

Asia's leading life science company uses multi-layered, AI driven approach for advanced email protection

Barracuda delivers clean bill of email health to Avalon Biomedical (Management) Limited



Suspicious email bypasses security

When Avalon's Senior IT Manager, Ryan Lee, received a call from an employee in finance asking him to check a suspicious email from a supplier, he sensed there was something wrong. Once Lee opened the email, everything about the message looked authentic and it was only the request to pay money into a different bank account that raised a warning flag.

As Lee and his team examined the email, they were alarmed to discover an impersonation attack was in progress. "Everything about the email content looked normal. The address was right, and the email signature was the same as usual. But there were two errors. There was an extra letter in the sender's email address and the bank account was different though the reason for this appeared plausible."

"Although this threat was neutralised, we realised if one attacker had bypassed the email gateway and our existing network security, there may be others lurking in inboxes ready or launching attacks from within. Had it not been for the employee flagging the email, the attack might not have been thwarted."

As a Hong Kong homegrown biomedical group, Avalon is dedicated to creating a better life for everyone by incubating biomedical ideas from Greater China and nurturing them into viable healthcare solutions that can be brought to the Asian markets and beyond. Unfortunately, the healthcare sector is particularly prone to cyberattack mainly for financial gain, intellectual property, and credential theft; even more so after COVID-19 as Lee knows only too well.

Profile

- Leader in next generation healthcare solutions
- Founded in 2013 in Hong Kong
- 130 employees globally

Challenges

- Increase in email-borne threats mainly spam, phishing, spear-phishing, and business email compromise
- Executives and employees in procurement and finance specifically targeted
- IT resources stretched due to threat volume leading to network downtime and loss of productivity

Solution

- Barracuda Essentials
- Barracuda Sentinel

Results

- Gained comprehensive protection against phishing, and other email-borne attacks
- Customised and detailed reports provide understanding of email attack tactics
- Streamlined IT resources
- Reduced risk of financial loss, data leak and reputational damage

“Before Covid hit, there were sustained ransomware attacks, and other email borne threats but the protection we had worked well. Or so we thought. After the pandemic began, these attacks rocketed, and the network struggled to cope putting a severe strain on IT resources and normal operations.”

Now with the uncovering of a business email compromise that had somehow bypassed security, Lee knew something had to be done. And fast.

Network scan reveals worrying pattern

Lee quickly reached out to Superhub, a major cloud solutions provider in Hong Kong, to arrange meetings with email threat protection vendors but discovered only Barracuda Networks offered comprehensive email threat protection.

Wanting to learn more, Lee attended a Barracuda webinar and, impressed with what he saw, trialed Barracuda’s free Email Threat Scanner to see what threats were inside Avalon’s network.

“The results were astonishing. Over twenty phishing attacks were detected and, when these were examined, it was clear the victims were totally unaware there was anything wrong and there was a high risk of fraud. The results also revealed that the existing security was not up to the task of rooting out sophisticated email-borne threat.”

Twelve thousand organisations have used Barracuda Email Threat Scanner to uncover 10 million email threats. Using artificial intelligence and Application Programming Interfaces (API), Barracuda Email Threat Scanner works by zeroing in on all email threats including social engineering attacks sitting in corporate mailboxes.

“The attacks were sophisticated enough to bypass security and socially engineered to fool the recipient into ongoing email conversations. In fact, the scan report highlighted a clear pattern of finance and procurement employees being subjected to more phishing and spear phishing attacks than in any other department.”

Advanced protection beats advanced threats

Impressed with the trial, Lee decided to deploy Barracuda Essentials and Barracuda Sentinel to sanitise the network from attackers, prevent inbound email threats, and stop the unauthorised exfiltration of data and sensitive information.

Barracuda Essentials defends against advanced threats, including those built to evade email filters, by using a combination of advanced technologies including multiple, layered analytic engines with behavioral analytics, static analysis, and CPU-emulation sandboxing to detect known and unknown threats. By stopping threats at the gateway before they have a chance of finding their target mitigates financial loss and reputational damage risks.

“Because Barracuda Essentials checks every single email only those messages with a clean bill of health are delivered. This protects the company from email-borne threats, increases productivity, and frees up IT resources.”

Barracuda Essentials can also prevent outbound sensitive – employee information, intellectual property etc. – data from leaving the corporate network. This might involve encryption, quarantining, or even blocking certain outbound emails based on their content, authorisation, sender, or recipient.

“Because business email compromise is typically content based fraud, Barracuda Sentinel outsmarts attackers through the harnessing of artificial intelligence to analyse and detect signs of malicious intent and deception”.

Ryan Lee

Senior IT Manager

Avalon Biomedical (Management) Limited

Predicting vulnerable employees and groups

Further hardening Avalon's email threat protection is Barracuda Sentinel. Fully integrated with Office 365, Sentinel learns communication patterns to detect personalised fraud to protect against business email compromise and account takeover.

"Because a business email compromise typically is content based fraud, Barracuda Sentinel outsmarts attackers through the harnessing of artificial intelligence to analyse and detect signs of malicious intent and deception."

There was another key reason why Lee was keen to deploy Barracuda Sentinel; the power to predict employees most at risk for business email compromise.

"Barracuda Sentinel puts us ahead of the threat curve because we can now predict the employees most vulnerable to spear phishing and credential theft. All this takes place in the cloud without risking network integrity and gives vital information about the methods used by attackers."

"Barracuda Sentinel puts us ahead of the threat curve because we can now predict the employees most vulnerable to spear phishing and credential theft. All this takes place in the cloud without risking network integrity and gives vital information about the methods used by attackers".

Ryan Lee

Senior IT Manager
Avalon Biomedical (Management) Limited

Smooth installation with instant impact

"Deployment took just three days and was made easier by Barracuda's automatic configuration allowing fast license setup and connections. Once the solution went live, we saw an instant and dramatic decrease in scam traffic without any network degradation."

"Thanks to Barracuda Essentials and Barracuda Sentinel, Avalon Biomedical's network is protected against incoming and outgoing email threats, neutralising risks associated with financial loss, data leaks, and reputational damage."

Learn more about Barracuda Essentials and Barracuda Sentinel

barracuda.com/products/essentials

barracuda.com/products/sentinel

