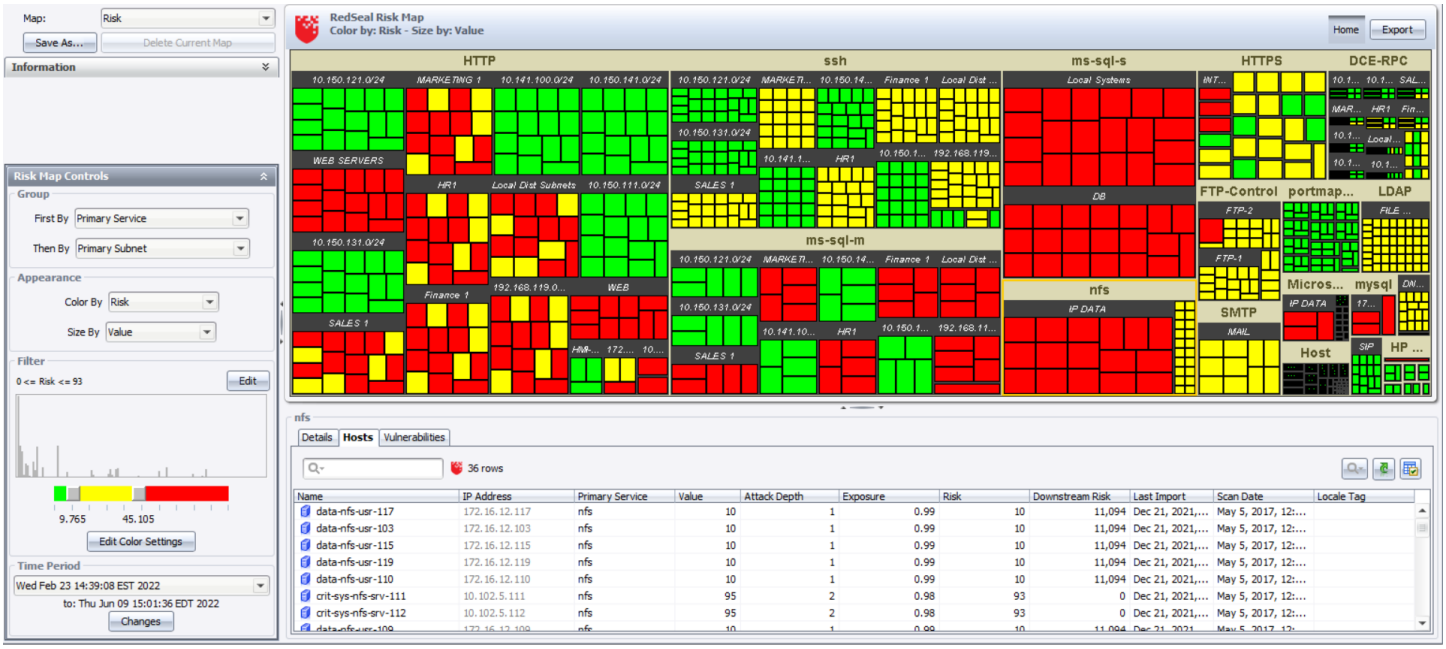


Figure 2: End point risk status

Audit and compliance in the intelligent community

At this point, the Defense Threat Reduction Agency and other intelligence community audit teams asked, "What do you use to pass audits so well?" and word of RedSeal spread.

For example, one intelligence agency had a team of five contractors assigned, among other things, to verify compliance with PPSM. They expected this would take ten percent of one contractor's time, but it became a full-time project for the entire team for two years—and they still couldn't validate PPSM compliance. Why? They just didn't know the actual state of the network's configuration. Then, the agenvcy's security team implemented RedSeal to automate and validate their actual network configurations and access. RedSeal was able identify the PPSM policy violations and quickly bring and keep the intelligence agency in compliance with the standards. And, the five contractors were able to do what they had originally been hired to do.

Another intelligence agency had a vulnerability assessment program that was expensive and sub-optimal. The program was run by two internal employees and 16 contractors. They went from data center to data center, conducting assessments that could each take from two months to a full year.

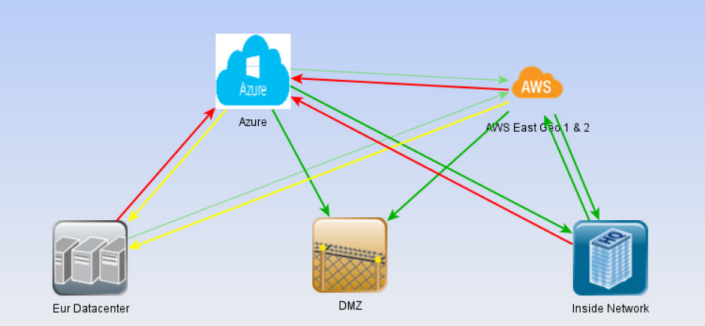


Figure 3: Example of PPSM compliance

First they had to inventory each data center and find all the configuration files. Then they had to review each set up to make sure it was updated and had applied best security practices. At that point, they could create a network map.

With the static network map, they could finally begin to manually analyze the network for compliance. Given time and resource constraints, the team was forced to triage. They ignored medium and low level vulnerabilities to focus on a short list of the most critical.

> *"We realize now that we can't leverage the other cybersecurity tools unless we have RedSeal.*
>
> *RedSeal is core to our cybersecurity plan."*
>
> **– Intelligence Agency Cybersecurity Team**

Of course, by the time they completed their analysis, the whole network had changed. The network map was merely a snapshot in time. Plus, the vulnerability assessment reports didn't include paths that allowed intruders to "leapfrog" deeper into the network.

The agency realized that getting one or two reports per year on a network that had already changed—at a cost of $5 million—was not a situation that could continue.

After researching various cybersecurity tools and getting a glowing review from other cyber teams in the government, the agency's cybersecurity team realized that RedSeal was the solution they needed. They saw that RedSeal's continuous monitoring of configuration files on their network meant that their network map would never be out of date. RedSeal could drastically improve their situational awareness and ability to manage risk with its dynamic, logical network model of the network. Experts at In-QTel were brought to review RedSeal. Approval was quickly given. On a Monday, agency engineers told RedSeal, "We want it on Friday!"

Now, after deploying RedSeal agency wide and setting up 14 instances, the agency conducts continuous assessments year round across all data centers. After five years, their feedback has been hugely positive, "We realize now that we can't leverage the other cybersecurity tools unless we have RedSeal. RedSeal is core to our cybersecurity plan."

Measuring cyber security progress

While agencies are increasingly seeing how RedSeal can help with compliance audits, and with network and security resilience, they ask how they can measure the effectiveness of their cyber investments. There isn't a set, widely-accepted standard for cybersecurity resilience.

For the US Navy, network configuration checks and creating network access models was just the first step towards triaging vulnerability remediation and cyber incident response. As everywhere, their networks are constantly changing. The Navy wants to know how many networks there are and what is connected to them. They need to understand what risk any changes to network access can present to a mission.

The security metrics tracked today measure activities, not risk. For example, most organizations report on metrics including:

- Number of attacks
- Number of intrusions
- Number of patches
- Number of config changes approved

These types of metrics do not tell us how secure we are and how risk is introduced to a network. In cybersecurity, managers need metrics to help them make decisions based on risk and to answer questions on how secure they are in relative terms.

RedSeal's model of your network adds an understanding of network access to vulnerability prioritization and remediation. RedSeal is also able to measure the digital resilience of your network—based on how complete your network map is, how closely your device configurations adhere to industry best practices, and how severe and accessible your vulnerabilities are. From this analysis, you'll get a RedSeal Digital Resilience Score™, modeled after a creditworthiness score. The score will answer critical questions including how secure you are today, what has changed and what you should fix first. You'll be able to accurately measure how prepared you are to withstand an attack and actively manage progress toward where you want to be.

With RedSeal, you're able to understand the state of your network, measure its resilience, verify compliance, and accelerate incident response. You'll be continuously prepared for audits and be able to demonstrate your compliance with cyber mandates. RedSeal is the essential cybersecurity analytics platform that puts decision-making power right in your hands.

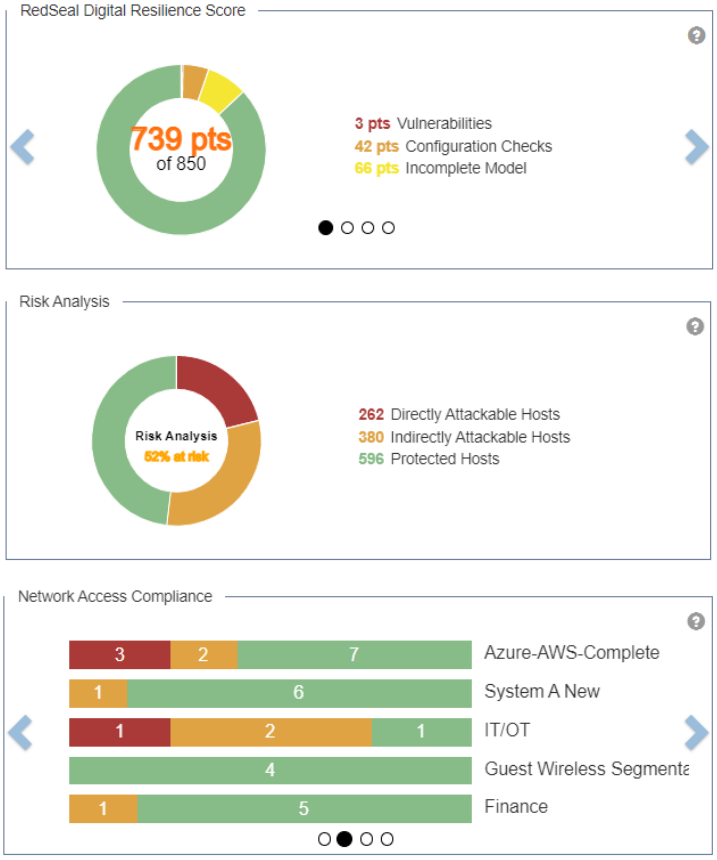


Figure 4: RedSeal Digital Resilience Score

ABOUT REDSEAL (redseal.net)

RedSeal — through its cloud security solution and professional services — helps government agencies and Global 2000 companies measurably reduce their cyber risk and show where their resources are exposed to the internet.

Only RedSeal's award-winning cloud security solution can bring all network environments– public clouds (AWS, Microsoft Azure, Google Cloud Platform and Oracle Cloud), private clouds, and on premises — into one comprehensive, dynamic visualization. RedSeal verifies that networks align with security best practices; validates network segmentation policies; and continuously monitors compliance with policies and regulations. It also prioritizes mitigation based on each vulnerability's associated risk. The company is based in San Jose, California.

REDSEAL +1 408 641 2200 | 888 845 8169 | redseal.net | info@redseal.net