BlackBerry
Intelligent Security. Everywhere.

Case Study

Reece Group Deploys BlackBerry Solutions To Protect Endpoints and Automate Threat Management

A Day in the Life

A plumber walks into one of Reece Group's 800 branches in Australia, New Zealand, or the United States to purchase supplies. The sales associate sits them down at a point of sale terminal and helps them search through an inventory of 80,000 parts for the items they need. Delivery and tracking information are produced if the goods will be trucked to the customer's worksite. Selected items are flagged for replenishment based on data mining rules that reflect previous purchasing trends. And thanks to the suite of specialized applications and digital tools Reece Group developers built to perform these functions, the whole process proceeds seamlessly and securely.

As head of security, Shane Laffin is responsible for protecting Reece's business-critical applications and information technology (IT) infrastructure from cyber attacks. "Our customers are at the center of everything we do, which means we take data integrity and cybersecurity very seriously," he says. "We're always looking at the market, assessing what's out there. It's a changing landscape. You can't rest on your laurels."

Reece Group

Industry:
Plumbing Distribution and Retail

Location:
Burwood, Australia

Products:
BlackBerry® Protect,
BlackBerry® Optics

Deployment:
10,000 endpoints

Website:
www.reecegroup.com.au

reece group™

Established in 1920 and listed on the Australian Securities Exchange, Reece Group is a leading distributor of plumbing, waterworks, and HVAC-R products to commercial and residential customers. The company has approximately 7,000 employees committed to improving the lives of their customers by striving for greatness every day.

Although it recently celebrated its 100th birthday, Reece Group is constantly innovating to stay competitive and pursue management's international growth strategy. "The 2018 acquisition of MORSCO accelerated our plans to enhance our cyber resiliency by reducing the complexity of our security stack, upgrading from our signature-based defenses, and streamlining endpoint security management," says Laffin. "We reached out to Cylance[1] partner CyberRisk for assistance."

Prior to co-founding CyberRisk, Director Leong Wang was among the first CylancePROTECT®[2] customers in the Australian region. "As early adopters of AI-based endpoint defenses, we understood the technology very well," says Wang. "Therefore, we were well-positioned to help Reece Group with its proof-of-concept planning."

The Proof Is in the Testing

Laffin and his team spent July and August of 2018 conducting paper-based assessments before inviting Cylance and two other firms to submit their endpoint protection, detection, and response solutions for a month of in-depth proof of concept (POC) testing.

"We began the POC by exposing the candidate solutions to 200 different malware strains to baseline their capabilities for malware detection and pre-execution prevention," says Laffin. "CylancePROTECT stopped all of them." Next, the solutions were exposed to attack simulations that utilized the APT29 tactics, techniques, and procedures (TTPs) documented in the MITRE ATT&CK® framework. "The MITRE ATT&CK simulation tests were eye-openers," says Laffin. "CylancePROTECT and CylanceOPTICS®[3] excelled over the other products we were considering. Their performance was exceptional."

Other tests focused on resource utilization. "It can be frustrating for employees when a scan or a signature update makes their system run sluggishly," says Laffin. "The Cylance solution was much more efficient with system resources than our legacy AV. It ran quietly in the background, protecting endpoints without making a fuss or requiring a cloud connection to function."

Laffin also assessed the candidate solutions for management efficiency. "Simplicity is important to me," he says. "The Cylance console[4] is extremely straightforward and easy to operate. I could immediately see that the learning curve would be a short one."

Management flexibility was another important consideration. According to Laffin, "We knew it would take months to integrate MORSCO's security infrastructure in the United States with our security systems and policies in Australia and New Zealand. During the build out, we'd want to manage our entire IT infrastructure from

> "The MITRE ATT&CK simulation tests were eye-openers. CylancePROTECT and CylanceOPTICS excelled over the other products we were considering. Their performance was exceptional."
>
> *— Shane Laffin, Information Security Manager, Reece Group*

a single pane of glass while monitoring security incidents in the two environments separately. Therefore, the option to deploy the Cylance console in a multi-tenant cloud configuration was especially attractive to us."

Ultimately, however, it was the experience and dedication of the Cylance and CyberRisk teams that convinced Laffin to invest in Cylance solutions. "It's always wise to surround yourself with people who are both technically astute and trustworthy," says Laffin. "I felt certain that our relationship with Cylance and CyberRisk would be a productive one."

In March 2019, Reece Group became a Cylance customer. The CylancePROTECT deployment kicked off soon afterwards.

A Two-Stage Deployment

Although he was confident that Reece's security and infrastructure teams would be able to implement both solutions successfully, Laffin decided to engage CyberRisk in the pre-deployment planning process. "CyberRisk advised us on the best practices for creating CylancePROTECT security zones and policies," says Laffin. "That saved us a lot of time and effort when we began scanning the environment and enabling security controls."

Within two months of deploying Cylance's unified agile agent technology, Laffin and his team had CylancePROTECT security controls for malware prevention, memory exploit protection, script control, device usage control, and application control enabled in full blocking mode. "Once we achieved that milestone, we were ready to begin operationalizing CylanceOPTICS," says Laffin.

During the POC, Laffin had envisioned numerous possibilities for incorporating CylancePROTECT and CylanceOPTICS into Reece's automated threat management program. "We already knew we'd be able to extract and load CylancePROTECT endpoint telemetry data into our LogRhythm® SIEM without much effort, since the two products had been integrated three years before[5]," says Laffin. "We began exploring ways to utilize CylanceOPTICS playbooks and MITRE detection rules to contextualize that data and assist with response and remediation."

"CylanceOPTICS can initiate a wide variety of automated response workflows, ranging from collecting and forwarding endpoint telemetry data to taking systems offline," explains Jason Duerden, Managing Director, BlackBerry Spark, Australia, and New Zealand. "Workflows can be triggered by our AI-based Context Analysis Engine (CAE) models, by custom rules defined by the customer, and by rules that leverage MITRE TTPs of advanced persistent threats. Often, detection rules don't fire at all because CylancePROTECT has already stopped an attack by preventing malware, or fileless threats from executing in the first place."

> "The Cylance solution was much more efficient with system resources than our legacy AV. The solution ran quietly in the background, protecting endpoints without making a fuss or requiring a cloud connection to function."
>
> — *Shane Laffin, Information Security Manager, Reece Group*

Author's note: Click here to learn how the prevention-first approach to cyber defense made possible by BlackBerry® Protect, BlackBerry® Optics, and BlackBerry® Guard was validated by a recent MITRE ATT&CK APT29 Evaluation.

Although security upgrades are ongoing, Reece Group has completed its transition to a proactive, prevention-first security posture. "Cylance has proven it can successfully address all of our endpoint protection, detection and response requirements from a security, operations and design perspective," says Laffin. "By automating and streamlining threat management, they've enabled us to scale and support our growing global business."

"Together with our channel partner, CyberRisk, BlackBerry is proud to have helped Reece Group transition successfully from a traditional AV model to an AI-driven, preventative approach to threat management," adds Duerden. "We're confident Reece Group is well-protected against both current and emerging threats."

> "It's always wise to surround yourself with people who are both technically astute and trustworthy. I felt certain that our relationship with Cylance and CyberRisk would be a productive one."
>
> — *Shane Laffin, Information Security Manager, Reece Group*

1 BlackBerry completed its acquisition of Cylance on February 21, 2019

2 CylancePROTECT® is now known as BlackBerry® Protect

3 CylanceOPTICS® is now known as BlackBerry® Optics

4 The Cylance console is now known as the UES console

5 Cylance® Expands Cyberattack Visibility through Integrations with Robust Ecosystem of Leading SIEM Technologies

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 150M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

For more information, visit BlackBerry.com and follow @BlackBerry.

BlackBerry
Intelligent Security. Everywhere.

BB20-CMAS | 200708