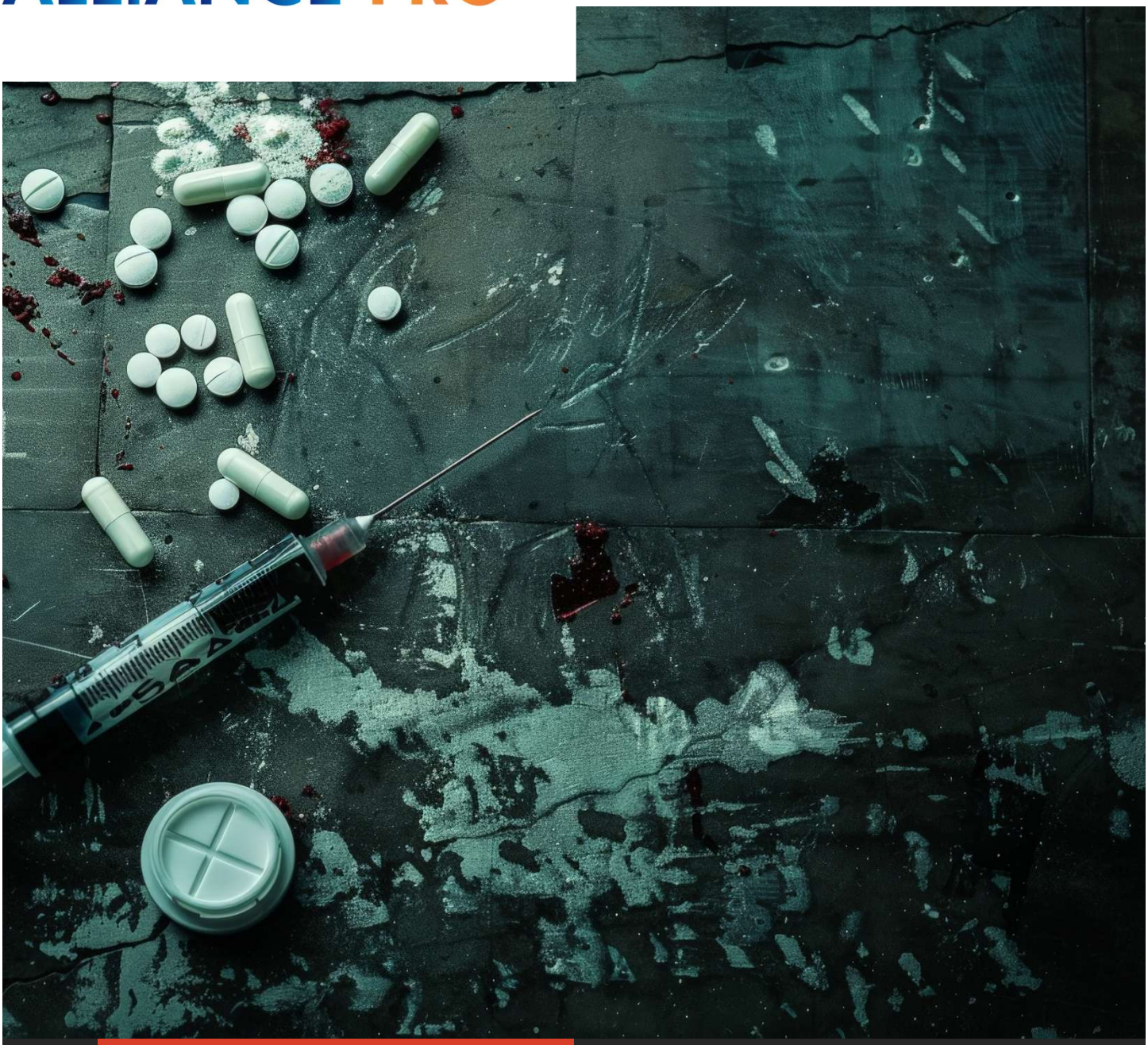
ALLIANCE PRO



THE BREACH THAT FROZE AN ENTERPRISE

CASE-STUDY

ALLIANCE PRO©

DISCLAIMER

This case study has been prepared by **Alliance Pro** for informational and illustrative purposes only. All client-specific identifiers, sensitive details, and proprietary information have been intentionally anonymized or generalized to protect confidentiality and security interests.
The methodologies, processes, and technical approaches described herein constitute the intellectual property of Alliance Pro and may not be reproduced, distributed, or used without prior written consent. This document does not disclose complete operational procedures or security configurations and should not be interpreted as a comprehensive incident response playbook.
Any resemblance to specific organizations, systems, or environments is purely coincidental.

EXECUTIVE SUMMARY

In early 2024, a leading pharmaceutical manufacturing enterprise headquartered in Hyderabad experienced a highly disruptive ransomware attack that brought its production and enterprise IT operations to a complete standstill. Within minutes, mission-critical systems spanning IT and OT environments were encrypted, core authentication services collapsed, and operational continuity was severely threatened.

What initially appeared as a ransomware incident quickly escalated into a full-scale cyber crisis involving **double extortion**, **cross-domain lateral movement**, and **simultaneous compromise of production and disaster recovery environments.**

Alliance Pro was engaged under emergency conditions to lead incident response, digital forensics, recovery, and long-term security hardening. Through rapid containment, disciplined forensic investigation, and resilient recovery engineering, Alliance Pro enabled the organization to restore operations in under 48 hours—**without paying ransom**, **without permanent data loss**, and **without regulatory fallout**.

Ransomware attacks no longer target just systems—they target **operations, compliance, and trust**. When executed with precision, they can halt production, cripple identity services, and erase recovery options within minutes.

This case study documents a real-world ransomware incident at a pharmaceutical manufacturing enterprise in Hyderabad, where a **double extortion ransomware attack** simultaneously compromised IT and OT environments, encrypted both production and disaster recovery systems, and exfiltrated sensitive data.

THE INCIDENT: WHEN SILENCE BECAME THE FIRST WARNING

It began with silence.
At **2:17 AM on a Friday**, the organization's IT team noticed something deeply alarming—production floor systems had gone dark. Core servers began returning connection errors. Active Directory authentication failed across the environment. Endpoint logs stopped flowing into the SIEM.
Within the next **15 minutes**, over **85% of IT and OT systems** were encrypted and rendered inoperable.
A sophisticated ransomware payload had been executed across the environment. Early indicators confirmed a **double extortion model**—systems were encrypted while sensitive data was simultaneously exfiltrated to an external **Command & Control (C2) server hosted outside India**.
The impact escalated further when it became clear that **both production and disaster recovery environments** had been compromised.
This was no longer an isolated cyber event.
It was a full-scale **operational hostage crisis**.

THREAT CHARACTERISTICS AND INITIAL FINDINGS

As the scope of the incident became clearer, several high-risk characteristics emerged:

- Widespread encryption across IT and OT systems
- Compromise of Active Directory authentication services
- Loss of endpoint visibility during the attack window
- Exfiltration of proprietary formulation data and compliance documentation
- Simultaneous impact on production and DR infrastructure

Subsequent analysis identified the ransomware payload as a **modified variant of LockBit 3.0**, known for rapid lateral movement, aggressive encryption, and extortion-driven tactics.

ALLIANCE PRO INCIDENT RESPONSE ACTIVATION

With operations frozen, Alliance Pro activated its **Cyber Emergency Incident Response Protocol**. By **9:00 AM**, a cross-functional Incident Response Strike Team—comprising incident responders, forensic analysts, network engineers, and data recovery specialists—was mobilized and deployed to the organization's **DC and DR facilities in one of the states of South India**

The engagement immediately transitioned into a structured response focused on rapid containment, evidence preservation, and safe recovery. Alliance Pro assumed centralized command of technical response activities to ensure decisions were evidence-led and recovery actions did not introduce reinfection risk.

Containment and Initial Response

The first phase of response focused on stopping the spread of ransomware and stabilizing the environment.

Network-level containment was initiated by isolating flat network segments and shutting down affected VLANs to eliminate east–west lateral movement. Endpoint containment followed, with infected systems identified using **EDR and Sysmon telemetry** and isolated from the network to prevent further propagation.

Initial forensic triage confirmed that the ransomware had been deployed via a **compromised Domain Controller**. Lateral movement was conducted using **SMB shares and PSExec**, allowing the attackers to rapidly distribute the payload. The privilege escalation path was traced back to a **compromised VPN credential**, reused across multiple services and operating without multi-factor authentication.

These findings confirmed that the attack was driven by **identity compromise and privilege abuse**, a common characteristic of high-impact ransomware incidents.

Forensic Investigation and Kill Chain Reconstruction

Alliance Pro conducted a deep forensic investigation to reconstruct the complete attack lifecycle and establish a verified recovery baseline. Using enriched log data and timeline reconstruction, the following kill chain was identified:

Attack Stage	Observed Activity
Initial Access	Compromised VPN credential
Credential Abuse	Reuse across multiple services

Lateral Movement	SMB and PSExec
Privilege Escalation	Domain-level compromise
Data Exfiltration	Transfer to external C2
Encryption	Widespread ransomware deployment

This forensic clarity was essential. It enabled the team to determine the **last known clean state**, exclude contaminated datasets, and ensure that recovery actions were both safe and defensible.

Recovery and Resilience Engineering

Despite the scale of encryption, Alliance Pro executed a controlled, multi-phase recovery strategy focused on integrity-first restoration.

Critical virtual machines were restored from **air-gapped, immutable backups** using isolated recovery workflows. Bare-metal restoration was performed in controlled environments, and systems were thoroughly validated before being reintroduced into production networks. During forensic validation, Alliance Pro identified and successfully recovered highly sensitive business data that was initially feared lost.

Proprietary formulation intellectual property, FDA audit documentation, and export compliance records were retrieved from **isolated shadow copies** that the ransomware failed to encrypt due to **NTFS permission constraints**. This recovery significantly reduced regulatory and legal exposure.

Stabilization and Security Hardening

Within **48 hours**, core business operations were restored. Alliance Pro then supported stabilization and hardening activities to reduce the risk of recurrence. Active Directory architecture was rebuilt using **Just-In-Time privileged access**, multi-factor authentication was deployed across critical access paths, and network segmentation was redesigned to limit blast radius.

A revised **Business Continuity and Disaster Recovery (BCP/DR)** plan was implemented with isolated testing, and security awareness training was initiated for senior staff to address credential hygiene and incident readiness.

OUTCOME: BUSINESS RESTORED, RISK REDUCED

What could have resulted in prolonged downtime, regulatory penalties, and permanent intellectual property loss was successfully contained and remediated.

The organization:

- Restored operations in under 48 hours
- Retained full ownership of its data
- Paid no ransom
- Passed its subsequent regulatory audit with **zero security non-conformities**

Most importantly, the enterprise emerged with a more resilient and response-ready cybersecurity posture.

KEY TAKEAWAYS

Rapid incident response is critical to protecting business continuity. Credential compromise remains a primary ransomware entry point, and immutable backups continue to be the final line of defense. Above all, forensic-led decision-making enables safe recovery without capitulating to extortion demands.

-END OF DOCUMENT-