⧩ ZAFRAN

The AI-Native Exposure Management Platform

PeerSpot No.1 Ranked CTEM Solution ★★★

Latio CTEM LEADER 2025

Proactively Stop Vulnerability Exploitation. Everywhere.

Zafran is the only AI-native Threat Exposure Management platform that deeply maps vulnerabilities to compensating controls, like EDR, NGFWs, WAFs, and cloud controls, to determine what is actually exploitable in your environment. By validating the real-world effectiveness of the defenses you already run, Zafran proves that up to 90% of "critical" vulnerabilities are not exploitable, so teams can focus on the 10% that truly put the business at risk.

Unified Vulnerability Management
Consolidate and deduplicate cloud, on-prem, and AppSec findings across existing scanners into a single source of truth for vulns.

Exposure Assessment & Prioritization
Prove real exploitability by correlating runtime presence, internet reachability, threat activity, asset criticality, and automated mapping of your compensating control configurations.

AI-Powered Remediation Operations
Transform vulnerability insights into focused, AI-optimized remediation by deduplicating tickets, generating clear remediation plans, and automatically routing tasks to the right owners at scale.
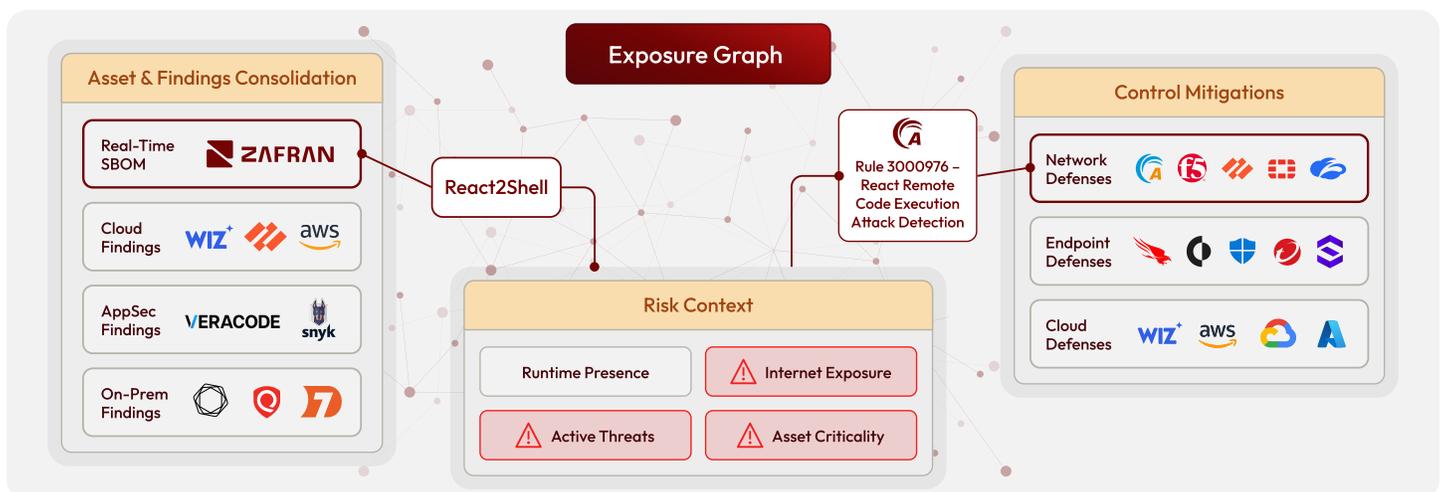
Mitigation Ahead of Patch Cycles
Zafran eliminates 90% of critical vulnerability noise to isolate the 10% that actually matter.

Autonomous AI agents for your entire vulnerability management lifecycle

Key Benefits:

- Shrink MTTR Across Security & IT
- Unify All Assets, Findings, Context & Controls
- Eliminate Manual Triage & Routing
- Mitigate Risk Before Patch Windows with Compensating Controls
- Autonomously Assess "Am I Exposed?"
- Deliver Instant, Audit-Ready Reporting and Dashboards

Continuously Maps Exposures to Compensating Controls

Asset & Findings Consolidation
- Real-Time SBOM — ⧩ ZAFRAN
- Cloud Findings — WIZ, aws
- AppSec Findings — VERACODE, snyk
- On-Prem Findings

Exposure Graph

React2Shell

Rule 3000976 – React Remote Code Execution Attack Detection

Risk Context
- Runtime Presence
- ⚠ Internet Exposure
- ⚠ Active Threats
- ⚠ Asset Criticality

Control Mitigations
- Network Defenses
- Endpoint Defenses
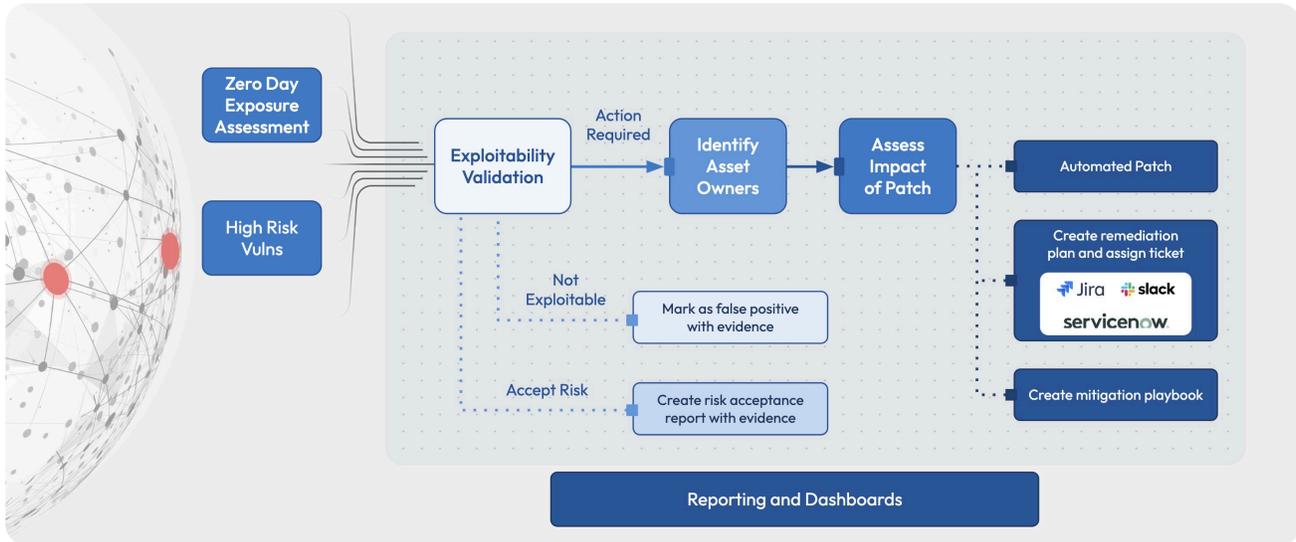- Cloud Defenses — WIZ, aws

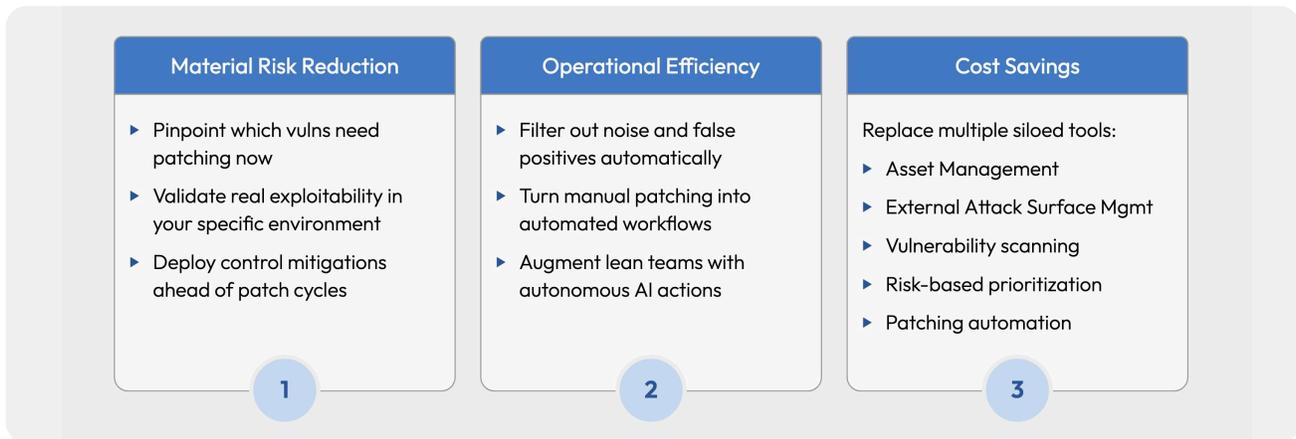# Autonomous AI Agents For Your Entire Vulnerability Management Lifecycle

Agentic Exposure Management uses autonomous AI agents to assess real exploitability, rapidly determine exposure to zero-days, generate prioritized remediation plans, and safely execute mitigations through existing controls. It also automates analyst-heavy work like ownership mapping, reporting, and dashboard generation, removing humans from the critical path and shrinking exposure windows to match attacker speed.

> "With Zafran, we know what is truly exploitable, allowing us to quickly execute remediation efforts."
>
> *Greg Garneau*
> *VP & CISO, HSHS*

The Value of Zafran Threat Exposure Management

Material Risk Reduction

▸ Pinpoint which vulns need patching now

▸ Validate real exploitability in your specific environment

▸ Deploy control mitigations ahead of patch cycles

1

Operational Efficiency

▸ Filter out noise and false positives automatically

▸ Turn manual patching into automated workflows

▸ Augment lean teams with autonomous AI actions

2

Cost Savings

Replace multiple siloed tools:

▸ Asset Management

▸ External Attack Surface Mgmt

▸ Vulnerability scanning

▸ Risk-based prioritization

▸ Patching automation

3

Trusted by Leaders

CHIPOTLE   KraftHeinz   LUMEN   netskope

> "Zafran has proven to be a force multiplier to mitigate risks in our environment."
>
> *Brett Wentworth*
> *VP & Deputy CSO, Global Security, Lumen Technologies*

About Zafran Security

Zafran Security has created the new operating model for vulnerability management. We use your existing defenses and analyze your unique risk context, to reveal and remediate the exposures most likely to be exploited. For most customers, this reduces critical vulns by 90%, freeing up resources to focus on the real risks.

ZAFRAN

www.zafran.io
info@zafran.io