CASE STUDY

Top Property Developer Deploys FortiRecon:

Safeguarding Digital Assets and Brand Reputation Against External Threats

Hong Kong's Chinachem Group is one of the city's most trusted brands. Over the past six decades, it has grown from a small chemicals company into one of Hong Kong's largest property developers, with a portfolio of more than 300 properties spanning residential developments, shopping malls, office blocks, and hotels. The group has a 4,000-strong workforce and over HKD141 billion in assets.

Chinachem places its contribution to the community and the environment on equal footing with its profitability. This triple-bottom-line approach is strengthened by its unique ownership structure. Neither publicly owned nor family-held, Chinachem Group takes on diverse projects like the culturally sensitive revitalization of Hong Kong's historic Central Market and the development of the age-friendly Mount Anderson residential complex, as well as investing in supporting local start-ups in the smart city technology space.

"The preservation and enhancement of the legacy that we operate is of the utmost importance to the group," said Ben Fung, Chinachem Group's Senior Associate Director of Information Technology and Solutions. "This is part of the reason that we have accelerated our own digital transformation and pioneered the application of property technology (PropTech) applications to help lead our industry forward. It also means that we take cybersecurity very seriously."

External Threats to Trusted Brands

The Chinachem IT team leverages up-to-date cybersecurity solutions and systems to secure its on-premises and cloud infrastructures. At the same time, it is well aware of the limitations of traditional enterprise security architecture: while these tools and processes can protect networks, users, and data, they are no longer sufficient to fully protect an organization's digital assets and brand.

Criminals today deploy sophisticated tools and tactics to target vulnerabilities. They might buy leaked credentials or ransomware-as-a-service from the dark web, scan for unpatched or misconfigured assets, or create fake social media accounts or websites to trick customers into divulging their personal data and bank details.

"Safeguarding Chinachem's brand against malicious activity is crucial in today's digital landscape," Fung explained. "Deceptive platforms like fraudulent websites and social media pages pose a significant threat, potentially tarnishing the trust we have built over more than 60 years and negatively impacting our brand and business."

When Chinachem Group discovered a website impersonating its brand and purporting to offer investment solutions in 2021, it acted swiftly. After alerting the police, it engaged a local service provider to provide emergency domain impersonation monitoring. However, Chinachem recognized that a more

CHINACHEM GROUP 華懋集團

"FortiRecon complements our existing security solutions. It provides us with complete real-time visibility of our external attack surface, as well as insights that enable us to take controlled, risk-based security actions earlier to reduce the impact and cost of a cyberattack, and protect our brand from abuse."

Ben Fung
Senior Associate Director of Information Technology and Solutions,
Chinachem Group

Details

Customer: Chinachem Group

Industry: Property Development

Location: Hong Kong, China

Business Impact

- Complete real-time visibility of the external attack surface, enables the IT team to identify and mitigate exposed assets
- Actionable, organization-specific threat intelligence, prioritizes risks and exposures

comprehensive solution was required to detect and deal with this type of malicious activity and help the team stay abreast of security market news amidst the challenges of busy daily operations.

"Our goal was to actively monitor our external attack surface to ensure timely detection and mitigation of fraudulent activity. But we also needed a better way to safeguard our brand and assets against known emerging threats and to fortify our infrastructure against unknown future threats, too," Fung said.

Best-of-Breed Digital Risk Protection from Fortinet

Apart from FortiGate Next-Generation Firewalls (NGFWs), Chinachem selected FortiRecon, Fortinet's Digital Risk Protection software-as-a-service solution, to proactively protect its digital assets, data, and brand from external threats.

FortiRecon comprises three integrated technologies and services: External Attack Surface Management, Brand Protection, and Adversary Centric Intelligence. Together, these provide organization-specific, expert-curated, and actionable external attack surface intelligence on exposed assets and threat actor activities, tools, and tactics. In short, FortiRecon operates outside the organizational boundary to provide the sort of visibility that an adversary has. When risks or abnormal activity are identified, FortiGuard Labs Threat Intelligence delivers an early warning, allowing swift mitigation.

"FortiRecon complements our existing security solutions. It gives us complete real-time visibility of our external attack surface, and insights that allow us to take controlled risk-based security actions earlier to reduce the risk, impact, and cost of a cyberattack and protect our brand from abuse," Fung says.

Real-Time Visibility of the External Attack Surface

The External Attack Surface Management (EASM) module within FortiRecon gives Chinachem an adversary's view of the organization and its subsidiaries' digital attack surface. With complete visibility into the external threat landscape, the Chinachem IT team can rapidly identify exposed assets, both known and unknown, and prioritize remediation.

The EASM service provides detailed descriptions of security issues it finds—such as configuration errors, Domain Name System issues, exposed database services, or leaked credentials—accompanied by actionable remediation information. FortiRecon also prioritizes risks and exposures, using a powerful combination of human resources and artificial intelligence. With a prioritized view of the organization's vulnerabilities, administrators can choose to mitigate the most severe threats first, in a controlled manner, before they become a problem.

Said Fung, "FortiRecon auto-delivers highly relevant data and updates that save our analysts time in threat research. It provides contextual visibility, relating specifically to our infrastructure, data, and brand, and translates threat intelligence into actions that we can take to prioritize protecting what matters most."

Wide-Ranging Brand Protection

FortiRecon expands Chinachem's brand protection capabilities by extending threat intelligence visibility to mobile apps, code repositories, the dark web, and social media—areas typically outside the security team's scope. FortiRecon Brand Protection (BP) swiftly identifies risks across brand, enterprise assets, and data, using proprietary algorithms to provide early warnings and allow fast action.

Business Impact (cont.)

- Monitoring the dark web, social media, mobile apps, code repositories enables early threat detection and takedowns when required
- Faster response to incidents, imminent threats, and misconfigurations, reduces the impact and cost of attacks
- Better overall protection of digital assets, data, and brand from external threats

Solutions

- FortiRecon
- FortiGate Next-Generation Firewalls

Services

- FortiRecon Digital Risk Protection Services

"While we were still in the proof of concept phase of the project, FortiRecon BP successfully identified a fake social media page that was impersonating our Nina Hotel social media account. We've also leveraged FortiRecon BP to locate and take down a fraudulent website and mitigate the damage caused by an identified log stealer, helping us protect our brand value and safeguard brand trust."

Ben Fung
Senior Associate Director of Information Technology and Solutions, Chinachem Group

The FortiRecon BP dashboard also offers access to specialized take-down services that empower Chinachem to remove unauthorized content or a fraudulent subsidiary website and shut down brand impersonation on social media.

"While we were still in the proof of concept phase of the project, FortiRecon BP successfully identified a fake social media page that was impersonating our Nina Hotel social media account. We've also leveraged FortiRecon BP and ACI to find and take down a fraudulent website and to mitigate the damage of an identified stealer log, helping us protect our brand value and safeguard brand trust," Fung revealed.

The FortiRecon Adversary Centric Intelligence (ACI) service monitors the dark web to quickly identify when sensitive information falls into the hands of cybercriminals. This reduces the window of opportunity for criminals to copy, use, or sell the data. It also enables teams to take proactive steps, such as a password reset, to prevent or block an attacks. Chinachem also added FortiGuard AI-Powered Unified Threat Protection, which is used for deep packet inspection.

Faster Response to Imminent Threats

FortiRecon ACI leverages FortiGuard Labs Threat Intelligence to provide comprehensive coverage of dark web, open source, and technical threat intelligence, including threat actor insights. With curated, relevant, and contextual insights into imminent threats to Chinachem, the IT team is able to respond faster to incidents and uncover and fix misconfigurations in the company's exposed assets before they are used by an attacker.

"This additional layer of visibility in attack surface monitoring, alongside insight into security risk trends, allows us to identify emerging threats, take timely corrective measures, and bolster our overall security defenses," Ben Fung added.

"Fortinet's FortiRecon offer is broad and valuable," he reiterated. "It covers critical areas of exposure, monitoring the entire external attack surface, and provides early-warning intelligence and new insights into malicious activity targeting our company and credible threats to the brand. This enables faster action and ultimately helps reduce the impact and cost of attacks."

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

October 18, 2024 9:40 AM / 2854703-0-0-EN