Case Study

Heritage Bank Moves to the Cloud with Advanced Malware Protection

EXECUTIVE SUMMARY

Customer Name: Heritage Bank

Size: 800 employees, 300,000 members

Industry: Financial Services

Location: 61 branches in Queensland with a presence in every state and territory in Australia

"Since we deployed AMP for Endpoints integrated with Threat Grid, and soon AMP for Networks, we definitely sleep easier now. It only takes one computer somewhere in the world to get compromised by a malware variant, and the instant Threat Grid detects it, the rest of the fleet is protected."

Lachlan Peters
Security Team Leader, Heritage Bank

As Australia's largest customer-owned bank, Heritage Bank has been putting "people first" (its motto) since 1875. The bank was formed in 1981, a result of the merger of two century-old building societies that focused on pooling funds to finance building houses for members. With no shareholders to cater to, profits are reinvested in Heritage to deliver great products, great rates, and great service.

"People first" is more than a motto. It's a mindset that permeates the bank and its culture, extending to how Lachlan Peters, Heritage Bank's Security Team Leader, views security.

"Looking after our members includes giving them the freedom to pursue their goals without having to worry about their livelihood, which means we are continuously modernizing security in lockstep with the products and services the business must offer," said Peters. "We were using traditional protection solutions, but with a rise in cloud-based solutions, email, and collaboration, these solutions weren't able to fill security gaps across the board."

Peters explained that Heritage's security methodology had traditionally been built from a brick and mortar viewpoint – strong walls to keep the bad guys out, with more free rein once inside.

However, with the advent of encrypted traffic and advanced attacks, Peters and his team needed increased visibility to gain the full protection they were looking for.

"The prevalence of cloud solutions, SaaS, and web-based apps is leading to a greater use of encryption to keep others from seeing traffic in transit, but our security solutions couldn't see it either, which was a problem," explained Peters. "Another challenge is that our employees tend to get targeted by a fair amount of phishing and spear-phishing campaigns, and there are always the zero-day attacks. Signature-based security isn't sufficient to detect and stop these kinds of threats."

With Cisco AMP for Endpoints and Threat Grid, Heritage Bank can:

Save two man-days per month manually reviewing suspicious emails.

Securely transition to the cloud and SaaS with greater confidence.

Seeking protection against advanced persistent threats, Heritage engaged in an evaluation process that included solutions from FireEye and Cisco.

"We found that Cisco AMP for Endpoints with Threat Grid built-in provides continuous endpoint security – blocking threats outright, but also monitoring, heuristics, and sandboxing to get the full protection we were looking for," says Peters. "Cisco's solution was more well-rounded, and, as a security institution, Cisco emphasizes integration with its other solutions, like AMP for Networks, and it's all backed by threat intelligence from Talos. This ability for various solutions to all talk together is mutually beneficial. Other solutions don't have the same visibility across the progressive threat plane."

Securely Enhancing the Business

Since deploying Cisco® AMP for Endpoints and Cisco Threat Grid, Peters and his team have seen both business and security enhancements.

"AMP for Endpoints has increased our confidence level, which has allowed us to relax some of our more traditional gateway solutions that were impacting business processes, specifically delaying the processing of emails," said Peters. "AMP for Endpoints has a very high success rate in identifying malicious files, and also, on the flip side, a very low false positive rate. Knowing this, we've been able to save two man-days right away because we don't have to review emails manually, which is significant for our three-person team."

Heritage is also able to better protect against advanced threats that previously could evade other layers of protection and dupe unwitting users.

"Last year there was an influx of macro-enabled word docs that traditional signature-based solutions couldn't keep up with. All they have to do is make a slight change to their ciphers so that the signature doesn't match and the threat gets through," says Peters. "AMP for Endpoints is catching these types of attacks and filling in a gap that other layers of security, like our gateway and other endpoint solution, couldn't."

User education is always a challenge and phishing and spear-phishing attacks rely on users clicking on malicious links and attachments. But according to Peters, AMP for Endpoints has been a strong last line of defense, detecting and stopping phishing scams that would otherwise make it through to the end user.

These types of threats can lead to more significant, disruptive, and costly attacks like ransomware. But for Heritage Bank, ransomware and other attacks that use social engineering are now less of an issue.

"Everyone needs to be concerned about ransomware," Peters affirms. "But since we deployed AMP for Endpoints integrated with Threat Grid, and soon AMP for Networks, we definitely sleep easier now. It only takes one computer somewhere in the world to get compromised by a malware variant, and the instant Threat Grid detects it, the rest of the fleet is protected."

Fill in security gaps, prioritize threats, and remediate faster and easier.

Security has provided Heritage with a safe way to take advantage of new technologies to run their business better.

"There is only so much a proxy server can do and there is only so much an IPS can do once traffic is encrypted on the network," says Peters. "AMP for Endpoints and Threat Grid give us confidence to support the business as users move forward with cloud-based and other solutions that are typically difficult to secure. With AMP for Endpoints, you're no longer up at night wondering if someone is out there potentially accessing things that other solutions are unable to scan or see."

Integration Breeds Success

To gain a deeper understanding of suspicious files, Peters and his team tap into Threat Grid's behavioral analysis and sandboxing capabilities.

"The output we get from the Threat Grid reports allows us to craft Indicators of Compromise (IoCs) and check firewall logs," says Peters. "It provides peace of mind – determining whether or not a file is malicious and, if it is, confirming that it is successfully blocked. Threat Grid integrated into AMP for Endpoints and AMP for Networks is a key way to stay ahead of the bad guys who are always trying to circumvent defenses; I don't know why you wouldn't have it."

To complement AMP for Endpoints, Heritage Bank is in the process of deploying AMP for Networks detect and stop threats inside the network, before they reach the endpoint.

"Now that we are starting to deploy AMP for Networks, we are seeing a real benefit in correlation between those two solutions," Peters explains. "We've been able to use AMP for Networks to detect a suspicious file, upload it to Threat Grid for analysis, and get a conviction – all before the user even gets access to the file. This takes some of the pressure off of AMP for Endpoints."

AMP for Networks also provides increased visibility to more accurately assess the impact of a threat, prioritize response, and remediate. "As we deploy AMP for Networks, it is already giving us visibility we never had before," says Peters. "In the past, we were aware of certain threats inside the network, but it was more of a hunch. With file trajectory, now we can actually see what is happening, which gives us the ability to prioritize any instances we do have. For example, we can see if a device is executing malware and is fully quarantined or if a file tried to phone home. If we have something calling out, we know where we will focus first."

With an integrated approach to advanced malware protection, Peters and his team are able to accelerate time to detection. This mitigates damage from attacks and makes remediation faster and easier.

"It has been a while since we have had to do a full rebuild on an endpoint for security purposes, which reduces impact to staff members who lose their computer while the rebuild happens, and the IT department that has to do the rebuild," says Peters.

Products and Services:

- Cisco Advanced Malware Protection(AMP) for Endpoints
- Cisco Threat Grid
- Cisco AMP for Networks
- Cisco Firepower® Management Center

Comprehensive visibility across AMP for Endpoints, AMP for Networks, and Threat Grid is provided through the Cisco Firepower Management Center. Peters explains that they now have a more complete picture of the life of the malware and deeper insights.

"By implementing command line info in AMP for Endpoints, we can even see if the malware tried to disable some security features in certain solutions. We can also simply skim through and read a list of files looking for instances of low prevalence, in which case you just click a button and it gets retrieved and runs to make sure it is all cleaned," adds Peters.

Looking Ahead to the Cloud

As Peters looks to the future, he is considering more Cisco cloud-based, integrated security solutions, such as Cisco Umbrella, a secure Internet gateway that provides a first line of defense against bad domains, URLs, IPS, and files – blocking malicious connections before they are even established.

"DNS tunneling is potentially becoming more of an issue and this kind of protection, in addition to AMP, also helps stop a piece of malware from phoning home once it is on your network. If it can't phone home, it can't encrypt anything or cause other damage," Peters adds.

Peters is also considering CloudLock, the Cisco cloud access security broker (CASB) that helps to enable the discovery and control for software-as-a-service (SaaS) apps both on and off the network.

"With traditional IT relinquishing control to the business that is opting for more SaaS solutions, a CASB is a must-have moving forward," says Peters. "To allow for the same peace of mind we get from Cisco AMP and Threat Grid, we need oversight to make sure the business isn't accidentally ticking a box that makes everything available."

Continuing to stay ahead of the needs of its members and the business while delivering protection against advanced threats is what motivates Peters and his team.

"We are always doing our best to be on the front foot and offer unforeseen protection to our customers," says Peters. "There is a like mindedness across Cisco, and its size and ability to deliver an integrated, security architecture means the value we get is greater than the sum of its parts. It's a big win when you can benefit from shared intelligence across platforms."

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices**.

C36-738831-00 04/17