

RedSeal SRM 3000 defines a new breed appliance

Information systems risk management is a very difficult proposition. First, risk is hard to quantify in a credible manner because in today's complicated networks even defining information assets can be dicey. Once the assets are defined, valuing them and figuring out loss expectancies is more difficult yet. In short, the old ways of calculating risk are tedious and unreliable. That all may be ending with the emergence of a new class of risk management tool called security risk managers (SRM).

RedSeal Systems is a pioneer in introducing this type of tool and they deliver it as an appliance. The appliance is not exactly plug and play, but configuration actually is somewhat simpler than we expected. That said, once you start playing in this arena there are no really simple solutions. The problems simply have become too complex. If you plan to deploy an SRM, give yourself the time and resources to implement it fully and correctly. The alternative is yet another boat anchor that looked good on paper, but never really realized its potential.

A swing to shift management

RedSeal boasts that their product can allow you to benefit from risk management in minutes. What that means is that you can plug it in and turn it on. You'll get some simplistic responses. But to realize the real power of this product you need to give serious thought to what you want it to use as a basis for risk calculation.

On the other hand, if you give this product its due, you will gain an extremely useful tool for identifying and managing risk. This product bases its risk calculations on a true combination of threats, as well as data flows. It begins by mapping the network, but not in a simplistic device discovery mode. Instead, it examines data flows and decides where the information is moving on your enterprise.

The SRM automatically detects firewalls and routers and begins to gather data about them. This reveals misconfigurations, data flows and some other vulnerabilities. As it gathers an increasing amount of information about the network, its analysis becomes more finely tuned. The user can add additional information and, if the

device is fully and appropriately populated with enterprise details, the SRM can calculate quantitative risk values, mitigation and patching strategies and a host of other useful, actionable factors.

The key benefit of the SRM is that it provides actionable information that engineers can use to improve security on the network and, in some cases, actually improve network efficiency.

The SRM natively supports several flavors of routers and switches, firewalls, patch management systems and vulnerability scanners. It can be configured to understand certain applications running in your environment, thus preventing wasteful analysis of vulnerabilities on non-existent applications.

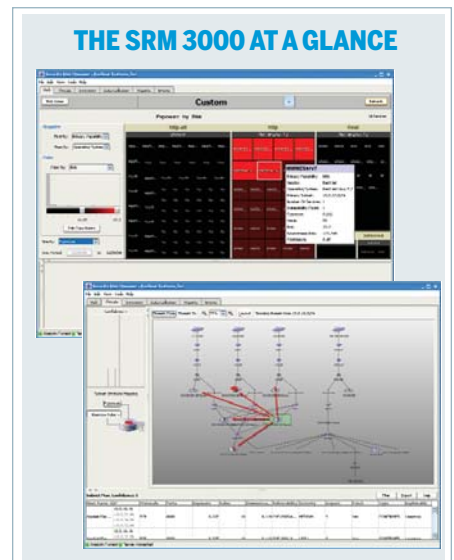
Powerful analysis tool

A characteristic of the SRM is its displays. It uses a combination of network topologies with overlaid risks, risk maps and reports to allow a combination of rapid visual identification of threats and risks, and detailed drill-down.

There is a lot to like about this product, but there also are pitfalls. As simple as it seems on the surface, to make it really dance you need to understand your enterprise and how risk management fits into your security plan. This is not the magic bullet that plugs into the enterprise and suddenly makes all risks go away. This is a very powerful analysis tool for savvy network administrators and security professionals.

Risk management is not trivial. Interestingly, C-level officers in many organizations do not view information systems risk management as important in the grand scheme of things. This is a case where the integration of information systems risk, along with other forms of risk that are more universally accepted as important, is the only way to "sell" IT risk management. SRM products can help you change that perception.

The approach of the SRM 3000 is to integrate risk management with threat and vulnerability management. Thus, the SRM 3000 becomes yet another tool to help make the IT and IT security functions more efficient by offering a risk-based view into the enterprise. In my opinion this is its most important and useful function. Highly recommended. — *Peter Stephenson*



Product: SRM 3000

Company: RedSeal Systems Inc.

www.redseal.net

Availability: Now

Price: Monthly subscription option: \$2,500/month; purchase option: \$30,000 plus annual support package.

What it does: The SRM 3000 is a security risk manager that provides views of threats, vulnerabilities and both qualitative and quantitative risks in a variety of formats and at a variety of levels of granularity, as well as suggesting risk mitigation strategies.

What we liked: This is the first product we have seen that truly understands IT risk and presents it in a manner that is extremely useful, both to IT and security teams. It is palatable to organizations that have trouble recognizing the role of information systems risk in their overall organizational risk picture.

What we didn't like: While there is nothing that we didn't like about the SRM 3000, there is a very strong caveat: Regardless of what the sales literature tells you, if you do not understand your enterprise, the role risk management plays in securing it, and if you are not prepared to invest the effort and time to exploit the capabilities of this device, don't bother with it.

Verdict: An extremely strong tool that has the potential to help shape the SRM product category, but that must be understood and deployed properly for maximum positive impact on your enterprise.



RedSeal Systems
 1820 Gateway Drive, Suite 280
 San Mateo, CA 94404
 Tel: (888) 845-8169
www.redseal.net

