Golden Insurance Brokers Strengthens Cyber Resilience with Radware

CUSTOMER:
Golden Insurance Brokers Co.

INDUSTRY:
Insurance Brokerage

CHALLENGES FACED:

- Traditional L3/L4 firewalls unable to address modern application-layer threats
- Need to protect websites, APIs, and HTTPS-encrypted sessions
- Limited visibility into malicious bot activity and high-frequency digital transactions
- APIs connected to backend systems and sensitive personal data
- Cybersecurity talent constraints requiring scalable expert support

Overview

Golden Insurance Brokers Co. is an insurance brokerage focused on building trust as a core part of its brand and customer experience. As the company continues to improve its digital service model to support more customers, services, online interactions, APIs, and partner-connected ecosystems, cybersecurity has become an important enabler of reliable service, compliance, privacy protection, and customer trust.

To support this progress, Golden Insurance worked with CHT Security to implement a one-stop WAAP architecture powered by Radware technologies, helping reduce risk, strengthen cyber resilience, improve operational efficiency, and support its long-term digital growth following its official OTC listing on March 30, 2026.

WHY RADWARE ?

- One-stop WAAP architecture with web, API, bot, and DDoS protection
- Radware cloud security platform for stronger threat detection
- AI SOC Xpert support for faster incident response and remediation
- Managed security services delivered with CHT Security
- Improved precision, operational efficiency, and cyber resilience

Challenges

Golden Insurance needed to strengthen security for a digital business model that increasingly depends on websites, APIs, high-frequency transactions, and partner-connected ecosystems. Traditional L3/L4 firewalls were no longer sufficient to address modern attacks hidden within legitimate traffic and HTTPS-encrypted sessions.

The brokerage also needed stronger protection for websites and APIs, better visibility into malicious bot activity, and a more unified security model that could reduce management silos while supporting digital service growth.

Key challenges included:

- **Modern attacks hidden within legitimate traffic**, requiring protection beyond traditional L3/L4 firewalls
- **Threats targeting HTTPS-encrypted sessions**, creating the need for stronger visibility and application-layer defense
- **Growing exposure across websites and APIs**, including APIs connected directly to backend systems and sensitive personal data
- **Malicious bot activity**, which required better detection and control
- **Frequent updates and integration requirements**, increasing the risk of exposure across the digital ecosystem
- **Limited cybersecurity talent**, making it important to strengthen protection without overburdening internal teams
- **Need for a unified security model**, reducing management silos while supporting high-frequency digital transactions

As Golden Insurance expanded its digital services, cybersecurity became closely connected to reliable service delivery, compliance, privacy protection, and customer trust. The company needed a scalable model that could help reduce blind spots, improve visibility, and protect sensitive digital interactions while supporting continued business growth.

Solution

To address these challenges, Golden Insurance worked with CHT Security to implement a one-stop WAAP architecture combined with managed security services. The solution brought together web protection, API security, bot management, DDoS mitigation, and expert monitoring to create a more integrated defense model.

Golden Insurance also adopted Radware's cloud security platform and AI SOC Xpert to enhance threat detection, incident response, and operational efficiency. The Radware deployment reduced mean time to recovery by 95%, while AI SOC Xpert enabled incidents to be identified and remediated within minutes.

During deployment, CHT Security used a learning mode to analyze policyholder login behavior and API call frequency before moving into blocking mode. Its consulting team fine-tuned allowlists and security policy settings to reduce false positives and business disruption, helping strengthen protection while keeping cybersecurity controls largely invisible to day-to-day business operations.

Radware also successfully blocked the high-profile Log4Shell vulnerability on the first day of the outbreak, demonstrating the platform's Day Zero response capability.

Benefits

By combining CHT Security's managed services with Radware Cloud Application Protection Services and Radware AI SOC Xpert, Golden Insurance established a more coordinated security architecture across its websites, APIs, and broader digital operations.

Key benefits include:

- **Stronger website and API protection**, helping secure digital services connected to backend systems and sensitive personal data
- **Improved visibility into malicious bot activity**, giving the company better awareness of threats targeting its digital ecosystem
- **Reduced security management silos**, unifying web protection, API security, bot management, DDoS mitigation, and expert monitoring
- **Faster incident response**, with mean time to recovery reduced by 95% according to the source material
- **Minute-level incident identification and remediation**, supported by AI SOC Xpert
- **Lower operational burden**, shifting intensive monitoring and policy-tuning activities to a specialized partner
- **Reduced risk of business disruption**, supported by learning mode, allowlist tuning, and phased policy enforcement
- **Stronger compliance support**, helping reinforce the company's position as the only insurance broker in the industry to simultaneously hold ISO 27001, ISO 27701, and BS 10012 international certifications

This approach enabled internal teams to focus more on innovation and digital business priorities while maintaining a stronger foundation of trust for customers and partners.

Conclusion

By working with CHT Security and adopting Radware Cloud Application Protection Services and AI SOC Xpert, Golden Insurance strengthened cyber resilience across its digital service ecosystem while reducing operational pressure on internal teams. The combined WAAP and managed-services model improved protection for websites, APIs, bot activity, and DDoS threats, while also supporting incident response, compliance, privacy protection, and customer trust.

As Golden Insurance continues strengthening its ecosystem-based security model, future priorities include improving visibility into open-source component risks, maintaining security standards for third-party API partners, and exploring additional monitoring capabilities to support long-term business resilience.

To learn more about how Radware Cloud Application Protection Services and AI SOC Xpert can safeguard your organization's web applications, APIs, and digital services

Contact Radware

RWI6416 | 07.09.2026