WHITEPAPER

Two Major Auto Breaches, One Fatal Flaw:

Why Detection-Based Security Can't Stop Modern Attacks

The automotive industry faces an unprecedented cybersecurity crisis. Just months apart, two major breaches have exposed the fundamental weaknesses in detect-and-respond strategies that organizations have relied on for decades. The recent Jaguar Land Rover and Stellantis breaches share disturbing commonalities - and point toward a critical need to shift from defensive to preventive cybersecurity architectures.

The Common Thread: Systems Built to Be Discoverable

Both the JLR and Stellantis attacks leveraged systems that attackers could fundamentally discover and reach. In JLR's case, cybercriminals chained together known SAP NetWeaver vulnerabilities (CVE-2025-31324 and CVE-2025-42999) to execute arbitrary system commands with administrator privileges. The compromised SAP system was internet-facing, creating a pathway for the Scattered Spider group to access internal networks.

Stellantis suffered a different but equally telling attack – part of the massive Salesforce breach campaign that compromised over 760 companies. The ShinyHunters group used sophisticated social engineering and OAuth token abuse to access Salesforce instances, stealing over 18 million customer records. The attack succeeded because legitimate business systems were accessible to attackers who obtained the right credentials through vishing campaigns.

> "Detect, triage, and remediate" is no longer an effective strategy. Attackers are now using AI to move faster than defenders, and AI for defense is not even close to being as effective as it is for attack."
>
> — Federico Simonetti
> CTO, Xiid

The Detection Trap: Always One Step Behind

Both breaches reveal the fundamental flaw in detect-and-respond strategies. JLR's security tools detected the intrusion, but only after attackers had already gained administrator-level access and begun moving laterally through systems. The company was forced to shut down production across multiple countries for weeks, losing an estimated £75 million in daily turnover.

Stellantis experienced a "silent" breach where attackers operated undetected within Salesforce environments, exfiltrating sensitive customer data over time. Traditional security controls failed to prevent the initial OAuth token compromise or detect the subsequent data extraction.

The Problem with Traditional Security Models

Both attacks succeeded because they exploited foundational architectural weaknesses that detection-based security cannot address:

Always-On Attack Surfaces

JLR's SAP NetWeaver system required internet connectivity for business operations, creating a persistent target for attackers. Once discovered, these systems become permanent fixtures on threat actors' target lists.

Credential-Based Authentication

The Stellantis breach demonstrates how even sophisticated multi-factor authentication can be defeated through social engineering. When authentication relies on something users know or have, those credentials can always be stolen, phished, or manipulated.

Network-Level Trust

Both organizations operated on implicit trust models where authenticated users and systems could access broad network resources. Once attackers obtained legitimate credentials or system access, they could move laterally with minimal resistance.

Reactive Detection

Security teams in both cases were relegated to post-breach response rather than prevention. By the time anomalous activity was detected, attackers had already achieved their primary objectives.

Prevention by Design: A New Security Paradigm

The solution isn't better detection – it's prevention by design. This approach eliminates attack surfaces before threats can exploit them, rather than trying to detect and respond after compromise occurs.

Making Systems Non-Routable

Instead of securing internet-facing systems with firewalls and detection tools, prevention by design makes critical resources completely unreachable from external networks.This approach uses outbound-only connections to eliminate the discoverable attack surfaces that allowed both breaches to occur.

Credential-less Authentication

Rather than relying on stealable usernames, passwords, or even OAuth tokens, zero knowledge authentication proves identity without transmitting any secret information. Even sophisticated social engineering campaigns like those used against Stellantis become impossible when there are no credentials to steal.

Process-Level Segmentation

Prevention by design implements process-to-process connections rather than network-to-network access. This approach would have contained both attacks at the point of initial compromise, preventing the lateral movement that caused extensive damage.

Quantum-Safe Encryption

Both breaches involved the potential for long-term exposure of encrypted data. Prevention by design implements multiple layers of quantum-resistant encryption, protecting against both current attacks and future "harvest now, decrypt later" strategies.

The ROI of Prevention

One insight on preemptive security economics is particularly relevant: Preemptive security is the only one with compound ROI. When you prevent an incident instead of detecting and remediating it, you avoid downtime, business disruption, legal exposure, forensics, and churn.

The JLR breach cost the company millions in lost production, regulatory investigations, and reputation damage - costs that continue to compound. The Stellantis breach exposed 18 million customer records to potential fraud and identity theft. These incidents represent exactly the types of cascading costs that prevention by design eliminates.

Overcoming Implementation Barriers

The primary obstacle to prevention by design isn't technical – it's organizational. As Fed Simonetti notes, "The hard part is not the tech. It's the change. Leaders are used to detect and respond, so moving to preemptive controls feels unfamiliar."

Start with Proof, Not Philosophy
Rather than attempting organization-wide transformation, begin with proof-of-concept deployments that demonstrate measurable risk reduction. Xiid's SealedTunnel technology, for example, can secure critical assets without requiring infrastructure replacement.

Focus on Business Outcomes
Frame prevention by design in terms of business continuity, regulatory compliance, and competitive advantage rather than technical specifications. The JLR production shutdown demonstrates how cybersecurity directly impacts core business operations.

Plan for Coexistence
Solutions designed for prevention should be integrated into the existing infrastructure instead of necessitating a complete replacement. This approach reduces implementation risk and enables gradual migration from detect-and-respond to prevention-based architectures.

The Path Forward

Both the JLR and Stellantis breaches could have been prevented through prevention by design architectures. JLR's SAP systems could have operated through outbound-only connections, making them completely unreachable by external attackers. Stellantis's authentication systems could have used credential-less protocols that render social engineering attacks impossible.

With its long asset lifecycles, complex supply chains, and increasing digitalization, the automotive industry exemplifies why prevention by design is becoming essential. If security tools are not designed for prevention, entire systems are always operating at risk.

The choice is clear: continue playing defense against increasingly sophisticated attackers or adopt prevention by design architectures that eliminate the attack surfaces these threats depend on. The JLR and Stellantis breaches show us what happens when we choose the former. The question is whether we'll learn from these failures and choose the latter.

Prevention by design isn't just a security strategy – it's a business imperative for organizations that can't afford to be the next headline.