Case Study

Providing Advanced, Easy-to-Manage Endpoint Protection as a Service to Delighted School System

After seeing how well McAfee® Endpoint Security protects and simplifies endpoint protection, site IT administrators across this geographically dispersed school system have quickly signed up to have it protect their school's endpoints. And, thanks to its powerful central management console, a small security team can support endpoint protection for an entire school system.

Catholic Education South Australia (CESA)

Customer profile
Second largest education provider in South Australia.

Industry
K-12 education.

IT environment
Approximately 20,000 endpoints across 94 sites.

Challenges
- Provide visibility across widely dispersed school system.
- Provide robust yet easy-to-manage endpoint security that falls within tight education budgets.

McAfee solutions
- McAfee Endpoint Security
- McAfee Complete Endpoint Threat Protection
- McAfee® ePolicy Orchestrator® (McAfee ePO™)

Results
- Comprehensive visibility across endpoints.
- Dramatically improved security posture.
- Greater coverage, thanks to improved visibility and widespread adoption.
- Reduced complexity for site IT administrators.
- Avoidance of days spent in remediation thanks to blocking of ransomware.

The Catholic education system is the second largest provider of education in Australia. In South Australia, Catholic Education South Australia (CESA) works in partnership with the region's 103 primary, secondary, and tertiary Catholic schools to promote excellence in teaching and learning for their combined 6,000 staff and 48,000 students. Senior Network Engineer Simon Sigré is part of a school-centric services team that designs and delivers best-of-breed technology services, including security technologies, for CESA schools

Multitenancy Model as Opposed to Centralized Control

Sigré and the team act as a managed service provider for the South Australian region, essentially providing on-demand, multitenancy services. "We don't force our schools to use our services," says Sigré. "Our schools are charged based on consumption of services, by number of seats. Our goal is to build great services for them. If a service is designed with the customer in mind, most likely our schools will want to participate."

In the past, only half of the 20,000 protectable endpoints in the region subscribed to the anti-malware protection that the CESA team provided. In addition, with separate management consoles at each school to manage endpoint protection, visibility across all of the schools was challenging at best. With so many consoles, it was nearly impossible to tell how many nodes were being protected at any given time or whether any nodes were inadvertently being overlooked.

"The Best Management Console I Have Ever Seen"

When CESA came to the end of the license period for its previous antivirus protection, Sigré and others evaluated market-leading options for endpoint protection. Sigré recalls that CESA's partner, Secureware, and the Intel Security account manager, Tom Beresford, built such a compelling case and made the technology so accessible that it forced the team to question its default position to stay with the incumbent product. After very thorough analysis, Intel Security emerged as the clear winner, primarily because of McAfee ePO software, a central management console that is built into the majority of Intel Security products and is, says Sigré, "a product in its own right." McAfee ePO software provides easy-to-use, intuitive, at-a-glance dashboards, as well as the ability to drill down for greater detail and out-of-the-box and customized reports.

"The decision to go with McAfee [Intel Security] was unanimous," remembers Sigré. "McAfee ePO software is a titan as far as solutions go; it's the best management console I have ever seen."

Simplifying Job of Site IT Administrators

The role-based administration functionality of McAfee ePO software enables Sigré and the team to deliver its endpoint protection in their modus operandi—that is, as service providers, delivering security as a cloud service. Authorized administrators can log in to McAfee ePO software anytime, whether or not they are within the CESA network, to see pertinent security information they need to

"We haven't had a CryptoLocker outbreak in six months. With McAfee Endpoint Security, we have more visibility, more coverage, and more customer confidence than we have had in 12 years."

—Simon Sigré, Senior Network Engineer, Catholic Education South Australia

do their job as efficiently as possible. Since McAfee ePO software is tied into CESA's identity management system and enterprise directory, access is granted only to authorized users.

"Of course, it's impressive that we can provide support for all 20,000 endpoints across 94 sites from a single screen, but even more impressive is that site IT administrators can log in to view and manage their own school's endpoints without ever requiring a deployment of McAfee ePO software onsite," notes Sigré. "Our School Support team, (another as-a-service offering provided by CESA) can continually monitor the security posture of the 70 sites it supports. Thanks to McAfee ePO software, we've assisted in making the work of all those site administrators and the support team more efficient."

Superior Detection and Blocking with McAfee Endpoint Security

CESA recently rolled out McAfee Endpoint Security across all 20,000 endpoints. McAfee Endpoint Security provides Sigré and the team superior threat detection, remediation, and forensics capabilities. The McAfee Endpoint Security framework also communicates using the McAfee Data Exchange Layer fabric used by McAfee Threat Intelligence Exchange, which CESA owns and plans to deploy in the future. With McAfee Threat Intelligence Exchange, the organization's entire security environment will be enhanced significantly with near real-time exchange of global and local threat information between the endpoint and other security solutions.

Sigré and the team deployed McAfee Endpoint Security version 10.2 across all sites but one, easily migrating approximately 4,000 nodes per day. At the one site without McAfee Endpoint Security 10.2, they are piloting McAfee Endpoint Security version 10.5, which boasts additional improvements in performance and Real Protect machine learning and behavioral analysis detection capabilities. Sigré looks forward to rolling out McAfee Endpoint Security version 10.5 in the near future to take advantage of these additional enhancements.

"Our migration to McAfee Endpoint Security has already allowed us to build our own behavioral rules to adapt to some unique use cases," says Sigré. "It has definitely strengthened our defense."

For instance, over a span of nine months, the McAfee Endpoint Security behavioral detection configurations designed by the team stopped infections from 32 separate phishing campaigns masquerading as AGL (Australian Gas and Light utility) bills or Australian Post parcel collection notices. McAfee Endpoint Security prevented countless ransomware infection attempts from these campaigns by preventing them from executing their initial JavaScript, potentially saving days that would have been spent in remediation.

Greater Visibility and Better Coverage

"Even more important to us than advanced detection capabilities and more efficient scanning, however, is the ability to have a 1,000-foot view," says Sigré. "At the end of the day, if you don't know whether or not you are covering all your nodes, it doesn't matter whether or not you have a slightly higher detection rate. If you have the best antivirus protection possible on 999 of the 1,000 devices on a site, it's that one that isn't covered that nails the server."

In the past a significant number of the CESA schools' nodes were not receiving protection because they were monitored by a management console that no one was looking at. "By consolidating many separate consoles to one

centralized console, we now have multiple sets of eyes looking at the same console, whether onsite or on the services team," explains Sigré. "Someone can say, 'Wait, I know that site has more devices than are showing up on this report—let's investigate. It's a collective effort. As a result, we no longer have nodes falling through the cracks."

Sigré and CESA IT administrators also use McAfee ePO software as an auditing tool. Using McAfee ePO software, it is easy to count devices or determine the prevalence of various operating systems—for instance, how many devices are using Windows 7 versus Windows 10, which can be especially useful at sites where many users bring their own devices.

Confidence in McAfee Endpoint Security Driving Widespread Adoption

Sigré runs a Twitter feed that pushes out important technology and security-related news to CESA schools' site IT administrators. On the feed are numerous tweets promoting how CESA's endpoint protection service, McAfee Endpoint Security, has blocked malware attacks. According to Sigré, the site IT administrators hunger for confidence that their school is well protected, so the tweets help reinforce the effectiveness of the CESA service, as well as drive demand.

"Since implementing McAfee Endpoint Security, site IT administrators and users have been delighted with the protection and ease of management of our endpoint protection service, and word has quickly spread," says Sigré. "We've doubled the number of endpoints we serve. Today the majority of schools under the CESA umbrella have signed up for it."

"McAfee Endpoint Security has become such a fundamental piece of what we do to keep our schools safe and give our site administrators peace of mind," notes Sigré. He also points out that other business he sees are crippled with anxiety over potential cyberattacks through endpoint infection, but that CESA schools protected by McAfee Endpoint Security no longer live in such fear.

"We haven't had a CryptoLocker outbreak in six months," concludes Sigré. "With McAfee Endpoint Security, we have more visibility, more coverage, and more customer confidence than we have had in 12 years."

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com