九龍建業有限公司
KOWLOON DEVELOPMENT COMPANY LIMITED

CASE STUDY

Enhancing security posture with Zero Trust Network Access at Kowloon Development Company

Kowloon Development Company, a leading property development company based and listed in Hong Kong, turned to Palo Alto Networks to enhance its security posture and protect against sophisticated threats with the PA-3220 Next-Generation Firewall.

paloalto NETWORKS

IN BRIEF

Industry

Real Estate

Challenges

Kowloon Development Company was looking for an innovative and easy-to-use cybersecurity solution to keep up with business growth and deal with increased cyberattacks.

Solution

Kowloon Development Company turned to the PA-3220 Next-Generation Firewalls (NGFWs) to accelerate detection of cyberattacks and manage its security policies to effectively keep up with business growth.

Benefits	Quantifiable Data
Enhanced detection and prevention	+ Quickly identify issues and/or threat origins + Faster malware detection
Elimination of manual activities and reduction of human error	+ Easy-to-use systematic design with simplified process with 30% time savings
Simplified security policies implementation	+ 60% time savings with faster implementation of security policies
Enabling efficiency	+ Creation of actionable and insightful reports for both senior management and IT department

Kowloon Development Company Limited (KDC), a member of the Polytec Group, is a Hong Kong-listed company (SEHK:34) engaged in property investment and investment holdings. Since then, it has principally engaged in property development in Hong Kong and Mainland China. Its businesses involve multiple stakeholders and large financial transactions, which allows no room for mistakes and requires risk management in all dimensions.

As cyberattacks gain in speed, sophistication and frequency globally, organisations are becoming more cognizant of their cybersecurity risks. KDC understood the growing importance of cybersecurity—to protect privileged and confidential client information, maintain the company's operational efficiency, and adhere to strict regulatory and compliance requirements.

CHALLENGE

Difficulty in detecting rampant and advanced cyberattacks

The COVID-19 pandemic made it evident that the global cyberthreat landscape was worsening, as many organisations were ill-equipped—in terms of digital tools and from a security standpoint—to ensure a seamless transition to work from home (WFH) as the default mode of work.

"In short, the legacy firewalls posed multiple problems for us; out-of-date and complex operations which were not designed to detect and prevent human misconfiguration nor errors," shares Group IT Head, Kowloon Development Company.

As such, KDC looked to Palo Alto Networks Next-Generation Firewalls (NGFWs) to ensure that the organisation was taking a more proactive approach to cybersecurity and also reflect the importance KDC attaches to cybersecurity. KDC also sought to elevate its cybersecurity posture for both its Hong Kong headquarters and offices in Mainland China.

REQUIREMENTS

Best-in-breed cybersecurity solutions to address a new era of cyberthreats

KDC looked to identify new cybersecurity solutions that would construct a Zero Trust security model and meet the following requirements:

- **Effective detection of new cyberattacks**, including the use of machine learning (ML) in analysing cyberattack paths and methods, thwarting further attempts.
- **User-friendly and minimise repetitive tasks**, such as command input, into a few clicks—a better-designed, more automatic system to prevent human errors.
- **Automate data collection** from different security tools and generate an easy-to-read report with actionable insights.
- **Build a Zero Trust cybersecurity environment** that can determine users' authorisation in consideration of different factors to secure on-premises and cloud operations.
- **A reliable partner** that understands the latest trends in cyberattacks and has the long-term vision and capability to help KDC and other clients respond to different forms of cyberattacks and address their challenges accordingly.

SOLUTION

With PA-3220 NGFWs deployed, KDC now has peace of mind that it is more effective in responding to cyberattacks and is able to achieve end-to-end protection. Being ML-powered, the PA-3220 NGFWs target high-speed internet gateway deployments and secure all traffic, including encrypted traffic, using dedicated processing and memory for networking, security, threat prevention, and management. ML embedded in the core of the firewall provides inline signatureless attack prevention for file-based attacks while identifying and immediately stopping never-before-seen phishing attempts.

In the past, KDC required the assistance of third-party software to verify the user identity in question. That has since changed, as the PA-3220 enables visibility, security policies, reporting, and forensics based on users and groups, not just IP addresses. With Panorama™, KDC has a unified user interface and benefits from centralised management, configuration, and visibility for multiple distributed NGFWs (irrespective of location or scale).

> "With Palo Alto Networks Next-Generation Firewalls (NGFWs), we can now quickly implement security policies, create reports, and save our time from identifying issues and threat origins."
>
> **— Group IT Head, Kowloon Development Company**

BENEFITS

Detection and prevention of attacks

The PA-3220 NGFWs can detect and prevent known and unknown threats—including all port invasions, malware and spyware—detecting and preventing more potentially advanced cyberthreats than the firewalls previously deployed by KDC.

In the past, when the IT department discovered abnormal usage patterns, there was a tedious process involved as they could only identify IP addresses of the device in question as the first step before turning to third-party systems to further identify related users. PA-3220 NGFWs provide a single platform to identify the related person and suspicious activities from a multi-user computer system, allowing staff to understand the circumstances and provide subsequent training for staff awareness and education where required.

Easy to use and 30% time savings for IT team

In the past, KDC's IT team was required to carry out multiple procedures on the legacy firewalls' operation system in order to complete their work, and this led to human error due to the complicated operating process. With the PA-3220 NGFWs, this is now a simpler operation that has replaced the repetitive and cumbersome procedures, which has in turn greatly reduced human error. Additionally, this resulted in a 30% reduction of time for the IT team, giving the team time to focus on strategic work and other priorities.

Simplified security policies implementation resulting in 60% time savings

While KDC has a bring-your-own-device policy (BYOD), it can cause significant challenges for the IT department from a device identification and security policies implementation standpoint. The PA-3220 NGFW and Panorama enforce consistent security policies across all devices, regardless of operating systems—changing a three-step procedure to a single-step procedure on a single platform.

Enabling efficiency in creating insightful reports

The PA-3220 NGFWs can automate data collection from different security tools, identifying useful data with actionable insights and enabling the IT team to generate easy-to-read reports for senior management. The attack surface is widening with remote work, and the IT department looks to cooperate with innovative vendors that are willing to invest in cybersecurity solutions.

CONCLUSION

Securing the network and minimising unknown threats with the PA-3220 NGFWs

With the PA-3220 NGFWs, KDC has enhanced its effectiveness in detecting and preventing cyberattacks and minimises the potential attacks that corporate networks could face. Under a simplified procedure to identify and respond to cyberthreats, the company can reallocate its manpower to more complicated job duties instead of repetitive duties.

At the same time, the PA-3200 NGFWs automate their data collection and shorten the preparation time for creating reports, which allows management to make quick decisions, eventually elevating the company's general work efficiency and reducing uncontrollable risks. For KDC, whose business often involves large financial transactions, its risk management control is most crucial. With Palo Alto Networks, KDC can rest assured these controls are in place to support business management.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com