DEEPWATCH™
Always Watching. Always Protecting.™

CUSTOMER SUCCESS STORY

Informatica Transformed Vulnerability Management Across 100+ Teams with The Deepwatch Guardian MDR Platform™

"The Deepwatch Guardian MDR Platform gave us visibility we didn't think was possible. In just weeks, we went from manual spreadsheets to real-time insights across 100+ teams and multiple business units."

— Nikhil Singh, Senior Security Engineering Manager, Informatica

CHALLENGE

The DIY Trap: Fragmented Tools, High Costs, and Limited Visibility

Initially, Informatica's DIY approach to vulnerability management seemed straightforward. However, complexities quickly emerged, from stitching together disparate tools to managing stateful data, and accurately attributing ownership. Transitioning away from StackRox was particularly challenging, as containerized environments made asset-level attribution extremely difficult. This fragmentation severely hindered reporting accuracy, creating time-intensive manual processes to inform leadership.

Over two years, the team spent the equivalent of $250,000 in engineering hours building internal visibility for StackRox. When they made the business decision to switch scanning tools, their entire reporting infrastructure collapsed.

"We were building everything ourselves—normalization, attribution, reporting. It wasn't scalable, and it tied us to a single vendor," said Singh. Containers introduced another layer of complexity. Each image consisted of multiple layers, often owned by different teams. ***"Without proper layer-level attribution, we couldn't assign vulnerabilities accurately or track ownership across teams and BUs,"*** Singh explained. Reporting to leadership and auditors was also hindered—data lived in siloed systems and required hours of manual spreadsheet work.

ENTERPRISE DETAILS

Industry: Cloud Data Management

Services: Data Integration, Cloud Management

Revenue: $1.5B

Employees: 6,000+

SOLUTION

Centralized Visibility, Attribution, and Speed-to-Value

Informatica selected Deepwatch to unify and normalize its vulnerability data pipeline. Deepwatch quickly delivered several critical capabilities:

- **Attribution by Team and Business Unit:** Deepwatch enabled vulnerability assignment by asset ownership, including mapping container image layers to the correct owning teams across hundreds of teams and multiple business units.
- **Risk Reprioritization:** Informatica integrated its own threat intel feed into Deepwatch, allowing vulnerabilities to be rescored based on exploitability, asset exposure, and environmental context.
- **Custom Metrics and Reporting:** Deepwatch's data was piped into Informatica's internal portal (Orion), enabling real-time leadership and board reporting without manual preparation.

"Deepwatch didn't just provide a tool—they fundamentally changed how quickly we gained meaningful insights and our approach to risk and reporting. Critical features were delivered within two weeks, a speed we've never seen before."

- Nikhil Singh, Senior Security Engineering Manager Informatica

DEEPWATCH™

OVERVIEW

Overcoming Security Complexity at Scale

Informatica, a global leader in cloud data management, faced escalating complexity managing security across its cloud-native architecture. With vulnerability data pouring in from tools like Qualys and Prisma Cloud, teams struggled to unify disparate insights and assign ownership. Attempting a DIY approach, Informatica invested over $250,000 worth of internal engineering hours building a custom data pipeline for StackRox visibility. While functional at first, the homegrown solution became increasingly difficult to maintain—especially as toolsets evolved.

After two years, they needed to migrate away from StackRox, but the custom pipeline was deeply bespoke to StackRox and changing tools broke everything downstream. Informatica became effectively vendor-locked, forced into costly rebuilds with tool change—until Deepwatch stepped in.

Deepwatch quickly delivered seamless visibility and data normalization, solving attribution challenges within weeks rather than months, while enabling smooth transitions between tools, a critical benefit to Informatica's security strategy. ***"Deepwatch made us truly vendor-agnostic. Their seamless integration capability is a huge value for security leaders who inevitably switch tools over time."***

- Nikhil Singh, Senior Security Engineering Manager Informatica

CUSTOMER TESTIMONIAL

"If you're struggling with fragmentation and reporting complexity, Deepwatch delivers immediate value with best-in-class support. We're now operating at a level I didn't think was possible in such a short time."

- Nikhil Singh, Senior Security Engineering Manager Informatica

CYBER OUTCOMES

The outcomes have been transformative, delivering immediate operational and strategic benefits:

- **Cost Savings:** Replacing legacy and internally-maintained pipelines significantly reduced operational expenses of $77,000 per year.
- **Attribution Clarity:** Teams now receive only the vulnerabilities they own, accelerating remediation and eliminating bottlenecks.
- **Proactive Build-Time Security:** Early identification of vulnerabilities in shared image layers reduced production-stage risk and allowed earlier remediation.
- **Leadership Confidence:** Real-time dashboards enable executives to dynamically explore enterprise-wide security posture, adherence to SLAs, and compliance metrics at the business unit and product-line level.

"Our leadership can now drill into specific reports dynamically—by business unit, timeframe, or product line. This didn't exist before. We've replaced hours spent building manual PowerPoint decks with instant access."

- Nikhil Singh, Senior Security Engineering Manager Informatica

Future Vision—Looking Ahead to AI-Powered Capabilities

Informatica anticipates continued innovations from Deepwatch, particularly leveraging AI-driven automation and endpoint integration, directly aligning with Informatica's strategic security roadmap.

Upcoming features include:

- AI-powered report generation through a chatbot-style co-pilot interface, significantly reducing manual workloads.
- Real-time compliance queries for auditors, simplifying reporting demands.
- Expanded integrations with security solutions like Cortex XDR, unifying endpoint management and vulnerability data to close critical coverage gaps.

"These AI-driven capabilities align directly with our strategic goal of automating compliance and security operations, shifting our team from reactive to proactive management."

- Nikhil Singh, Senior Security Engineering Manager Informatica

DEEPWATCH™
Always Watching. Always Protecting.

ABOUT DEEPWATCH

Deepwatch® is the leader in Precision MDR powered by AI and humans. We amplify human expertise with AI insights to reduce the risks that matter most to your business. Our protection is proactive, preemptive and responsive, tuned to your business, with no black boxes, and watched by experts 24/7/365.

CONTACT US

GET STARTED

250 Cambridge Avenue
Palo Alto, CA 94306

www.deepwatch.com