FIREEYE™ | MANDIANT®

CUSTOMER STORY

Asia Media Giant Secures Data and Delivers In-Demand Content

Singapore Press Holdings Enhances Multi-Vector Security with FireEye and Mandiant

sph

FACTS AT A GLANCE

INDUSTRY

Media

SOLUTIONS AND SERVICES

- FireEye Helix
- FireEye Email Security
- FireEye Endpoint Security
- FireEye Network Security
- Mandiant Managed Defense
- Mandiant Incident Response Retainer

BENEFITS

- Integrated solutions provide seamless protection across multiple attack vectors
- Centralized management console consolidates feeds from many vendors to deliver resource efficiencies and expedited response times
- Pre-established incident response retainer maximizes budget impact
- Strategic partnership and sourcing of expertise multiplies team effectiveness

CUSTOMER PROFILE

Asia's largest media organization—Singapore Press Holdings (SPH)—connects millions of people to the latest news. Since its incorporation in 1984, SPH's delivery has grown to include print, digital, and radio media. The company's portfolio also includes aged-care services, event management and properties in Singapore, the United Kingdom and Germany. SPH is staffed by 4,000 employees.

Millions of people count on Singapore Press Holdings (SPH) for seamless, dependable delivery of the news. The organization's most popular newspaper—The Straits Times—has a combined daily digital and print circulation of more than 450,000.

SPH's customer-focused business strategy centers around ensuring its audiences always have access to the content they need. This means that the company's systems must be continually running and operationally ready to deliver print and digital media. SPH CTO Glen Francis, responsible for cyber security strategy—is particularly mindful of the attacks that target the company's content. He reflected, "Just imagine if we went down just as we needed to get urgent news to our readers? We have to ensure that we constantly protect and stay vigilant over the systems we manage and the data that is within them."

To enhance his company's security posture and elevate the effectiveness of his own team, Francis sought outside advice. He approached FireEye and met with Mandiant consultants to get guidance on a wide range of security-related topics after seeing how the experts resolved threats to nation-states and high-profile companies.

Framework for Success

The discussions with FireEye included best practices for architecting a security stack capable of supporting the company's enterprise risk management (ERM) strategy. "We needed to identify a layered set of solutions to protect our primary threat vectors with each one needing to be best of breed and integrate well into our existing environment," explained Francis.

Francis adopted a holistic approach and established a company-wide program to protect the company from threats that could impact its ability to disseminate news. The ERM framework—modeled on ISO 31000: 2018 risk management principles and guidelines—encompasses the strategic, operational, financial, compliance and IT risks facing SPH.

"The worldwide shortage of cyber professionals dictated that whatever we implemented should be easily managed from a central location and give us the ability to efficiently respond to alerts without requiring huge amounts of effort."

"By having the right technologies and processes in place—coupled with access to expertise when we need it—we are discovering that we can be lean and agile, without compromising the security of the company. Partnering with FireEye and Mandiant acts like a force multiplier for us."

— **Glen Francis,** Chief Technology Officer, Singapore Press Holdings

FireEye Reduces Event Complexity

Following further recommendations from the Mandiant team, Francis used the free FireEye Redline endpoint security tool to identify indications of malicious activity—using memory and file analysis—and created a detailed threat assessment profile.

After completing its due diligence, SPH collaborated with regional partner Ensign InfoSecurity to secure its environment by deploying:

- FireEye Network Security—Provides advanced threat protection for attacks hidden in internet traffic using a signature-less analysis engine and intrusion prevention system to stop known and unknown threats.
- FireEye Email Security—Inspects all email attachments and URLs. Provides insights on how to respond to detected malware.
- FireEye Endpoint Security—Monitors perimeter traffic to identify and isolate compromised devices.
- FireEye Helix—Cloud-hosted security operations platform that integrates data feeds from multiple vendors into a unified, centralized view to help simplify logging, monitoring, and alert management and investigation.

"It's easier for us to view threats holistically and understand the complexity of the alerts by relying on a single company that can pull everything together and be responsible. if you have solutions from different vendors each one is managed separately and can cause unnecessary complexity," Francis explained.

To further bolster its revamped security posture, SPH uses the Mandiant Managed Defense service to access an advanced suite of managed detection and response capabilities. A Mandiant Incident Response Retainer was added to ensure IR expertise is always on standby to accelerate the identification of potential malicious activities and mitigate business impact in the event of a security incident.

"We see FireEye and Mandiant as a core part of our overall cyber security strategy: We receive an integrated set of industry-leading solutions and services that incorporate well into our existing security stack, backed by a world-class team of experts," stated Francis.

"By having the right technologies and processes in place—coupled with access to expertise when we need it—we are discovering that we can be lean and agile, without compromising the security of the company. Partnering with FireEye and Mandiant acts like a force multiplier for us."

Fundamentals in Place

The multi-dimensional ERM framework includes an analysis of the various risk factors present in SPH's environment. Francis recounted: "You can never be 100% immune to attacks but understanding the nature of our vulnerabilities enables us to invest in the areas with the biggest bang for the buck and ensure that we have taken care of the fundamentals."

He continued, "Mandiant is renowned for being called in to handle some of the largest cyber security breaches in the world. Although I hope to never have to use the Mandiant Incident Response Retainer we have in place, this credibility gives us confidence and a high level of trust that the expertise is there should the need arise."

Prepared for Tomorrow's Challenges

As a sought-after expert in multiple IT-related disciplines, Francis understands the value of forging the right partnerships to achieve his goals. He articulated, "We are just at the beginning of a whole new era of cyber security. I've watched the progress of technologies such as quantum computing and can see the potential for criminals to use its inherent processing power to create threats that are even more sophisticated, like unraveling the encryption algorithms that underpin most of today's security solutions. Staying ahead is a constant challenge.

"This makes it imperative to have a security partner that understands how to harness intelligence from its ecosystem and actively communicate these insights. Having visibility across the globe, FireEye and Mandiant are very forthcoming in sharing this knowledge and how best to deal with the most relevant threats. FireEye and Mandiant have helped us tremendously: They ensure we stay ahead of the curve!"

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

At FireEye, our mission is to relentlessly protect organizations with innovative technology, intelligence and expertise gained on the frontlines of cyber attacks. Learn how at www.FireEye.com

About Mandiant Solutions

Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce business risk.