CASE STUDY

High-Growth FinTech Company Unifies View of Cyber Risk

> *"Tenable.io has unified our vulnerability management program under one tool set. It's brought together teams across different business units to use a common language around vulnerability posture. The solution is easy to use and streamlines our reporting!"*

PATRICK KING
Head of IT Operations & Security

ORGANIZATION SNAPSHOT

COMPANY
Global Payments AU/NZ, a division of Global Payments Inc.

NUMBER OF LOCAL EMPLOYEES
300

NUMBER OF BUSINESS UNITS
4

INDUSTRY
Financial Technology

CHALLENGES

- Difficulty establishing one comprehensive view of Cyber Exposure across new acquisitions, including both traditional and modern IT assets
- Simplify reporting and communication of data-driven insights
- Quickly onboard new organizations with minimal overhead
- Efficiently deliver on PCI and internal audit requirements

SOLUTION

tenable.io

IMPACT

- Peace of mind with improved visibility across critical and user assets
- Streamlined vulnerability management across all business units
- Saved hours of time with actionable dashboards and low touch administration
- Increased efficiency in meeting compliance standards

GLOBAL PAYMENTS AU/NZ, A DIVISION OF GLOBAL PAYMENTS INC.

Global Payments AU/NZ is a division of Global Payments, Inc., an industry-leading payment processing and software organization undergoing worldwide growth. In Australia and New Zealand, Global Payments operates Ezidebit, eWAY, Storman and Sentral, all of which are expanding their services in high-growth industries such as alternative finance, insurance and equipment rentals.

As the parent company acquires new organizations in Australia and New Zealand – each with different cyber risk profiles and technologies – its IT and cybersecurity teams must quickly onboard the organizations and assess risk across a complex IT landscape.

The local cybersecurity team is responsible for protecting personally identifiable information (PII) as well as the valuable credit card data the software and payment processing organizations manage. They also need to assess internal networks and workstations to identify and remediate security issues.

CHALLENGES

As the organization grows its cyberattack surface is quickly changing and expanding.

Patrick King, head of IT operations and security for Global Payments' local brands in Australia and New Zealand, oversees cyber risk across four local organizations currently, each with different risk profiles and diverse IT environments.

King and his team of 30, focus on remaining agile and efficiently managing cyber risk across their business units. King explains, "When a new acquisition comes on board, it's a whole new environment and a whole new team of people. The systems are running in different cities, different data centers, and at times in different cloud environments." The team required a flexible solution to address the following challenges:

- **Difficulty establishing one comprehensive view of Cyber Exposure across new acquisitions, including both traditional and modern IT assets**
  The team needed to quickly identify and manage risk across traditional assets (e.g., Windows and Linux servers) and payment processing systems. They also needed to protect user endpoint devices, web applications and cloud-based environments.

  King says, "Our attack surface is changing, we're migrating more and more workloads into the public cloud. We need a solution that scales across public cloud and at the same time integrates with data centers."

  King explains, "Each business unit was using different security tools to manage their cyber risk. We weren't really feeling comfortable that we were getting the full picture of what was going on in all the internal environments. We were getting different reports out of different tools, and results meant different things depending on the business unit." He says, "It wasn't apples to apples when we were looking at metrics and comparing our position across the business. We needed a solution that provided an accurate, consolidated picture of our Cyber Exposure."

- **Simplify reporting and communication of data-driven insights**
  King's team needed to easily obtain and deliver vulnerability performance data to their head office. They required flexible, customizable reporting and intuitive dashboards that enable the team to quickly assess risk across all business units.

- **Quickly onboard new offices with minimal overhead**
  The team had limited resources for configuration and administration and needed an easy way to onboard new office sites around the world. King reflects, "It was important to us to have a cloud-based solution that we could deploy quickly, and get it across our environments easily."

- **Efficiently deliver on PCI and internal audit requirements**
  The team needed to meet stringent Payment Card Industry Data Security Standard (PCI DSS) audit requirements. They also had to adhere to internal audit requirements, reporting the vulnerability status for all business units up to the head office monthly.

SOLUTION

King and his team had experience with products from both Tenable and Rapid7. They evaluated these solutions and selected Tenable.io for several reasons:

- **Full visibility across both traditional and modern assets**
  King and his team now have full visibility into a complex attack surface thanks to Tenable.io's wide variety of data collection technologies. Nessus sensors within Tenable.io provide active and agent scanning to accurately identify assets and assess their environment for vulnerabilities. King prefers the use of agents to collect as much data as possible about known assets and uses scanners to assess the rest of the environment.

  Additionally, they are well-positioned for growth as the businesses move more and more workloads to public cloud environments.

- **Flexible reporting and real-time dashboards**
  Tenable.io's intuitive reporting and actionable dashboards give King the consolidated, easy-to-communicate insights they need to reduce cyber risk, and provide monthly updates to the head office. King mentions, "The flexibility we have in reporting is really impressive. It has saved our team hours of time. We are able to quickly build several custom reports that we just couldn't do in other products."

- **Cloud-managed Tenable.io provides a consolidated picture of cyber risk**
  King mentions, "Because Tenable.io is cloud-managed, our business units can upload data to a central location quite easily. The networking we would have to do with other products to get a similar operation is just not feasible."

  Each business unit now easily manages its cyber risk using the same Cyber Exposure platform, providing King and his team consistent metrics and an accurate, comprehensive picture of their attack surface. Additionally, they rely heavily on vulnerability risk scores and prioritization guidance provided by Tenable.io.

- **Easy set-up and deployment across all business units**
  "A key need for us was the ability to roll this solution out everywhere, easily. We knew that pulling out our existing tools and deploying a new solution was going to be a really big job," explains King.

  He continues, "We went through the pilot with Tenable.io and it was very, very easy to roll out. We got it up and running really quickly. Everything seemed to just work. For a team with limited resources that is really important to us. We can spend our time in the right areas, securing our assets and networks."

  King and his team also found it easy to work with the Tenable sales team. They helped get a working proof of concept set up within the short timeframe required.

- **Efficiently deliver on PCI and internal audit requirements**
  Tenable's pre-built templates allow King's team to assess and report on PCI compliance requirements and internal audits efficiently.

IMPACT

- **Peace of mind with improved visibility across traditional and modern assets**
  They have broad coverage and comprehensive visibility across their new and changing assets, with increased confidence all of their assets are being scanned and actively monitored.

- **Streamlined vulnerability management across all business units**
  With a single view of their full cyber risk across multiple environments, the team is able to accurately identify, investigate and prioritize vulnerabilities. Each organization is using the same product and metrics to monitor their environment.

  King says, “Tenable.io has unified our vulnerability management program under one umbrella, and one tool set. It’s brought together different teams across different companies. It’s easy to use and really streamlines our reporting.”

- **Saved hours of time with actionable dashboards**
  With Tenable.io’s intuitive dashboards and customizable reporting, they have saved hours of time creating reports and assessing threats. They can quickly deliver comprehensive updates to the head office.

- **Increased efficiency in meeting compliance standards**
  The team saves time preparing for both internal and external audits, and is able to focus resources on securing their assets and networks.

CONCLUSION

King and his team now have one Cyber Exposure platform, empowering them to effectively manage a constantly changing attack surface. Cloud-managed Tenable.io enables King's team to easily onboard new organizations – contributing to the strategic growth of the business.

Partnering with Tenable, King and his team plan to continue elevating their vulnerability management program to reduce cyber risk. What's next? They want to automate their service management processes with Tenable.io's easy-to-use APIs, and are looking forward to new capabilities included in the Tenable product road map.

To learn more visit tenable.com | Contact Us: marketing@tenable.com