SONICWALL™

# Healthcare technology company improves security to enable continued growth

Orion Health satisfies both internal and customer security requirements while reducing IT workload and speeding setup of new sites with SonicWall and KACE solutions.

"Thanks to the SuperMassives, we have significantly improved the security and stability of our core enterprise systems, and we can easily pass audits of our financial systems and audits from potential customers."

*Brad Clark, Systems Engineer, Orion Health*

**Customer profile**

ORION HEALTH
THINKING SOFTWARE FOR LIFE

| | |
|---|---|
| **Company** | Orion Health |
| **Industry** | Software & Services |
| **Country** | New Zealand |
| **Employees** | 1,100 |
| **Website** | www.orionhealth.com |

## Business need

To ensure continued business growth and reduce risk, Orion Health needed next-gen firewalls with centralized management, plus asset management for its Windows, Mac and Linux clients.

## Solution

Orion Health dramatically improved security, halved firewall management work, enabled setup of new offices in one-third the time, and gained comprehensive cross-platform asset management with SonicWall and KACE solutions.

## Benefits

- Reduced risk by significantly improving system security and stability
- Delivered easy, centralized management of firewalls, cutting associated IT workload in half
- Supported fast business growth by reducing the time required to set up new offices by 67 percent
- Reduced security and compliance risks by providing comprehensive cross-platform asset management

## Solutions at a glance

- Endpoint Systems Management
- Network Security

Founded in 1993, Orion Health has grown at breakneck speed, from five employees dabbling in health IT to a leading global health software organization with 1,100+ employees, and plans to hire more. To secure its growing network and effectively manage its multi-platform inventory of desktops and laptops, Orion Health chose SonicWall next-generation firewalls and firewall management system and the KACE systems management solution.

"We simply run a report and the K1000 will show us which machines need patching or other changes, reducing security risk. And the K1000 supports all of our machines —Linux, Mac and Windows alike."

*Brad Clark,*
*Systems Engineer, Orion Health*

## Security demands modern firewalls and easy, centralized management

Clinicians, provider facilities and OEM partners rely on Orion Health to facilitate data exchange between hospitals, health systems, health information exchanges (HIEs), affiliated providers and medical devices in order to improve care coordination, cost savings and quality of care. The company has a sophisticated IT infrastructure, with 15 offices worldwide and an additional 10 service offices that connect via a virtual private network (VPN). Client machines run the gamut, with desktops and laptops running three versions of Mac OS X, three versions of Windows and many different flavors of Linux.

Security is critical to Orion Health. In fact, the organization has an entire security team at its New Zealand headquarters and another in North America. These teams focus on security not only for the internal enterprise environment, but also for its products, which integrate with customers' critical systems. For example, one of Orion Health's products is a portal that provides clinicians and patients with access to various systems. Another, the Rhapsody Integration Engine, provides connectivity between legacy and new health systems for health departments and other organizations. "Potential customers almost always do a security audit of Orion before they allow us to take on a project because our implementation staff will have access to their production systems," explains Brad Clark, systems engineer at Orion Health. "Therefore, it is essential that our network and solutions be secure."

However, Orion Health's Cisco ASA firewalls were so dated that some were no longer supported — a serious risk the company wanted to address. Simply upgrading the Cisco firewalls was not an acceptable option, primarily because managing them was so tedious and time consuming. "There was no nice way to manage all of our Cisco firewalls in one place," explains Clark. "For example, when we needed to open up services from Amazon Web Services to our development office, I had to manually add a lot of firewall rules for various network and port ranges — and not to just one firewall, but to all of the firewalls, individually, each time."

### Products & Services

**Hardware**

- SonicWall SuperMassive 9200 next-generation firewalls
- SonicWall NSA 2600 next-generation firewalls
- SonicWall NSA 220 next-generation firewalls
- SonicWall Global Management System

**Software**

- KACE K1000 Systems Management Appliance



SONICWALL™

## Risk mitigation and licensing compliance require effective asset management

In addition, Orion Health needed comprehensive, centralized management of its broad assortment of Windows, Mac and Linux desktops and laptops, both to mitigate risk and to ensure proper licensing. "Risk mitigation was a key concern — especially after we read about a hospital being fined an enormous amount of money because a staff member had lost a laptop containing sensitive protected health information that was not encrypted. We had established encryption as a policy but we have no way of enforcing that policy," notes Clark. "Plus, everyone here is the local administrator on their own machine, which means they can install whatever software they want — but we had no way to track what was installed where. Therefore, we needed a cross-platform asset management solution that would enable us to track what is on each of our machines."

## Next-generation firewalls that are easily managed, plus cross-platform asset management

After careful research of the options on the market, Orion Health chose to implement four SonicWall SuperMassive 9200 next-generation firewalls in high-availability (HA) pairs, along with SonicWall NSA 2600 and NSA 220 next-generation firewalls at the smaller offices. To efficiently manage the firewalls, the company also deployed the SonicWall Global Management System (GMS). And to manage its large, multi-platform inventory of PCs, laptops and servers, Orion Health chose the KACE K1000 Systems Management Appliance.

Orion Health was impressed with the power of the SonicWall firewalls and the easy management provided by GMS. During the proof-of-concept, they also discovered a bonus that made the solution even more attractive and cost-effective: integrated intrusion protection. "We learned that SonicWall would kill two birds with one stone: providing us with both our firewall for managing the VPN tunnels between our offices and all the connectivity pieces, as well as that IPS function, which saved us the expense of buying a separate IPS."

## Security and auditability reduces risk and drives business

With the SonicWall SuperMassive firewalls, Orion Health has been able to dramatically strengthen the security of its network. "Previously, we had a very flat network, which posed security risks. For example, developers were in the same network as the finance system, so they could attempt to access or change the finance system, and we would have no way to even know about it," says Clark. "Using the SuperMassives, we were able to separate out our internal networks into their own zones, segregating our core IT systems, our finance systems, our knowledge base, our ticketing system, and so on. I can't even imagine trying to do that on our previous Cisco firewall — it would have been nearly impossible. Thanks to the SuperMassives, we have significantly improved the security and stability of our core enterprise systems, and we can easily pass audits of our financial systems and audits from potential customers. Plus, we've also seen performance improvements."

The SonicWall firewalls have also eliminated the need to open ports and thereby introduce risk of malware or intrusions. "Previously, at our remote offices, if I needed to access a specific service from a specific partner or potential customer, I had to open ports in from firewalls all over the world — a security risk," notes Clark.

The firewalls' content filtering and Deep Packet Inspection add additional layers of security. "The deep packet inspection ensures that all of our internet traffic is being checked, so we are protected against viruses and other threats," Clark reports. "We have also enabled the content filtering and I haven't had to touch it yet — it's very impressive that we haven't had any false positives at all."

## Easy, centralized firewall management

Orion Health is saving considerable time and effort thanks to the centralized management provided by SonicWall GMS. "Making changes to the firewalls used to be a horrible task that we dreaded and avoided," recalls Clark. "Now I can log into one interface and make changes to multiple firewalls with GMS — that is Utopia for me. I estimate that tasks take half as long as they used to — I definitely get through the tickets a lot faster than I used to."

## Visibility into and tracking of all laptops and desktops — Windows, Mac and Linux

Orion Health is now also able to easily manage its wide portfolio of laptops and desktops using the KACE K1000 Systems Management Appliance, further enhancing security. "With the K1000, we get the visibility we need into the status of each machine," says Clark. "Previously, we would learn that a machine didn't have the proper updates or encryption only when the user reported a problem or we had some other reason for visiting that machine. Now we simply run a report and the K1000 will show us which machines need patching or other changes, reducing security risk. And the K1000 supports all of our machines — Linux, Mac and Windows alike."

The K1000's asset management is particularly valuable to Orion Health because the company gives developers control over their own machines. "We don't actively push software to machines a lot of the time, since developers know best which version of OpenSSL, for example, they need," notes Clark. "But with the K1000, we can at least track those versions and offer the updates to developers who might need them. And by giving us visibility into the software that everyone has installed, the K1000

> " I can log into one interface and make changes to multiple firewalls with GMS — that is Utopia for me."
>
> *Brad Clark,*
> *Systems Engineer, Orion Health*

enables us to ensure that we have all the proper licensing, reducing compliance risk."

The K1000 has also proven to be a boon for troubleshooting. "Users reporting a problem will often say they haven't installed anything since their machine went from working perfectly to broken," says Clark. "Rather than having to hunt around the machine, our desktop engineers can check the K1000 logs and see, for example, that the user has actually installed a toolbar, and quickly resolve the problem by removing it. It's quite a handy timesaver."

## Fast setup of new offices enables quick business growth

The solutions also slash the time required to set up a new office by 67 percent — a key benefit for a rapidly growing business like Orion Health. "Previously, setting up a firewall would have taken me the better part of a day and a half or more," explains Clark. "Setting up a new office with the SonicWall firewall takes less than half a day."

## Future plans

Orion Health is looking forward to further security enhancements that are possible thanks to the close integration between the SonicWall and KACE solutions. "We plan to implement further security checking with the solutions," reports Clark. "In particular, we will be able to use the SuperMassive to verify that a user is in the office and on our network, but deny them access to the finance system because the machine they're using does not have the KACE agent installed. That enhances security because we will be able to ensure that machines have anti-virus, are properly encrypted and so on."

View more case studies at www.sonicwall.com/casestudies







SONICWALL™