Sezione 2.1 - Minacce e Rischi Principali

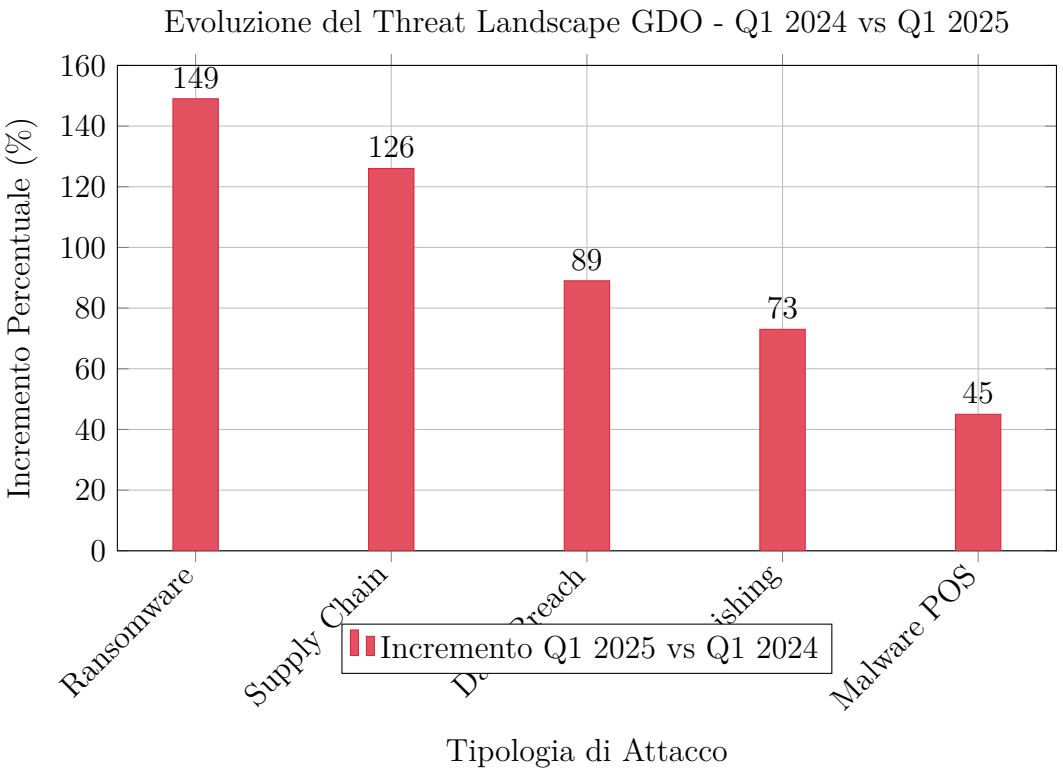

Figura 1: La figura mostra l'incremento percentuale delle diverse tipologie di attacchi nel settore retail, evidenziando la crescita del 149% per ransomware e del 126% per attacchi supply chain

Tabella 1: Evoluzione Tecniche Attacco POS

Generazione	**Periodo**	**Tasso Successo**	**Caratteristiche Principali**	**Contcaci**
Prima	2019-2021	73%	Malware semplice, vulnerabilità note	Antivi
Seconda	2022-2023	45%	Offuscamento, comunicazioni cifrate	Analistale
Terza	2024-2025	62%	Adattamento dinamico, manipolazione protocolli	Architrust

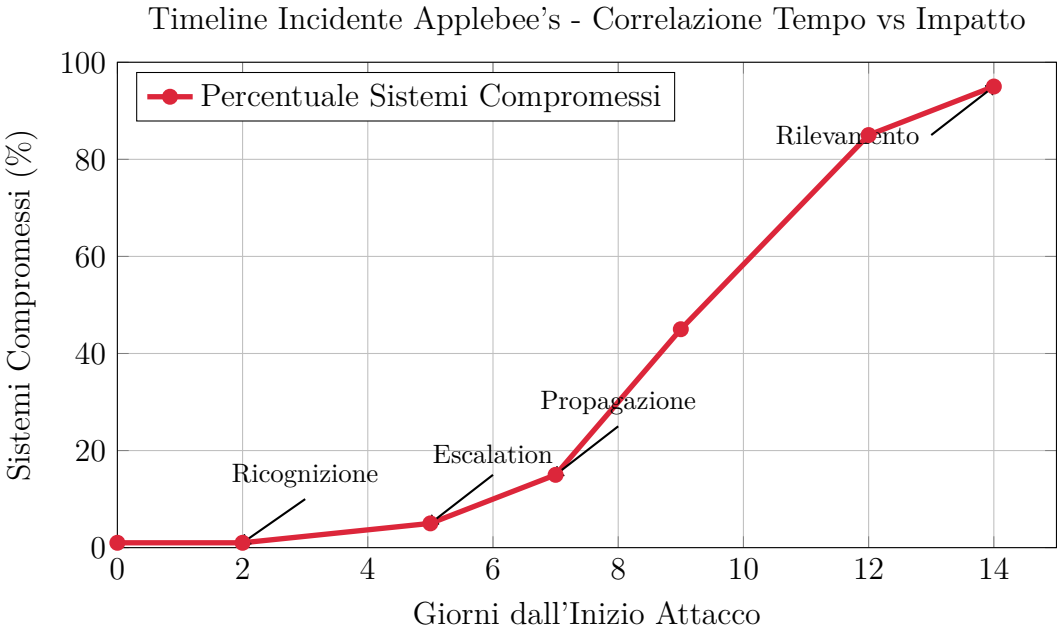

Figura 2: Il grafico mostra come l'impatto dell'incidente sia cresciuto esponenzialmente con il tempo, evidenziando l'importanza del rilevamento precoce

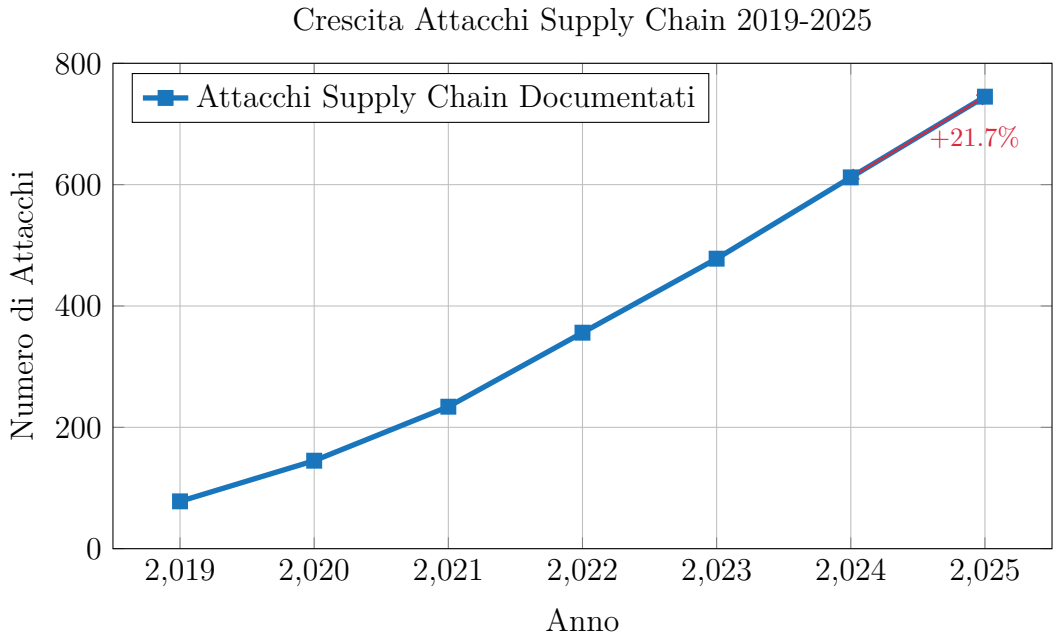

Figura 3: Il grafico mostra la crescita esponenziale degli attacchi supply chain, con particolare accelerazione nel 2024-2025

Sezione 2.2 - Tecnologie di Difesa Essenziali

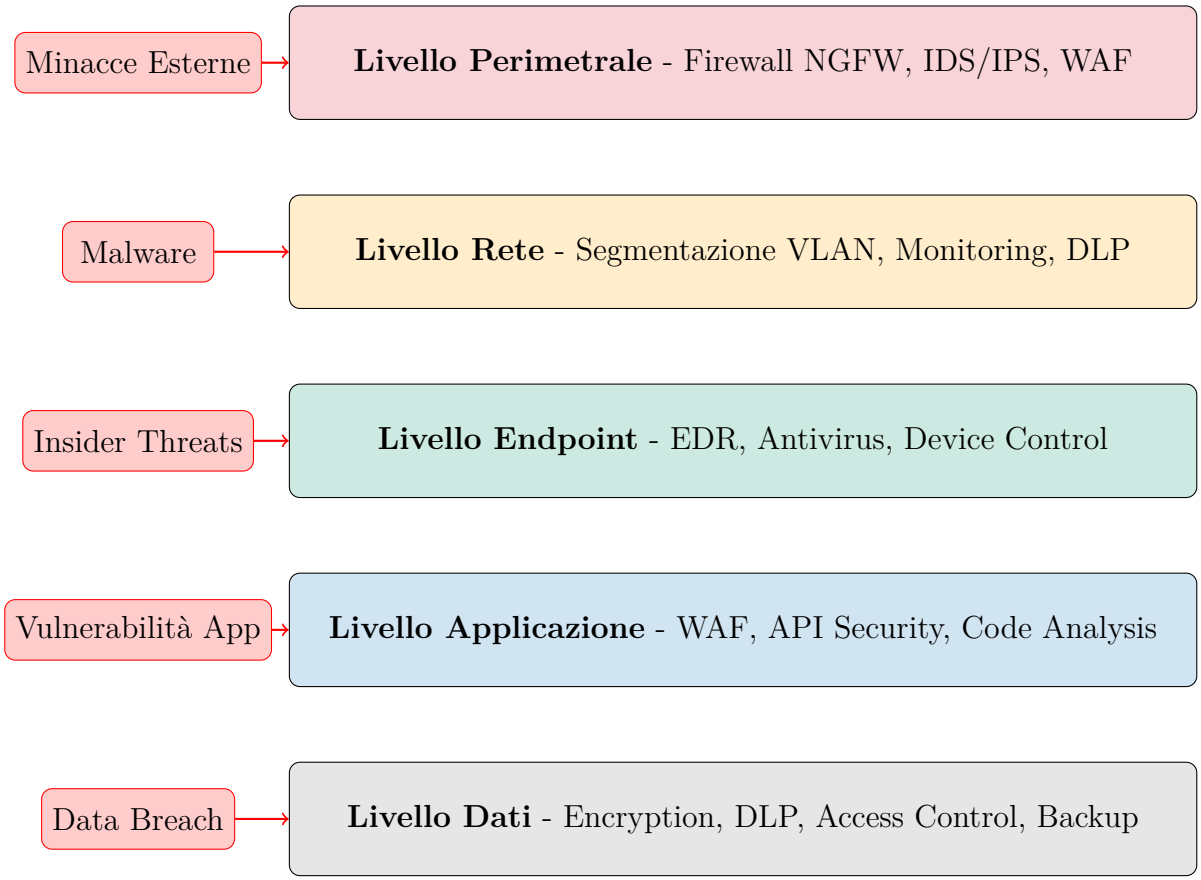

Figura 4: I cinque livelli principali di una difesa stratificata tipica per la GDO: perimetrale, rete, endpoint, applicazione, e dati

Tabella 2: Confronto Paradigmi Detection IDS/IPS

Aspetto	**Detection Firme**	**Detection Anomalie**	**Approccio Ibrido**
Falsi Positivi	Molto Bassi	Medio-Alti	Bassi
Zero-Day Detection	No	Sì	Parziale
Overhead Computazionale	Basso	Alto	Medio
Facilità Tuning	Alta	Bassa	Media
Adattabilità	Bassa	Alta	Alta

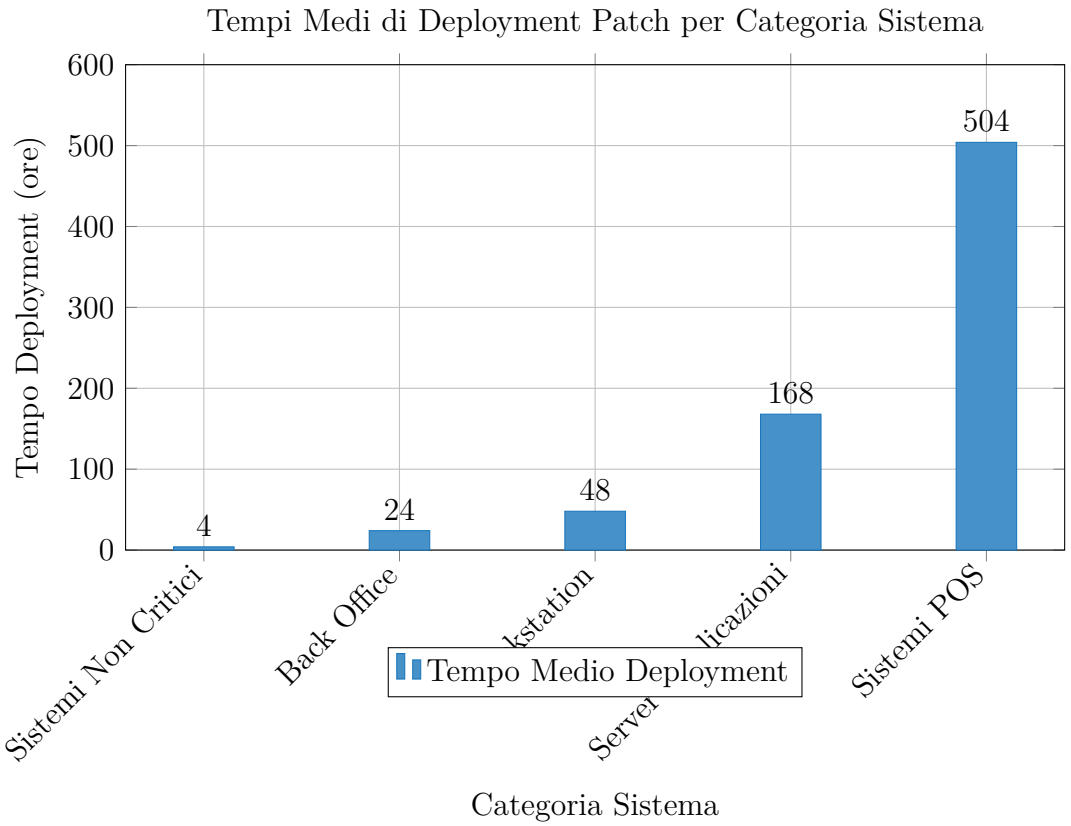

Figura 5: Il grafico mostra come i tempi di deployment varino significativamente tra categorie di sistemi, da poche ore per sistemi non critici a diverse settimane per sistemi POS critici

Tabella 3: Fattori di Prioritizzazione Rischio CSPM

Fattore	**Descrizione**	**Peso**	**Metrica**
Severità CVSS	Score vulnerabilità standard	25%	0-10
Esposizione Internet	Accessibilità dall'esterno	20%	Binario
Sensitività Dati	Classificazione dati contenuti	20%	1-5
Criticità Business	Impatto operativo disruption	15%	1-5
Facilità Exploit	Disponibilità exploit pubblici	10%	Binario
Patch Disponibili	Esistenza di fix	10%	Binario

Sezione 2.3 - Requisiti e Vincoli Architetturali

Tabella 4: Metriche di Performance Monitoraggio PCI-DSS

Componente	**Latenza Aggiunta**	**CPU Overhead**	**Storage/Giorno**	**RAM Richiesta**
Event Collection	2-5ms	3-5%	500MB-1GB	512MB
Real-time Analysis	10-20ms	8-12%	1-2GB	2GB
Correlation Engine	50-100ms	15-20%	2-3GB	4GB
Audit Storage	N/A	2-3%	2-5GB	1GB

Tabella 5: Tempi di Risposta NIS2 per Categoria Incidente

Categoria	**Severità**	**Detection Time**	**Response Time**	**Recovery Time**	**Reporting**
Critico	Alta	< 5 min	< 15 min	< 4 ore	24 ore
Importante	Media	< 15 min	< 1 ora	< 8 ore	72 ore
Standard	Bassa	< 1 ora	< 4 ore	< 24 ore	7 giorni

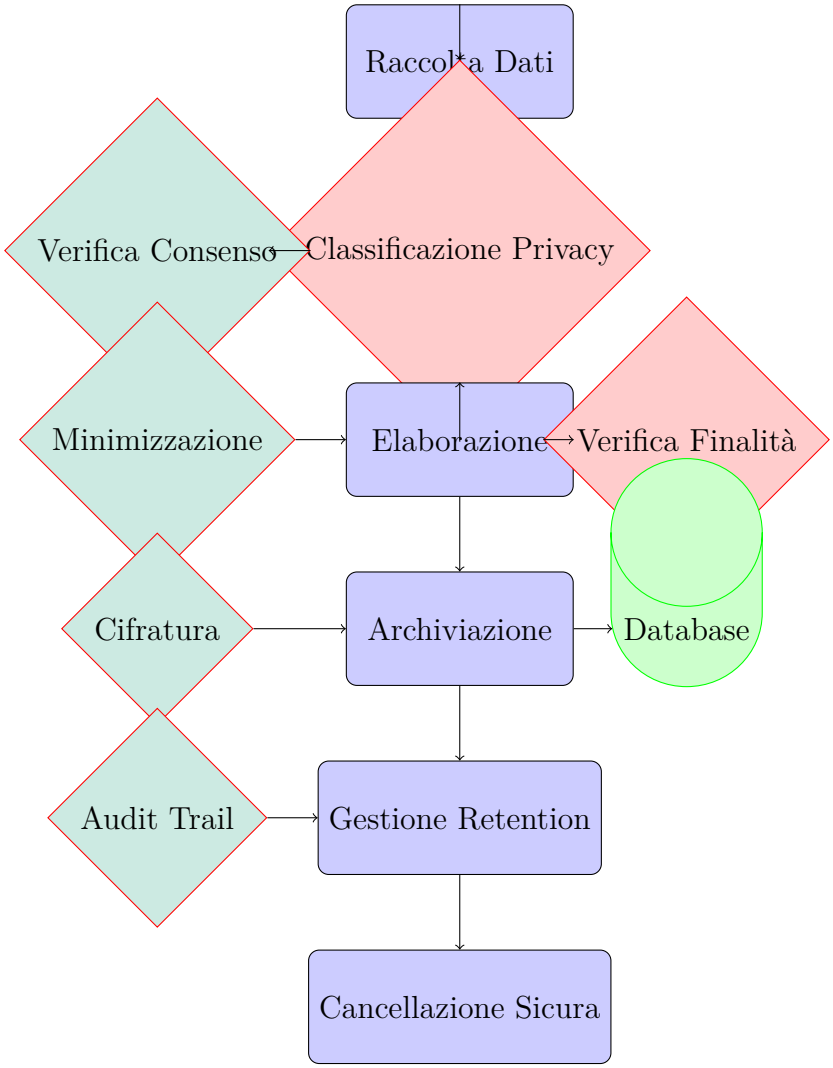

Figura 6: Il flusso di elaborazione dati dalla raccolta alla cancellazione, con controlli privacy integrati in ogni fase

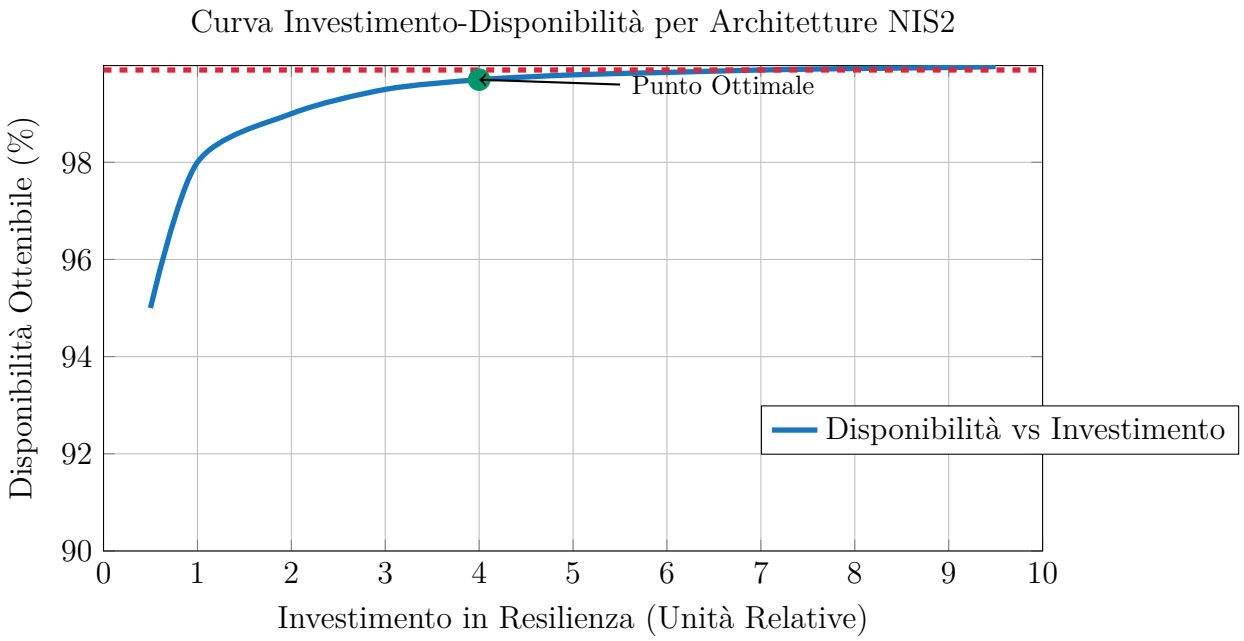

Figura 7: Il grafico mostra come la disponibilità aumenti logaritmicamente con gli investimenti in resilienza, con un punto di ottimizzazione intorno al 99.9%

Figura 8: Come i diversi standard vengano integrati in un motore unificato che ottimizza l'implementazione dei controlli