AUJAS
CYBERSECURITY
A NuSummit Company

aujas.com

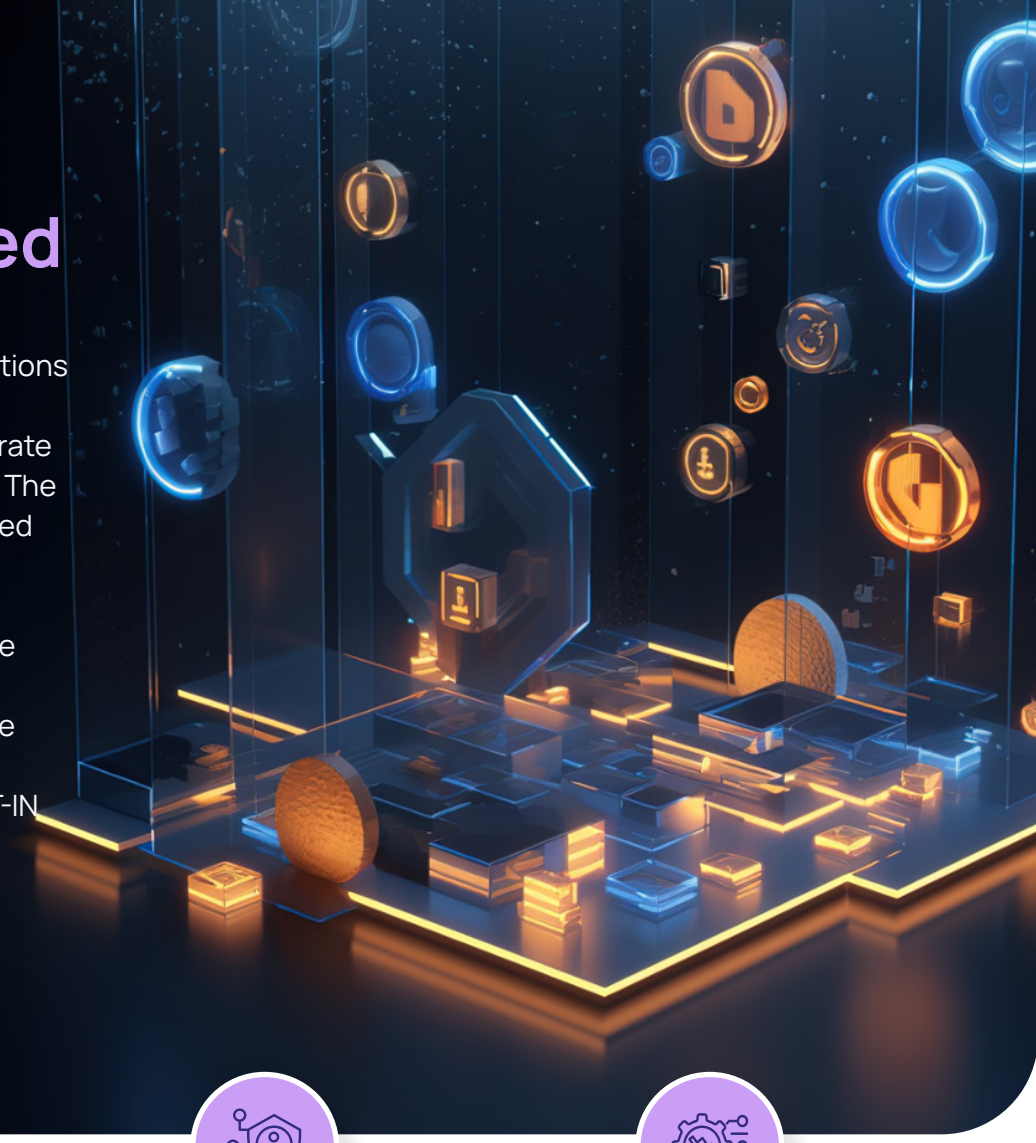
SUCCESS STORY

Enhancing Ransomware Resilience for Financial Services

SECURITY VERIFICATION SERVICES

Business Need

A leading Indian bank with operations nationwide faced increasing regulatory pressure to demonstrate its cybersecurity preparedness. The bank's customers were concerned about the safety of their data, and the bank wanted to assess its defenses against ransomware attacks proactively. The bank's management sought to meet the criteria for services provided by Payswiff from a third-party CERT-IN approved vendor:



Meet Regulatory Requirements

The bank wanted to comply with the Reserve Bank of India's (RBI) cybersecurity and data protection guidelines.

Protect Customer Data

The bank wanted to ensure customer data confidentiality, integrity, and availability.

Minimize Business Disruption

The bank aimed to minimize downtime and financial losses in the event of a ransomware attack.

Business Challenges

Lack Of Practical Testing

Despite having the security tools, the organization had never performed a simulated ransomware attack to validate their effectiveness under real-world conditions.

Unverified Effectiveness Of Security Solutions

The organization had deployed multiple security measures, including endpoint protection, firewalls, and backup systems, but lacked concrete evidence that these solutions could effectively stop a real ransomware attack. There was uncertainty regarding the tools' ability to detect ransomware behavior and prevent lateral movement.

Uncertainty In Detection And Response

The security team's ability to detect and respond quickly to ransomware activity was questioned.

Inadequate Backup Validation

The organization was uncertain if its backup systems were robust enough to recover quickly from a ransomware attack without data loss.

Lack Of A Coordinated Incident Response Plan

Although the organization had a plan, it was never tested, and leadership had concerns about the team's ability to execute it efficiently in an actual ransomware scenario.

Vulnerability Exploitation

Vulnerabilities that could be exploited by ransomware.

Limited Resources

The Payswiff Cybersecurity Team Was Lean And Needed External Expertise To Conduct The Simulation.

Our Solution

- The solution which we proposed was to perform a Ransomware Readiness Security Assessment. Aujas delivered a structured Ransomware Readiness Security Assessment designed to simulate real-world ransomware scenarios in a controlled, non-disruptive environment.
- Ransomware Readiness Security Assessment is performed in two different levels.
  1. Ransomware simulation activity
  2. Ransomware Table top exercise
- As a part of ransomware simulation activity, our team ran ransomware attacks using industry-recognized tools within the client's test environment to evaluate the Payswiff organization's endpoint security measure. This approach enabled us to safely mimic the behavior of real ransomware without causing any harm or data loss.
- The goal was to test whether the client's existing security solutions (such as antivirus, endpoint detection and response (EDR), and network defenses) could detect, block, and respond to ransomware-like activity.
- As a part of ransomware tabletop exercise, our team reviewed the preparedness of the organization in terms of People and Process to check and evaluate the incident response capabilities in an event of an active ransomware attack. This involved discussions and practicing of roles, responsibilities, and response actions for the key stakeholders from following teams in a controlled and collaborative setting.
- We have derived a ransomware simulation solution approach to perform the activity.

Business Impact

The ransomware simulation successfully executed and encrypted the test systems, giving the organization a realistic view of its exposure to such attacks. As a result, the client gained critical visibility into existing security gaps and could take informed action to strengthen their defenses.

The attack bypassed current endpoint defenses, confirming that the existing solutions required enhancement. Following our detailed recommendations, the client improved their security configurations to detect and respond to ransomware-like activity more effectively.

The simulation revealed procedural gaps in the incident response process. While some processes existed, they lacked automation and coordination, mainly due to the absence of a dedicated SOC team. Recommendations were made to enhance these processes and implement a dedicated Security Operations Center (SOC) team.

The simulation demonstrated that existing endpoint defenses were inadequate, allowing the attack to bypass them. The client implemented recommended security configurations to improve detection and response to ransomware-like activity.

It was observed that the organization's email security and endpoint protection controls were insufficient, potentially allowing initial infection vectors like phishing emails or malicious attachments to succeed. The client strengthened these controls, reducing the risk of future attacks.

Project Differentiator

Real-World Simulation

Mimicked actual ransomware attacks in a controlled environment.

Actionable Insights

Delivered fast and practical recommendations for quick remediation.

Holistic Approach

Validated technical, people, and process controls for comprehensive security enhancement.

Collaborative Approach

Our team worked closely with the client's team, making the assessment more valuable and actionable.

Non-Disruptive and Efficient

The simulation was conducted quickly and safely, without affecting live systems, and delivered fast and actionable insights that enabled the client to respond promptly to customer deadlines.

Customized Approach

Our team provided tailored recommendations based on the client's specific infrastructure, regulatory requirements, and simulation findings.

Conclusion

Our ransomware readiness assessment empowered the client to strengthen their defenses and improve resilience against ransomware attacks. By identifying security gaps and providing actionable recommendations, we enabled the client to enhance their endpoint protection, incident response, and backup strategies, ensuring faster recovery and reduced risk.

About Aujas Cybersecurity

Aujas Cybersecurity - A NuSummit Company, helps build and transform cybersecurity postures to enable businesses to mitigate risks. We are a pure-play cybersecurity services company with deep expertise in Identity and Access Management, Risk Advisory, Security Verification, Managed Detection and Response, and Security Engineering services. Our unique products and services help businesses build and transform security postures while mitigating risks. Our focus is to strengthen security resilience by minimizing the occurrence of attacks, threats, and risks so that you can drive change, innovate, and accelerate growth.

For more information, visit us at www.aujas.com or write to us at contact@aujas.com.

Cupertino | Dallas | Jersey City | Ottawa | Riyadh | Dubai | Mumbai | New Delhi | Bangalore

---

For more information, visit us at **nusummit.com**

Follow us at: