

Safeguard Salesforce with Comprehensive SaaS Security

The Challenge

The security of Salesforce is not just a technical requirement but a business imperative, given its role as a central repository for critical business data. As Organizations grow, the scale and complexity of Salesforce environments also grows. Maintaining visibility and control over configurations, user permissions, and data access across numerous Salesforce orgs becomes cumbersome. The shared responsibility model underscores this challenge; while Salesforce provides a secure infrastructure, it is incumbent upon organizations to manage configurations and access controls effectively.

This is not a trivial undertaking, as evidenced by AppOmni's SaaS risk assessments, which found that over 95% of companies had over-permissioned and inactive users in their Salesforce instances. This directly correlates to the insufficient user access control and oversight, which can lead to unauthorized access and potential data breaches. Misconfigurations that expose sensitive data and vulnerabilities from third-party apps connected to Salesforce further compound these risks.

One of the key challenges is that organizations are simply unaware of the extent and complexity associated with ensuring correct app configuration and permission settings for each app instance. Manual processes simply are unable to keep up with the significant changes that occur on a daily and weekly basis.

Implementing a comprehensive security solution is essential to mitigate these significant risks and safeguard data integrity.

The Solution

AppOmni ensures robust security for Salesforce by establishing a secure connection to monitor and safeguard the entire platform. Its continuous monitoring and deep scanning capabilities proactively detect and mitigate risks such as misconfigurations, lack of MFA enforcement, and vulnerabilities and threats including unauthorized third-party app connections, offering a strong defense against breaches. AppOmni monitors for malicious, suspicious, or anomalous activity within Salesforce, generating notifications or alerts when



THE CHALLENGE

- Large deployments across multiple Salesforce orgs are diverse and complex
- Difficult to manage and monitor dynamic Salesforce configurations and security controls
- Permissions oversight is often lax and leads to access risk
- Inadvertent misconfigurations by users who are not responsible for security exposes sensitive data



THE BENEFITS

- Enhanced visibility and granular control over your Salesforce ecosystem at any scale
- Proactive threat detection enabling rapid response
- Streamlined compliance and audit readiness
- Secure Salesforce tenants with transparent and guided remediation

potential security incidents are detected. As deployments grow in size and complexity, the alert system continuously monitors for threats without requiring increases in manual oversight or resources. AppOmni's identity security capabilities enhance access control measures by providing an identity-centric view of users and their permissions across multiple SaaS applications, helping to proactively manage the SaaS attack surface.

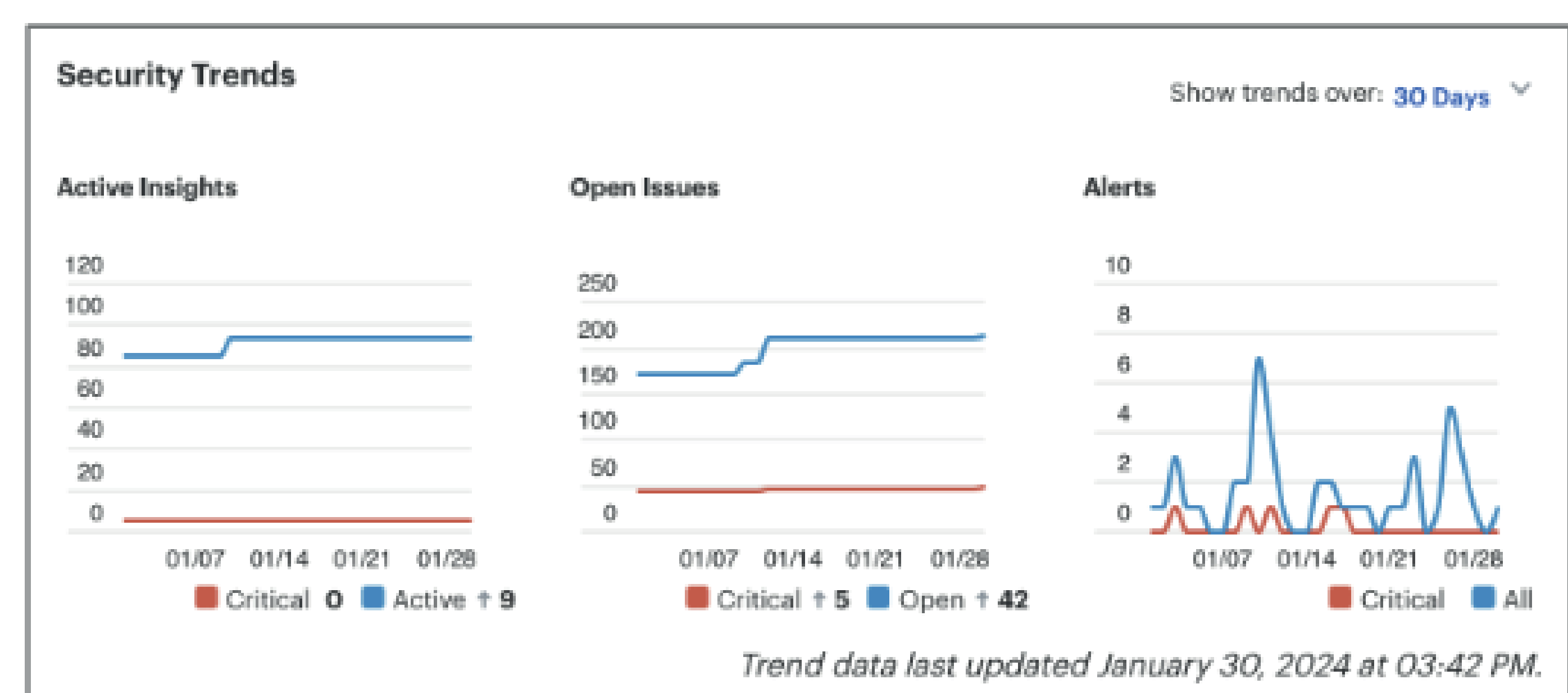
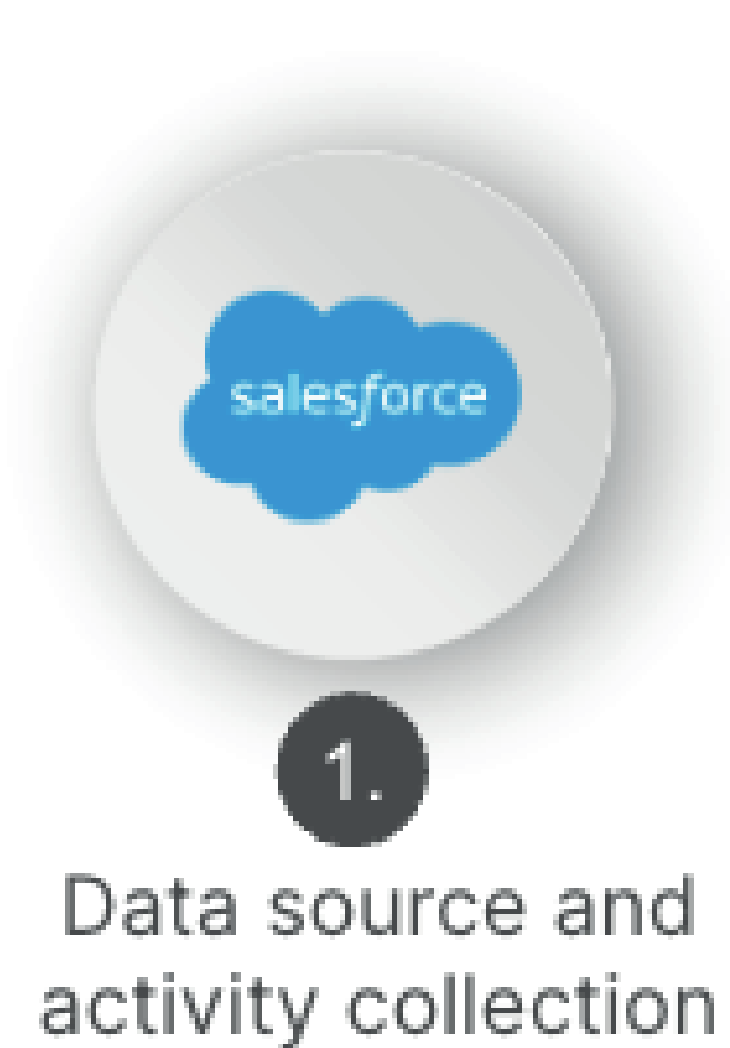
In addition to Salesforce, AppOmni provides visibility into the broader SaaS ecosystem customers are leveraging today, empowering these organizations to effectively manage cyber risks and maintain compliance at any scale. Visualization tools aid in discovering and monitoring third-party app connections, preventing data leakage and ensuring ecosystem integrity. Simplify compliance reporting and security audits, with on-demand compliance reports that provide actionable insights for administrators. With AppOmni's comprehensive security approach and real time security command center, organizations can safeguard their sensitive data in the Salesforce ecosystem and beyond.



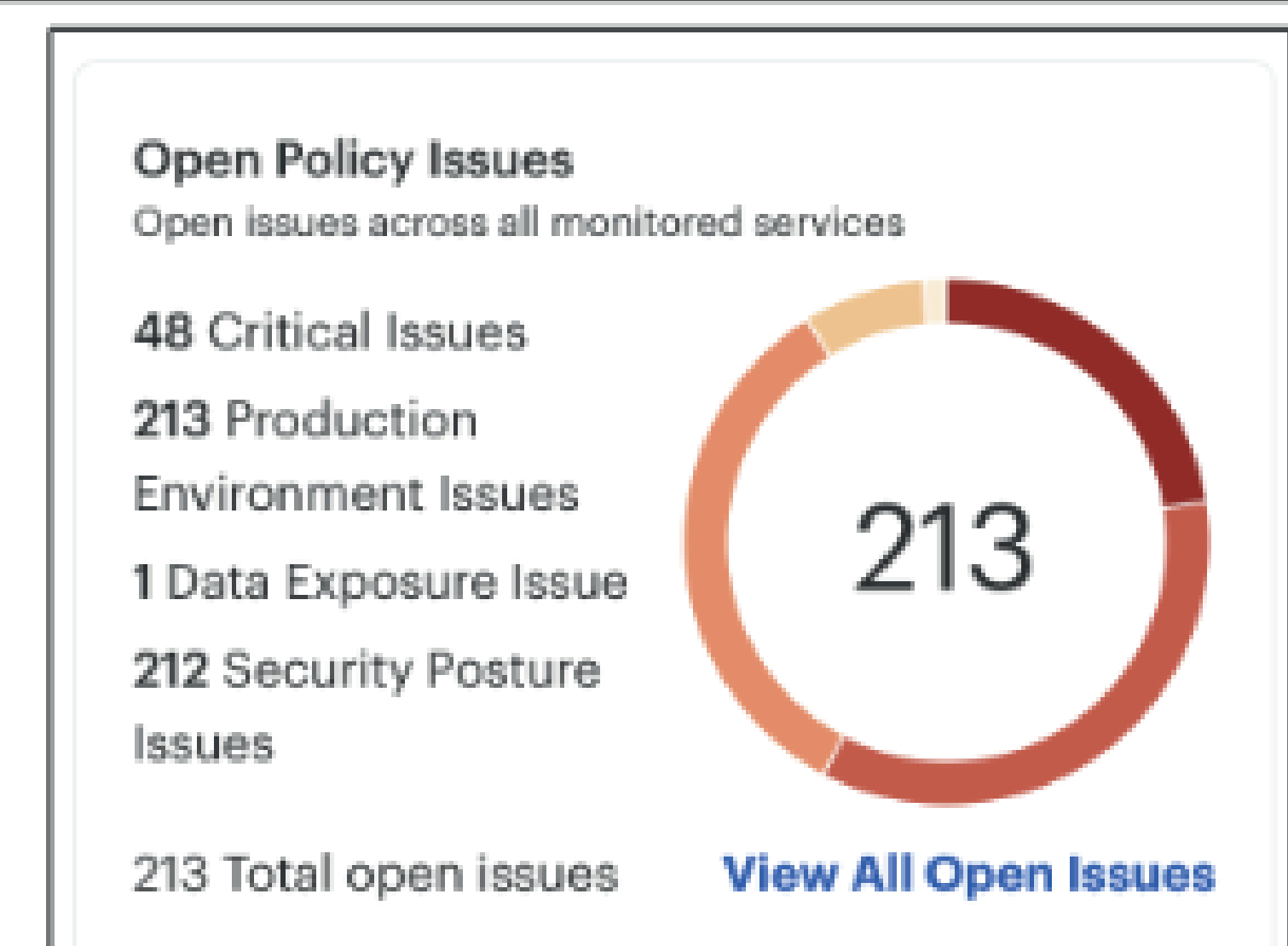
THE SOLUTION

- Continuous Monitoring
- Config and Posture Assessments
- Threat Detection
- Identities and Access Explorer
- Third-party Access Monitoring
- Compliance and Security Audits
- Vulnerability scanning & remediation

Continuous Security Monitoring



3. Analyze Salesforce compliance and security postures from a centralized AppOmni console

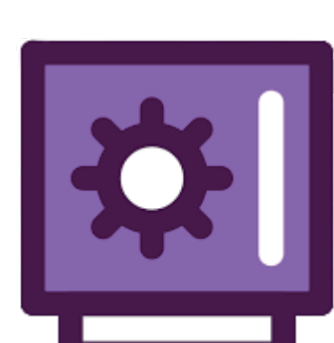


Key Capabilities

AppOmni's SaaS Security platform mitigates Salesforce security risks by providing Security, Compliance, and IT teams with the proper tooling to effectively manage security across all Salesforce environments.



Health Cloud



Financial Services Cloud



B2B Cloud



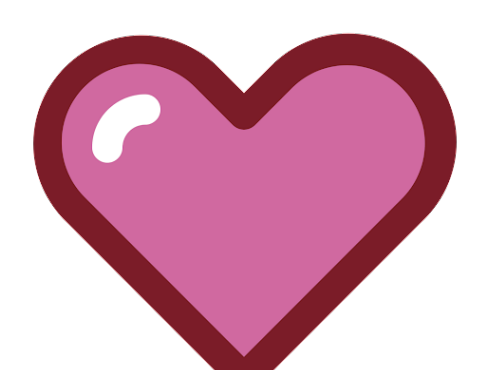
Custom Apps



Marketing Cloud



Sales Cloud



Service Cloud

KEY CAPABILITIES

Capabilities	Description	Real World Example
Advanced Scanning and Monitoring	AppOmni's advanced scanning for Salesforce detects specific risks including data records exposed to the anonymous world, external users with API access, secrets stored insecurely and more, alerting administrators to secure data proactively.	A hospital network was alerted by AppOmni's advanced scanning for Salesforce when a misconfiguration allowed external contractors API access to patient treatment records, enabling the hospital's IT team to promptly revoke the access and prevent a potential violation of patient privacy and healthcare regulations.
Identities and Access Explorer	Ensure only authorized users have access. AppOmni synchronizes user identities, aligning and maintaining an up-to-date view of users and their associated permissions across Salesforce and your SaaS ecosystem providing a centralized view of users and their sub-accounts.	A retail organization leveraged AppOmni to synchronize and maintain an up-to-date view of employee access permissions across Salesforce and other SaaS applications, ensuring that only authorized sales representatives could access customer data.
Third-party Access Monitoring	Get a comprehensive view of connected SaaS applications to your Salesforce environment with unparalleled visibility into data access and the ability to manage compliance and security risks across your organization's SaaS landscape.	A tech startup identified an unauthorized third-party app connected to their Salesforce instance through AppOmni's SaaS-to-SaaS access monitoring. Once identified, they immediately severed the connection, preventing potential data leakage and securing their sensitive customer data.
Compliance and Security Audits	Administrators can export data directly from the table views in AppOmni, which aids in compliance reporting and security audits.	A financial services firm prepared for an upcoming audit by using AppOmni. They streamlined their reporting process by exporting compliance-related data directly from AppOmni's compliance dashboard, quickly gathering the necessary documentation to prove compliance with industry regulations.
Vulnerability scanning & remediation	Simplify Salesforce security, offering intuitive scanning and guided fixes, ensuring robust protection without needing expert knowledge.	Prior to deploying a new CRM feature, a tech enterprise leveraged AppOmni to conduct targeted scans of their Salesforce permissions, swiftly correcting misconfigurations and enhancing access controls, streamlining security without deep technical know-how.

About AppOmni

AppOmni's patented technology scans APIs, security controls, and configuration settings to compare the current state of enterprise SaaS deployments against best practices and business intent. The solution offers fast deployment, deep visibility, and makes it easy for security and IT teams to protect and monitor the entire SaaS environment, from each vendor to every end user. As SaaS applications evolve, AppOmni stays current with all updates and releases to keep customer environments secure over time.

To learn more, email us at info@appomni.com or visit appomni.com