MISSION DEBRIEF
From the Frontlines
FENIX24 CASE STUDY

From Shutdown to Full Operations: How Fenix24 Recovered 600+ Critical Servers for a Global Defense Contractor

The Challenge:

A global defense contractor experienced a ransomware attack that brought production to a halt across several critical facilities. Sensitive data was encrypted globally, compliance concerns escalated, and the company faced immense financial and operational pressure to recover quickly to continue serving its defense and commercial clients.

The Solution:

Fenix24 mobilized immediately. Within days, the team:

- Rebuilt numerous servers and hosts impacted by the attack.
- Decrypted the company's data and restored operations for critical systems in only two days.
- Recovered the remaining global data in the following four days.
- Validated over 600 critical servers remotely in only two days through health server testing.

Following recovery, the company invested in Fenix24's Securitas Summa program, our comprehensive managed service that includes ongoing backup management, system hardening, and a 5-year retainer to ensure resilience against future attacks. This solution was deployed across mission-critical facilities in the U.S., France, and Germany.

The Outcome:

The company was able to resume production for its defense clients without interruption. With recoverability now assured and stakeholder confidence restored, the company continues to meet the strict delivery demands of some of the world's largest military customers.

By working with Fenix24, what began as a shutdown-level crisis became a demonstration of resilience: rapid recovery, continuity of operations, and long-term protection against future disruption.