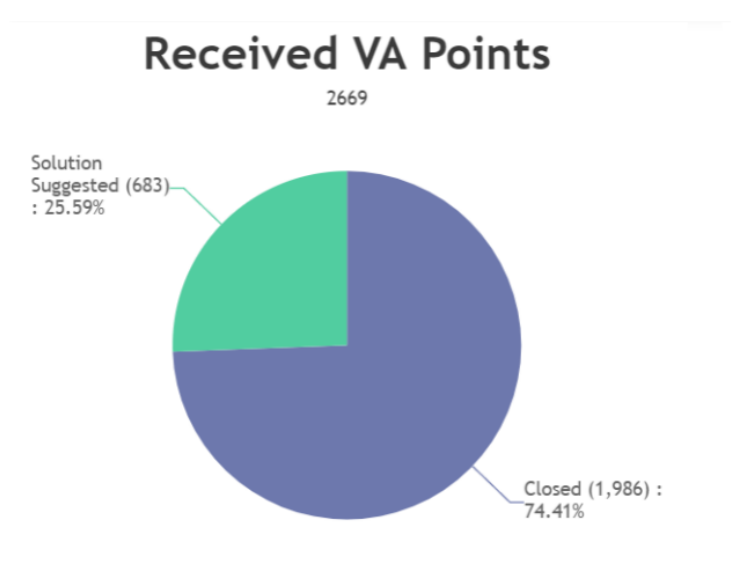
Infopercept races to patch thousands of vulnerabilities, saving top Indian insurer from cyber crisis

About the customer

- One of the most trusted life insurance companies in India.
- Serves individual and group customers through its range of products, including protection, savings, pension, and health solutions.
- With over 1000 offices, 20K+ employees, 200K+ agents, 40K partner branches, and 70+ corporate agents, the client has an ecosystem spanning India.

- Resolved 2669 vulnerabilities identified through VA and EPT methodologies
- Patched 75% of the vulnerabilities
- Created 15 PoCs to patch vulnerabilities in critical apps in the production environment



The client is a trailblazer in the insurance industry, leveraging cutting-edge technologies and customer-focused digital solutions to serve a diverse customer base across India. To establish a cyber-safe ecosystem for its customers and to meet compliance requirements, the client carried out offensive security practices, including Vulnerability Assessment (VA) and Exploit Penetrating Testing (EPT) regularly through cybersecurity solution providers. The testing identified over 2600 vulnerabilities, but none of the existing partners had the end-to-end capabilities to resolve them. This left the client's internal and external apps wide open to escalated attacks from cyber adversaries. Regulatory pressure mounted. To avert disaster, the client urgently sought a partner with expertise in development, security, and patching. It quickly identified Infopercept as having this unique trifecta of capabilities. The Infopercept team speedily patched most of the vulnerabilities and provided PoCs for a few vulnerabilities in critical apps in the production environment, setting up a robust foundation for long-term patch management.

Summary of IT, OT, and security infrastructure requirements:

- As a pioneer in the insurance sector with a strong digital presence, the client's IT team oversaw internal applications, web applications, and mobile applications
- Vulnerabilities uncovered in these assets shed light on a need for immediate and long-term patch management

Challenges and Solutions:

No.	Challenges	Solution
1.	The client performed periodical security testing of their web, mobile, and internal applications and identified a huge volume of vulnerabilities. While existing partners were able to share valuable insights, a new partner who had the expertise to resolve the situation rapidly was needed.	The client's cybersecurity providers tested the apps through Vulnerability Assessment (VA) and Exploit Penetrating Testing (EPT). VA had identified 2669 vulnerabilities, and EPT detected 34. Infopercept's engineering team comprises experts who provide code-level security patching of apps. The team skilfully offered phase-wise solutions, due to which 1986 VA-identified vulnerabilities were patched successfully; some with the help of the client's coding team. All 34 vulnerabilities identified through EPT were also fixed at a rapid clip.
2.	Six hundred and eighty three vulnerabilities in some of the client's critical apps had to be patched urgently. However, given their importance to business continuity, Infopercept was asked to suggest an approach rather than perform the patching themselves.	Infopercept's engineering team suggested solutions to fix the remaining 683 vulnerabilities identified in the VA testing. Our team also created 15 PoCs for some of the vulnerabilities in critical apps. The PoCs enabled the client's dev team to patch the vulnerabilities effectively and seamlessly at a later stage.

Infopercept Solution:

In just three months, the client's patch management was enhanced to enable worry-free digital engagement in a competitive landscape
Infopercept's engineering team implemented a phase-wise approach to resolve the security issue.

Phase 1: Setting up the process

Repeatability is key to continued problem resolution and the team achieved this by setting up a process to patch the vulnerabilities in the internal, mobile and web apps. The team began with the code development to patch the vulnerabilities.

Phase 2: Bug fixing

Bugs arise as a consequence of any development process. But the team rapidly set up a bug fixing process and implemented it.

Phase 3: Securing the landscape

Nearly 75% of the vulnerabilities identified in VA were fixed by the Infopercept team, some in collaboration with the client's development team. All the vulnerabilities detected in EPT were also patched successfully.

Phase 4: Solutions recommendation

The remaining 25% of the bugs identified in VA were in critical apps in a production environment and central to business continuity. Since working on them directly was not possible, the Infopercept team suggested viable solutions to patch these vulnerabilities at a later stage.

Phase 5: PoC creation

To fix some of the vulnerabilities in critical apps, our team created 15 PoCs, which can guide the client's coding team to perform the patching efficiently later.

Infopercept's engineering team understood the complex requirements swiftly and began delivering results right from the first week. The entire exercise including the PoC creation was completed within 3 months.

Infopercept ROI:

- With comprehensive patching of thousands of application vulnerabilities, and Infopercept's continued engagement with process automation, best practices and regular patching, the client has minimal risk levels for the foreseeable future.
- Regulators and management are satisfied with the patch management, and client teams are now confident enough to improve current apps and build new ones for a strong digital presence.

About Infopercept - Infopercept is one of the fastest-growing comprehensive cybersecurity companies in India, serving global clients. It provides platform led managed security services that covers all areas of cybersecurity, including defensive, offensive, detection and response, and security compliance. Infopercept has its own cybersecurity platform, 'Invinsense,' which integrates tools such as SIEM, SOAR, EDR, deception, offensive security, and compliance tools. Its cybersecurity and MDR services include dedicated teams of experts, ensuring that organizations have 24x7 cybersecurity operations support

Imprint

Publisher

3rd floor, Optionz Complex, Chimanlal Girdharlal Rd,Opp. Regenta Central Antarim Hotel, Navrangpura,Ahmedabad, Gujarat 380009, INDIA

Contact

sos@infopercept.com
www.infopercept.com/case-study