CASE STUDY

China Pacific Insurance Protects Business and Customers with Security Management System

Robust defense system to protect data and mitigate security risks

China Pacific Insurance Group

Customer Profile
National insurance company of mainland China

Industry
Financial/Insurance

IT Environment
30,000+ endpoints, thousands of servers

China's second-largest property insurance company confidently leverages new technologies and Big Data, thanks to a security management and control platform based on the McAfee® SIEM solution.

China Pacific Insurance Group, or CPIC, is the second-largest property insurance company and third-largest life insurance company in mainland China. It offers an array of integrated life insurance, property insurance, and reinsurance services as well as investment, wealth management, and asset management services. Headquartered in Shanghai, CPIC provides services to approximately 80 million customers throughout China.

Industry Related Technological Changes Introduce New Security Risks

In China as elsewhere, widespread adoption of the Internet, smartphones, Big Data, and cloud computing have dramatically altered the way in which traditional insurance companies provide products and services. These technologies have produced tremendous opportunities to improve interactions with customers, provide more personalized service, and grow business. However, CPIC has been quick to recognize that hand in hand with benefits have come numerous security challenges.

For instance, enabling CPIC customers to access account information and pay bills online from a desktop or mobile device has increased the risk of leakage of credit card numbers and account information. In addition, the tremendous growth in the amount of data captured by CPIC for "big data" analysis, and the significant monetary value of that data, has increased incentives for hackers to target the company. Internally, the potential ramifications of improper authorizations or staff errors has become much more serious than before.

Need for Rapid Detection and Response to Security Incidents

"With all these security challenges, we knew we needed a more robust defense system to provide full and timely detection, identification, analysis, and response to security incidents," says CPIC General Manager of Information Security and Internal Controls, Ms. Li Lihong. "Cyber threats will only continue to increase and become more sophisticated, so we needed to implement a system that could continue evolving as complex attack methods continue to evolve."

CPIC's initial solutions to manage security information and events were not up to the task. The company could not log the massive amount of security-related events and flows fast enough from all the various sources—firewalls, switches, Active Directory, and other hardware and software—for timely analysis, thus delaying time to identify and respond to security threats. Passive and fragmented monitoring of security information and events also hindered effectiveness. With so much valuable data at stake, even a few seconds of delay to stop a breach could spell incalculable losses to the business, so the company resolved to find a more powerful, agile, and effective security information and event management (SIEM) solution.

Challenges

- Previous SIEM solution inadequate
- Leverage emerging technologies but mitigate security risk
- Protect large amounts of data from external as well as internal threats
- Accelerate detection of and response to security incidents

McAfee Solution

- McAfee Enterprise Security Manager
- McAfee Network Security Platform
- McAfee Web Gateway

Results

- Centralized management and control of security incidents
- Reduced IT compliance risk
- Faster detection and intelligent analysis of security events
- Dramatically improved overall security posture
- Industry recognition for information security excellence

McAfee-Based "Hawkeye" SIEM

After many rounds of evaluation and comparison of leading SIEM options, CPIC decided to partner with McAfee to create a platform to protect its valuable data. Building upon the McAfee SIEM solution CPIC created a big data security management and control platform it dubbed "Hawkeye." At the foundation of the security platform, McAfee Enterprise Security Manager delivers the performance, actionable intelligence, and real-time situational awareness required to identify, understand, and respond to stealthy threats.

"The McAfee SIEM solution underlying our Hawkeye big data security management and control platform makes it possible to identify risks, control security events, view trends, and run security operations—all much faster and more effectively than in the past," summarizes CPIC Deputy General Manager of Information Security and Internal Control Department, Mr. Zhang Jun. "We call the system 'Hawkeye' because it allows us to rapidly pinpoint critical security incidents so we can respond immediately."

The Hawkeye system automatically collects and stores approximately 1.5 billion logs daily, generated by 32 different types of sources—the company's McAfee Network Security Platform (IPS), McAfee Web Gateway, other network devices, operating systems, databases, middleware, auxiliary systems, applications, and others—and keeps the information available for immediate ad hoc queries, forensics, rules validation, and compliance. No longer is performance an issue; the massive amount of relevant information can be captured and analyzed quickly for appropriate remediation and rapid incident response.

As soon as the log data is captured, Hawkeye automatically indexes, normalizes, and correlates the information to discover isolated events from among the massive and diverse body of data. From the more than one billion events and flows collected, the system identifies approximately 5,000 threat warnings daily. "Potential security issues that we could not detect in the past—such as "worm spread," "developer's access to production data," and "bypass access through the bastion host"—are now detected automatically," notes Guo Lin, Hawkeye project manager.

More Intelligent Correlation and Automated Prioritization

With the McAfee SIEM solution, CPIC now benefits from more intelligent correlation and automated prioritization. McAfee Enterprise Security Manager calculates baseline activity for all collected information, in real time, and provides prioritized alerts with the goal of discovering potential threats before they occur, while simultaneously analyzing that data for patterns that may indicate a larger threat. Correlation goes far beyond pattern matching, The McAfee system leverages contextual information and a myriad of threat models—from access violations and account abuse to botnet activity, different types of intrusions, and vulnerability exploitations—to enrich each event for a better understanding that enables smarter decisions faster. By providing rapid detection, alerts, and automated responses, the system makes security operations more reliable and efficient at protecting the organization from external or internal attacks.

> "The McAfee SIEM underlying our big data security management and control system empowers us to discover, prioritize, and respond to threats faster and more efficiently. As a result, CPIC can focus more on business innovation and embrace with confidence the new technologies that enable greater customer satisfaction and business growth."
>
> — Zhang Jun, Deputy General Manager of Information Security and Internal Controls, CPIC

Easy-to-Use Centralized Management

By centralizing management and automating compliance monitoring and reporting, the Hawkeye system has extended visibility and eliminated time-consuming manual processes. From the dashboard, CPIC information security administrators have a centralized view of the entire enterprise security posture, compliance status, and prioritized security issues that require investigation, and can easily create ad hoc or automated reports as needed.

CPIC highly values the ease-of-use of the McAfee Enterprise Security Manager solution central console—with over 240 built-in reports, views, rules, and alerts—as well as its customizability. In addition to out-of-box rules, the company uses 58 rules that it customized and 18 compliance reports that it fine-tuned. CPIC also customized the dashboard to tailor visualization of security threats and risk trends to suit their administrative preferences.

Industry Recognition for Information Security Excellence

CPIC is not alone in facing growing security challenges as the entire financial industry faces these same obstacles. CPIC's forward-looking vision and success with the McAfee-based Hawkeye big data security management and control platform have earned it significant industry recognition. In the 2nd Conference on China Information Security, CPIC was awarded second place for "Excellent Case of Information Security" success. In addition, the Hawkeye project won the award, 2015 Future-S IT Governance and Management Practice in China.

In short, CPIC and its Hawkeye system have become a model of information security excellence for financial industries in China.

Empowered to Embrace New Technologies that Grow Business

"The McAfee SIEM underlying our big data security management and control system empowers us to discover, prioritize, and respond to threats faster and more efficiently," says Jun. "As a result, CPIC can focus more on business innovation and embrace with confidence the new technologies that enable greater customer satisfaction and business growth."

McAfee
Together is power.

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