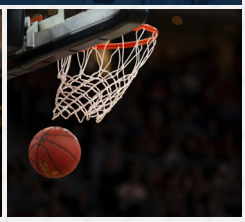

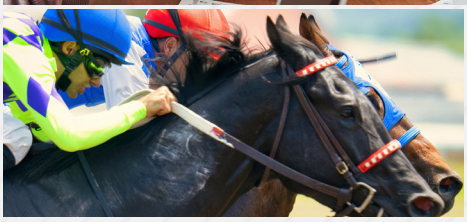

Tabcorp

Tabcorp Partners with CrowdStrike to Drive Stronger Security from Endpoint to Cloud

Tabcorp is an Australian betting and entertainment experiences business operating across three main brands: TAB, Australia's biggest multichannel wagering brand; Sky Racing and Sky Sports Radio, which broadcast racing and sports programs and expert analysis; and MAX, Australia's leading gaming services provider. The company uses cutting-edge technology to create exciting, immersive social experiences for its customers and is constantly exploring how to continually innovate and sustainably grow its business.

In addition to protecting its corporate assets and services, Tabcorp's primary concern is for the safety and financial protection of its customers and their data. The company has a strong focus on sustainability to ensure all wagering and gambling activities happen in a responsible manner. Tabcorp proactively ensures customers have an integrated entertainment experience that is safe from both cyberattacks and the potential harms of gambling.

"Our customers think about Tabcorp the same way they see their bank, trusting us with their identity, money and financial information," said Himanshu Anand, Head of Cyber Threat Management at Tabcorp.

The biggest threat to Tabcorp is cybercriminals. However, a range of state-based, criminal and opportunistic threat actors target Tabcorp, and its defenses must continue to evolve and improve to stay ahead of new threats.

To protect its customers and systems, Tabcorp's cybersecurity team works with third-party security providers. Its relationship with CrowdStrike was first established in 2020, when Tabcorp selected CrowdStrike's endpoint protection platform.

"After a review and evaluation of four different solutions, we selected CrowdStrike on the basis of its lightweight agent, its multiple operating system support and the fact we could deploy and integrate it with other capabilities," said Mick McHugh, CISO, Tabcorp.

Building Trust and Business Context

Tabcorp's implementation of CrowdStrike Falcon® Complete managed detection and response extends beyond physical endpoints to its cloud infrastructure using CrowdStrike Falcon® Cloud Security. More recently, Tabcorp incorporated CrowdStrike Falcon® Intelligence and CrowdStrike® Falcon OverWatch™ for threat intel and threat hunting.

The CrowdStrike threat intelligence team keeps Tabcorp up-to-date on current and emerging threat actors, cybercriminal motivations and regions of operation, and the latest techniques being used that represent significant risks to Tabcorp. This provides Tabcorp with invaluable information on what it needs to protect against and how to tackle those threats.

Tabcorp also uses CrowdStrike Falcon® Intelligence Recon+ to monitor the deep and dark web for any leaked credentials from corporate users, Tabcorp brands or customers. This ensures Tabcorp can act quickly to reduce the threat posed by potentially compromised credentials.

In addition, Tabcorp has retained CrowdStrike's Incident Response Services to be ready to respond rapidly and work collaboratively with the SOC to handle critical security incidents.

"We expanded our relationship with CrowdStrike to get better visibility on who the threat actors are that are targeting us and to build out our understanding of dark web activity and threats," said McHugh. "The

INDUSTRY
Gaming/Media

LOCATION/HQ
Melbourne, Australia

CHALLENGES
- Complex hybrid environment with business undergoing significant cloud migration
- Regular, rapid escalations in business due to seasonal activity raising risk and impact level
- Critical requirement to protect users, their financial data and wagering systems

SOLUTION
Initially chosen to replace a legacy endpoint protection solution for existing on-premises infrastructure and to support Tabcorp's cloud migration program, CrowdStrike now provides comprehensive managed detection and response, threat intelligence and threat hunting capabilities, operating in collaboration with Tabcorp's SOC. The partnership is delivering assurance to Tabcorp's board and executive management team, and ensuring the trust of its customers.

RESULTS
- Comprehensive endpoint protection across a hybrid cloud and on-premise environment
- Greater visibility and control across endpoints, and proactive threat and risk insight
- Security services and security platform that can scale and adapt to an aggressive cloud migration strategy and peaks and troughs with seasonal business activity

"Our customers think about Tabcorp the same way they see their bank, trusting us with their identity, money and financial information."

Himanshu Anand,
Head of Cyber Threat Management, Tabcorp.

integration of the different services with CrowdStrike means that we can leverage multiple capabilities at the same time. The fact that the endpoint detections are linked up to our threat intel means the team looking at the alerts are the same people who can give us advice on recon and what we need to do to remediate things."

"CrowdStrike is one of our main security partners, and we trust the Falcon Complete and Falcon OverWatch teams completely," said Anand. "They have become an extension of our team in monitoring our systems, alerting us of any anomalous behaviour and containing any attacks right away. By providing us with 24/7 visibility and eyes on glass, CrowdStrike enables our team to look further into threats from the business context."

Tabcorp and CrowdStrike teams regularly interact and share feedback. Ongoing collaborative sessions enable Tabcorp to provide feedback to continually enhance the service and optimize protection.

"CrowdStrike has introduced product improvements based on the feedback we were providing them," said Anand. "When CrowdStrike sends us an alert, they now tell us whether it's the first time they've seen this or if they've seen this previously. Now, we don't have to check the same user every time we get an alert, and we'll know that we've already fixed the issue."

CrowdStrike helps Tabcorp identify users with anomalous behavior, allowing Tabcorp to discover if it is a true insider threat, an external threat actor or a user who has done something inadvertently.

Protecting the Cloud

Tabcorp has been undergoing a significant cloud migration. The first step is transitioning its on-premises infrastructure to the cloud.

"Cloud is a big part of our future," said McHugh. "CrowdStrike has given us the security baseline patterns we need to have to make sure that as we move into the cloud, the infrastructure that we are setting up is secure from the outset."

The extension of Falcon Cloud Security's cloud security posture management (CSPM) is ensuring Tabcorp has greater visibility and control to prevent potential misconfigurations from causing harm.

"CrowdStrike's cloud runtime protection means we are able to leverage the power of the cloud to execute this protection and detection at scale," said Anand. "Alerts get correlated very quickly in the cloud, and we only have to deal with high-fidelity escalations.

"We also use several CrowdStrike-supported technologies," he added. "That gives us an integrated environment from a threat perspective, with higher levels of automation and efficiencies as well."

Moving to Business-Centric Cybersecurity

Tabcorp is excited to move from an asset-centric model to true business-centric cybersecurity. From a technology perspective, this means increasing Anand's team's proactivity in managing the business's attack surfaces and a more holistic approach to protecting identity. This allows his team to better support Tabcorp's growth into new lines of business. It also enables his team to scale or manage heightened risk when needed, such as in the lead-up to the Melbourne Cup, one of Australia's most prestigious horse races.

This includes using CrowdStrike to produce special Spring Racing Carnival threat reports, ensuring the Falcon Complete team is on high alert and looking for any suspicious or anomalous activity during the SRC. During the event, Tabcorp also has an incident response service on retainer for additional support if needed.

"Our executive leadership team and board are very supportive of cybersecurity and aware of its importance to the trust placed in us by our customers and employees," said McHugh. "Our roadmap is to take a risk-driven approach so the business can look at cybersecurity not just as a cost center but as a revenue center as well."

Start Free Trial

Learn more **www.crowdstrike.com**

ENDPOINTS

10,000

CROWDSTRIKE PRODUCTS

- CrowdStrike Falcon® Complete managed detection and response
- CrowdStrike Falcon® Discover IT hygiene
- CrowdStrike Falcon® Insight XDR Endpoint Detection and Response (EDR)
- CrowdStrike® Falcon OverWatch™ managed threat hunting
- CrowdStrike Falcon® Intelligence
- CrowdStrike Falcon® Intelligence Recon+
- CrowdStrike Falcon® Prevent next-generation antivirus
- CrowdStrike Falcon® Cloud Security
- Incident Response Services

"Cloud is a big part of our future. CrowdStrike has given us the security baseline patterns we need to have to make sure that as we move into the cloud, the infrastructure that we are setting up is secure from the outset."

Mick McHugh

CISO, Tabcorp

ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data. Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

CrowdStrike: **We stop breaches.**

Follow us: **Blog** | **Twitter** | **LinkedIn** | **Facebook** | **Instagram**

CROWDSTRIKE

we stop breaches