CYBOTS

CYBER THREATS DON'T SLEEP. **NEITHER DO WE.**

CASE STUDY

SECURING A CONNECTED GLOBAL ENTERPRISE

Strengthening security visibility across a complex and constantly evolving digital landscape.



CYBOTS
CYBER THREATS DON'T SLEEP. NEITHER DO WE.

ONE SECURITY VIEW ACROSS A GLOBAL ENVIRONMENT

Bringing greater visibility and control to a complex, distributed digital ecosystem.

Client Background

A leading insurance provider in Malaysia operates across a broad portfolio of digital services, including customer-facing web platforms, mobile applications, and backend systems supporting policy management, underwriting, and claims processing.

Operating in a highly regulated environment, the organization is responsible for safeguarding large volumes of sensitive personal and financial data; making it a prime target for cybercriminals and fraud-driven attacks.

Industry Context: Why Insurance Is a High-Value Target

The insurance sector has become increasingly attractive to threat actors due to:

- High-value data (personal, financial, medical records)
- Complex digital ecosystems spanning multiple applications and APIs
- Frequent third-party integrations increasing attack surface
- Regulatory pressure requiring continuous validation of security posture

Modern attacks in this sector are no longer isolated. They are multi-stage and financially motivated, targeting identity systems, APIs, and customer data flows, often remaining undetected until significant damage is done.



The Operational Problem

The organization faced the challenge of securing a rapidly expanding and highly distributed digital environment:

- Hundreds of web and mobile applications
- Extensive IP address exposure
- Wireless and internal network dependencies

Despite ongoing security efforts, visibility into vulnerabilities was fragmented. There was no unified view of risk across the entire digital estate, making it difficult to:

- Prioritize remediation
- Understand true exposure
- Ensure readiness against sophisticated threats

THE CYBOTS APPROACH:

Security at Scale, Driven by Real Risk

Cybots approached the engagement as a comprehensive security validation program, not a standalone testing exercise.

A dedicated team of security consultants executed parallel assessments across the organization's digital footprint, ensuring both depth and scale.

Scope Covered:

- 50+ mobile applications
- 200+ web applications
- 1000+ IP addresses
- Wireless networks

Execution Timeline

Cybots deployed a structured, multi-phase approach:

Asset Discovery & Mapping

Identifying all exposed and internal assets across the environment

Vulnerability & Exploit Testing

Simulating real-world attack scenarios across applications, APIs, and infrastructure

Correlation & Risk Prioritization

Connecting findings across systems to identify critical attack paths

Actionable Reporting

Delivering clear, prioritized remediation aligned to business impact

A team of six consultants worked in parallel to ensure full coverage while maintaining consistency in methodology and reporting.



Outcome

The organization achieved complete visibility into vulnerabilities across its digital ecosystem—moving from fragmented insights to a unified, risk-based understanding of its security posture.

Key outcomes included:

- Identification of critical vulnerabilities across multiple layers
- Clear prioritization of remediation efforts
- Improved understanding of real-world attack paths



Business Impact

The engagement enabled the organization to transition from reactive vulnerability management to proactive risk control:

- Strengthened protection of sensitive customer and financial data
- Improved resilience against identity-driven and application-layer attacks
- Enhanced ability to meet regulatory and audit requirements
- Greater confidence at the leadership level in security readiness

