QUICK READ

oxsecurity

Eight Reasons Why a Data Fabric Will Improve Your AppSec

Eight Reasons Why a Data Fabric Will Improve Your AppSec

The current state of application security is a bit like trying to solve a 1,000-piece puzzle that doesn't include all the pieces. In the early days of AppSec, standalone tools were invented to tackle specific threats. Those tools served their purpose for the time and all was well. However, over time, as software development changed, attackers started to focus on its rapid evolution and the blind spots speed can create. As such, threats to the integrity of applications multiplied, as evidenced by the increasing number of successful attacks against them.

As this was happening, vendor companies were not asleep at the wheel. In fact, savvy entrepreneurs quickly noticed that there were significant gaps in software protection solutions, and new categories of tools were created to help builders of software protect not just software, but the process of building software. Subsequently, the number and types of AppSec and SDLC tools commercially available exploded.

Over time, as software development changed, attackers started to focus on its rapid evolution and the blind spots speed can create. As such, threats to the integrity of applications multiplied, as evidenced by the increasing number of successful attacks against them.

What happened next was a chaotic mess: siloed tools, each spitting out data in different formats, creating more confusion than clarity, and generating alerts that could keep a person awake for days. Security professionals, try as they might, attempted to loop developers into the security process and insert AppSec tools into developers' workflows. But these tools weren't purpose-built for developers. They slowed down processes and frustrated developers. Developers pushed back, and the infamous turf wars between DevOps and security teams began.

Next came organizations' attempts at DevSecOps, where security teams tried to literally embed security team members into development teams. This move was similarly met with resistance, and security teams had to find better processes — and tools — that would actually improve developers' processes.

What was desperately needed was an approach to AppSec that provides both security and development teams with accurate results, relevant data, and low false positive rates. This approach would introduce a collaboration that would allow each team to quickly understand the problems that arise throughout the software development lifecycle. And maybe more importantly, this would help each team focus on what needs to be done to launch secure, resilient software that enables business transformation.

Enter the data fabric — a smarter, more unified approach that offers a complete view of the security landscape and is quickly becoming the gold standard for application security.

ox security

What is an AppSec Data Fabric??

As with many cybersecurity categories, different constituencies have varying ideas about the definition of "data fabric." For purposes of this post, let's baseline that a "data fabric" is an integrated data management architecture that provides a consistent and unified way to manage and analyze data from a wide range of sources, formats, and digital environments. This architecture connects data silos, normalizes data sets for clarity, correlates them, then presents the data in a way that makes it easier to share, analyze, and act upon.

A generic data fabric could be assembled simply by connecting disparate technologies via API connections. This is a viable approach to data unification. However, what's missing with this "integration-only" methodology is a baseline — a way to verify that the data collected from all the various tools is valid, meaningful, and actionable. In other words, an AppSec Data Fabric up-levels a data fabric by bringing in proprietary data collection, analysis, and enrichment.

Now that we have a definition of "data fabric" established, what does it mean for AppSec teams, developers, and data owners? At least when it comes to application security and software supply chain security, we at OX think a ata fabric is best for these eight underlying purposes:

1. CENTRALIZED DATA COLLECTION

Traditional security setups often rely on multiple, isolated tools that gather data from silos — this is especially true for AppSec, as the industry has grown tool by tool, stage of development by stage of development. This fragmentation makes it challenging for security and development teams to correlate findings, which leads to inefficiencies and gaps in coverage. A data fabric, however, acts as a central hub that aggregates and normalizes data from all sources — from native scanning tools to third-party integrations. This consolidated approach eliminates the aforementioned chaos of managing disparate data sets and provides a holistic view of an organization's application security posture. The benefit: teams are able to detect and respond to threats more effectively.

2. IMPROVED DATA NORMALIZATION

One of the most significant advantages of a data fabric is its ability to normalize data from multiple sources into a consistent format. Why is this so important? Because different AppSec and general-purpose tools often use unique data schemas, making it hard to compare and analyze information across the entire application portfolio. A data fabric takes these disparate inputs and harmonizes them into a unified format. The benefit: faster and more accurate analysis of software and all its components, all the way throughout the software lifecycle.

3. ENHANCED CONTEXT AND PRIORITIZATION

Raw data about vulnerabilities isn't enough; context is queen. A data fabric doesn't just aggregate data — it enriches it by providing crucial context, such as exploitability, reachability, and potential impact. This added context allows AppSec and DevOps teams to prioritize vulnerabilities based on real-world risk rather than theoretical severity, ensuring that the most critical issues are addressed first. The benefit: a more efficient use of time and resources, with remediation efforts focused on what truly matters.

4. ACTIONABLE INSIGHTS FOR FASTER DECISION-MAKING

With a data fabric, AppSec and development teams gain actionable insights, not just raw data. By combining comprehensive data collection, normalization, and context, a data fabric highlights critical vulnerabilities, suggests remediation steps, and integrates seamlessly with existing workflows to automate responses. The benefit: significant reduction in the time spent on manual analysis and accelerated decision-making processes, both of which enable organizations to mitigate risks faster and more effectively.

5. REDUCED ALERT FATIGUE AND NOISE

One of the biggest challenges with traditional AppSec tooling (and security monitoring, in general) is alert fatigue. Traditional AppSec deployments often overwhelm teams with a deluge of alerts, many of which are false positives or low-priority issues. A data fabric dramatically reduces this noise (in OX's case, by 97%) by intelligently filtering alerts and providing only the most relevant, high-priority issues for review. The benefit: the drastic reduction in alert volume helps prevent burnout and allows teams to focus efforts on genuine issues.

6. INCREASED EFFICIENCY THROUGH AUTOMATION

A data fabric integrates data from various tools and sources into a single, unified management plane, which enhances automation. Development and security workflows can be streamlined, from vulnerability identification to remediation, with less manual effort. The benefit: Teams can maintain a high level of security without manual intervention for low-level tasks. This allows humans to focus on strategic decisions that enable faster and more accurate issue resolution.

7. REACHABLE VULNERABILITY INSIGHTS

Beyond simply identifying vulnerabilities, a data fabric provides deeper insights into which vulnerabilities are reachable and exploitable. The benefit: This critical information helps AppSec teams understand the actual business impact of potential threats, prioritize remediation based on actual risk, and reduce wasted effort on low-risk issues.

8. SIMPLIFIED COMPLIANCE AND REPORTING

For organizations that need to demonstrate compliance with regulations like GDPR, HIPAA, or PCI-DSS, a data fabric offers an integrated view that simplifies reporting. By providing a consolidated, real-time picture of an organization's security posture, a data fabric makes it easier to generate accurate, up-to-date compliance reports. The benefit: a decreased burden on audit, compliance, and security teams and demonstrably improved governance.

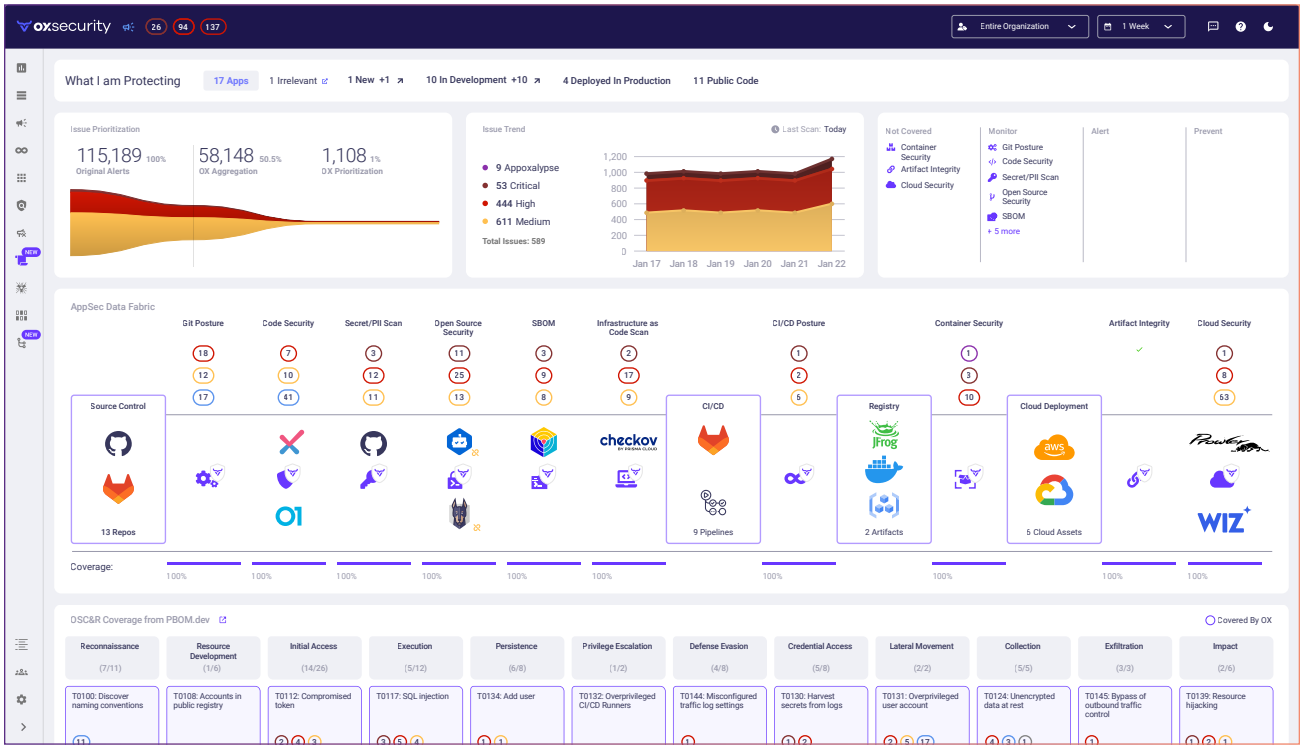
Why Choose an AppSec Data Fabric?

Many application security posture management (ASPM) companies can claim they use a data fabric architecture for AppSec data aggregation, normalization, deduplication, enrichment, vulnerability prioritization, and automated remediation. The concept of data unification has been around for years, and it's seen throughout all categories of cybersecurity tools. However, the missing element that turns this "table stakes" approach into a true AppSec Data Fabric is the provider's ability to baseline the collected, normalized, etc. data with reliable information from scanning solutions that are linked at their core — built on a connected architecture, using a common language.

The Data Fabric approach yields the highest caliber data because there aren't inconsistencies in the baseline source data. Coupling this high-quality data that is supplemented with context and reachability and exploitability analyses substantively reduces the noise of non-critical or irrelevant alerts that distract DevOps and security teams from real risks. What's more, a true AppSec Data Fabric incorporates and assesses critical environmental factors like compensating controls, connected technology stacks, and transitive dependencies. This is why an AppSec Data Fabric offers a superior approach to application and software security.

While stitching together data from disparate tools is better than no solution at all, the pure aggregation model falls short when it comes to noise reduction, prioritization, and actionability.

With an AppSec Data Fabric, DevOps and AppSec teams get an end-to-end view of the security posture of the entire SDLC — without gaps or blind spots. It is a streamlined process for security and development because it centralizes management of vulnerabilities and automates routine tasks, allows users to create custom workflows, and frees up both developers' and security teams' time to focus on higher-level, strategic issues that could impact the organization's ability to function normally.



Top Use Cases for an AppSec Data Fabric

REDUCE THE NOISE

An AppSec Data Fabric addresses noise and alert fatigue through active context and business-specific vulnerability prioritization. It identifies and prioritizes the most critical risks within organizations' environments, reducing security load and debt.

PRIORITIZE RISK

A multi-layered system based on factors such as exploitability, reachability, and business impact are built into a true AppSec Data Fabric. This contextual data clarifies the risk priorities for critical threats and streamlines alert handling, which allows security teams to focus on fixing high-priority security vulnerabilities while minimizing time wasted on non-critical issues that won't substantially impact business.

IMPROVE MEAN TIME TO REMEDIATION

An AppSec Data Fabric enhances visibility and traceability across users' SDLC with a unified view, seamlessly interfacing with their ecosystem, allowing a user to quickly identify an issue and respond. This provides the basis for detailed attack path mapping, which, in turn, facilitates identification, triage, and mitigation of the highest severity problems. Coupled with no-code automated workflows that can be configured per user and per organization, an AppSec program built on a data fabric reduces the need for manual efforts, increases accuracy, and keeps development cycles on track.

oxsecurity

Conclusion

In today's complex application security landscape, piecing together data from multiple, disparate sources is inefficient, time-consuming, and error-prone. An AppSec Data Fabric provides a superior solution by unifying data collection, normalization, and analysis in a single platform. It offers a complete, contextualized view of an organization's application security posture, diminishes alert noise, and automates big hunks of the remediation process. By prioritizing the most critical threats and streamlining workflows, a Data Fabric enables DevOps and AppSec teams to be more efficient and effective, ultimately lowering risk across the entire organization.

ABOUT OX SECURITY

At OX Security, we're simplifying application security (AppSec) with the first-ever Active ASPM platform offering seamless visibility and traceability from code to cloud and cloud to code. Leveraging our proprietary AppSec Data Fabric, OX delivers comprehensive security coverage, contextualized prioritization, and automated response and remediation throughout the software development lifecycle. Recently recognized as a Gartner Cool Vendor and a SINET 16 Innovator, OX is trusted by dozens of global enterprises and tech-forward companies. Founded by industry leaders Neatsun Ziv, former VP of CheckPoint's Cyber Security business unit, and Lior Arzi from Check Point's Security Division, OX's Active ASPM platform is more than a platform; it empowers organizations to take the first step toward eliminating manual AppSec practices while enabling scalable and secure development.

INTERESTED IN LEARNING MORE VISIT: WWW.OX.SECURITY/BOOK-A-DEMO/

oxsecurity