

Case Study: *POINTS*BET

Reinventing employee device security for better protection from cybercrime, end user experience and efficiency outcomes

When PointsBet accelerated its global growth within the high-risk, highly regulated and very competitive online gambling industry, they knew they needed to completely rethink their approach to employee device enablement. In 2019 PointsBet adopted Device, a cloud-based solution which has reinvented device security, quickly lifting their security maturity, providing a fantastic employee experience and gaining massive efficiency outcomes for the business.

The IT team now spends almost no time solving employee device issues, leaving them to focus on more strategic security and IT challenges to help drive PointsBet's stellar global growth and success.

**Easier employee onboarding**

New employee device deployment reduced from several days to 30 minutes, and no longer needs any hands-on IT assistance.

**Improved IT team productivity**

Employee numbers have grown by 400% but the IT support staff by only 20%.

**Positive end user experience**

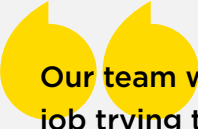
Over the past 12 months there have been no IT service desk requests about device management or security, despite onboarding hundreds of new employees.

**Uncompromising device security and compliance**

All on-going patching of employee devices, operating systems and applications, plus configuration of settings, now takes place automatically and optimally, without any human or agent involvement.

The Company

PointsBet is a fast growing, Australian-owned, ASX-listed corporate bookmaker, offering innovative sports and racing betting products and services direct to clients via its scalable cloud-based technology platform. Founded in 2015, PointsBet has achieved rapid growth to become the fourth largest bookmaker in the US with over 500 employees globally and expectations to reach 1000 by the end of 2021.



Our team were doing a great job trying to keep on top of deploying critical security updates, but it's a time-consuming process and the downtime was disruptive to our employees," said Head of Technology, Andrei Goutnik. "We knew we needed to rethink the way we were approaching this challenge if we were to achieve our ambitious expansion targets across the US.



The Challenge

The online gambling industry is an attractive target for cyber criminals, with 2020 seeing significant increases in DDoS and ransomware attacks. As a fast-growing company in a high-risk industry, PointsBet has complex security and compliance regulations as they rapidly expand their global presence. Establishing new offices and onboarding new employees in different territories became a constant requirement, and something the company needed to find a way to do more securely, efficiently and with a more positive end-user experience. Head of Technology for PointsBet, Andrei Goutnik, said that the rapid and distributed company expansion meant it had become unsustainable for the IT team to manually set up every machine, ship it to new hires and maintain compliance across everyone's devices.

PointsBet needed an employee device solution that could keep pace with the company's hyper-growth while meeting complex compliance requirements and demonstrating a high level of security maturity, as well as keeping its employees happy and productive.



The Device solution

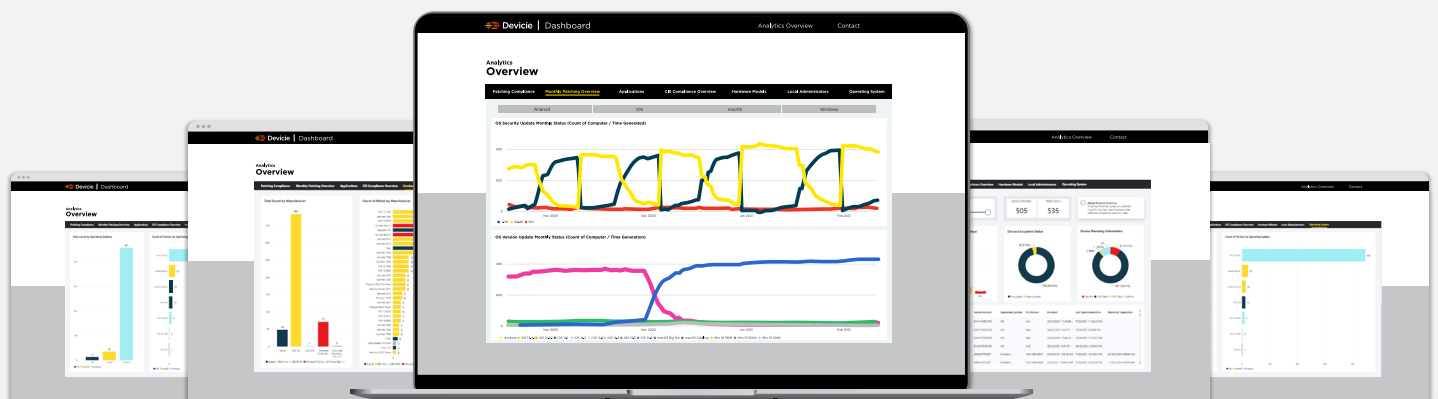
Device's solution quickly helped PointsBet to streamline their device security and management by establishing an automated Standard Operating Environment (SOE) via the MS Cloud. By deploying Device across all employee devices, all provisioning, packaging and on-going patching of devices, operating systems and applications, plus the configuration of settings, now takes place automatically and optimally, without any human or agent involvement.

PointsBet was an early adopter of Device and worked with the founding team to design, build and optimise the PointsBet SOE in the Device platform.

PointsBet had some specific operational issues and complex roles that needed to be captured and prioritised in the production environment.

This included:

- ✓ A range of new and old devices with various operating systems, different configurations, bespoke software and version conflicts
- ✓ Remote onboarding and urgent deployment of devices to a fast-growing global workforce
- ✓ An uncompromising deployment schedule of critical security patches and application updates to meet industry compliance regulations and improve PointsBet's security posture
- ✓ Minimise disruption to employee devices to maintain their productivity



Furthermore, the set-up and roll-out of Devicie's solution must not disrupt day-to-day IT and employee operations.

PointsBet opted to support five main device models rather than go fully BYOD and wanted to achieve significant measured improvements in their security posture, operational efficiency and employee experience through their Devicie roll-out.

The production validation process with PointsBet took four weeks, however, Devicie has advanced its process and is now able to complete this same process for other customers in two weeks.



The onboarding process was so simple that it felt too good to be true! Devicie's functionality was way ahead of other technologies.

Production validation included understanding and applying PointsBet pre-requisites, testing the platform with the development team, who have the most complex role and device requirements.

Andrei said the test was a resounding success with positive feedback from the development team about significantly reduced time to onboard and deploy security updates, an increased level of security, as well as the ease of access for employees via any internet connection. Further, the team noted a much better user experience.



Website

devicie.com

LinkedIn

au.linkedin.com/company/devicie