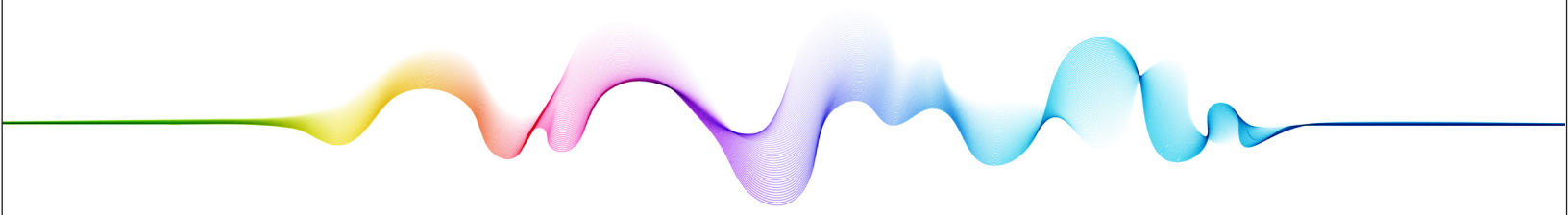
INSIGHT REPORT

OVERVIEW OF APPLICATION SECURITY COMMERCIAL MARKET



TAG CYBERSECURITY

TAG Insights Report Overview of Application Security Commercial Market

Prepared by
Dr. Edward Amoroso
Chief Executive Officer, TAG Infosphere, Inc.
Research Professor, NYU
eamoroso@tag-cyber.com

Version 1.0
February 4, 2024

Introduction

This TAG Insights Report on *Application Security* is intended to help companies, managers, practitioners, researchers, investors, and commercial vendors better understand current trends, issues, and market opportunities in this area. A list of representative commercial vendors working in various areas of application security is included. The five specific areas of covered in this report include:

1. API Security
2. Application Security Testing
3. Application Security Posture Management (ASPM)
4. Runtime Application Security
5. Software Bill of Materials (SBOM)/ Software Compositional Analysis (SCA)

This report is intended for general and unrestricted use, but interested readers are encouraged to connect with the TAG research and advisory team for more information on the private TAG Research as a Service (RaaS) community that covers, discusses, and shares information on these topics in more depth and includes a wider range of startups, vendors, and companies.

TAG Taxonomy

We organize this TAG Insights Report as per our updated TAG Taxonomy which includes twenty categories of modern solution areas where stakeholders and buyers can find suitable commercial products and services for purchase and use. Each category has five subcategories

that correspond to the main areas in which practitioners can focus. These subcategories are discussed below.

1 Application Security 1.1 API Security 1.2 Application Security Testing 1.3 Application Security Posture Mgmt. 1.4 Runtime Application Security 1.5 SBOM/SCA	**6 Email Security** 6.1 Anti-Phishing Tools 6.2 DMARC 6.3 Email Encryption 6.4 Phish Testing and Training 6.5 Secure Email Gateway	**11 Identity and Access Management** 11.1 Authorization 11.2 IAM Platforms 11.3 identity, Anti-Fraud, and KYC 11.4 Identity Governance and Admin. 11.5 Privileged Access Management	**16 Operational Technology Security** 16.1 ICS/OT Device Security 16.2 ICS/OT Visibility 16.3 Unidirectional Gateway 16.4 Vehicle Security 16.5 Zero Trust OT
2 Attack Surface Management 2.1 Bug Bounty Services 2.2 External Attack Surface Management 2.3 Automated Pen Testing/Red Teams 2.4 Breach and Attack Simulation 2.5 Security Ratings Platforms	**7 Encryption and PKI** 7.1 Certification Authority (CA) 7.2 Data Encryption 7.3 Key and Secret Management 7.4 Key and Certificate Protection 7.5 Post-Quantum Cryptography	**12 Security Operations and Response** 12.1 Data Forensics and eDiscovery 12.2 Incident Response 12.3 SIEM Platforms 12.4 SOC/SOAR Support 12.5 Threat Hunting	**17 Security Professional Services** 17.1 Penetration Testing 17.2 Security Assessments 17.3 Security Research and Advisory 17.4 Security Training 17.5 Value Added Resellers
3 Authentication 3.1 Biometrics 3.2 Multifactor Authentication 3.3 Passwordless Authentication 3.4 Password Management 3.5 Single Sign-On	**8 Endpoint Protection** 8.1 Antivirus Software 8.2 Browser Isolation 8.3 Content Disarm and Reconstruction 8.4 Endpoint Detection and Response 8.5 Security Enhanced Browser	**13 Managed Security Services** 13.1 DDOS Security 13.2 Managed Detection and Response 13.3 Managed Security Services Platform 13.4 Network Detection and Response 13.5 XDR Services	**18 Software Lifecycle Security** 18.1 AI/MLOps Security 18.2 Container/Kubernetes Security 18.3 Container Scanning 18.4 DevSecOps Platforms 18.5 Infrastructure-as-Code Security
4 Cloud Security 4.1 Cloud Data Fragmentation 4.2 Cloud Infrastructure Entitlement Mgmt. 4.3 Cloud Security Posture Management 4.4 Cloud Workload Protection Platform 4.5 Microsegmentation	**9 Enterprise IT Infrastructure** 9.1 Asset Inventory 9.2 Backup Platform 9.3 Infrastructure Resilience 9.4 Physical Security 9.5 Secure Sharing and Collaboration	**14 Mobility Security** 14.1 IOT Security 14.2 Mobile App Security 14.3 Mobile Device Management 14.4 Mobile Device Security 14.5 Mobility Infrastructure Security	**19 Threat and Vulnerability Management** 19.1 Digital Risk Protection 19.2 Security Scanning 19.3 Third Party Risk Management 19.4 Threat and Vulnerability Platform 19.5 Threat Intelligence
5 Data Security 5.1 Cloud Data Security Posture Mgmt. 5.2 Data Access Governance 5.3 Data Discovery and Classification 5.4 Data Leakage Protection 5.5 Data Privacy Platform	**10 Governance, Risk, and Compliance** 10.1 Continuous Compliance 10.2 Cyber Insurance 10.3 Incident Reporting 10.4 GRC Platform 10.5 Risk Management Platform	**15 Network Security** 15.1 Network Access Control 15.2 Next Generation Firewalls 15.3 Secure Access Service Edge (SSE) 15.4 Virtual Private Networks 15.5 Zero Trust Network Access	**20 Web Security** 20.1 Bot Management 20.2 Content Security 20.3 Secure Web Gateway 20.4 Web Application Firewall 20.5 Website Scanning

Figure 1. TAG Taxonomy for Cybersecurity

Overview of Application Security

The following emerging global commercial opportunities involving application security solutions are covered in this report, including the listing of several viable commercial entities providing solutions on the market today:

- Application programming interfaces (APIs) serve as essential bridges between different software components and systems, facilitating data exchange and functionality. However, they can also expose vulnerabilities if not properly secured. Application security involves rigorous API security measures, such as access controls, authentication, and encryption, to prevent unauthorized access and data breaches via API endpoints.
- Application security testing has always been an important component of the overall application security marketplace with a plethora of options for static, dynamic, interactive, and other forms of application security testing tools.
- Application security posture management (ASPM) typically references platforms that attempt to provide a single source of truth to identify, correlate, and prioritize security vulnerabilities across the software development lifecycle.
- Runtime application security focuses on the execution cycle for software to ensure that attention is placed on use-case analysis during the runtime behavior of an application.

- Software bill of materials (SBOM) and software compositional analysis (SCA) represent a collective effort by the application security community expose the components used to develop software, with particular emphasis on open source.

Application security thus encompasses the processes and technologies designed to minimize the vulnerabilities and risks associated with applications. These vulnerabilities can be exploited by cybercriminals for a range of malicious activities, including data breaches, financial fraud, and service disruption. The evolving threat landscape and the increasing reliance on software-driven solutions have pushed organizations to prioritize and invest in robust practices.

Focus Area: API Security

API Security, now commonly accepted as a required component of overall application security, plays a pivotal role in safeguarding data integrity, confidentiality, and availability during data exchanges between software components. Modern focus on securing APIs has certainly intensified, creating opportunities startups and established vendors to innovate and address evolving threats. The massive funding levels for many API security startups offers evidence of this enthusiasm.

API security solutions often encompass tokenization, where sensitive data within API payloads is replaced with tokens to mitigate the risk of data exposure. Startups are also developing specialized API gateways, security protocols, and authentication mechanisms to ensure comprehensive API protection. Established security vendors are also extending product portfolios with API security modules, typically featuring API key management, OAuth 2.0 authentication, and encryption protocols. Much emphasis is being placed on securing API endpoints, promoting secure API design practices, and addressing the demand for API security across enterprise.

API security strategies for both startups and vendors include continuous monitoring, anomaly detection, and threat intelligence integration. They also emphasize the importance of access controls, rate limiting, and content validation to protect APIs against unauthorized access and data manipulation. Adoption of API security standards, such as OpenID Connect and OAuth 2.0, is a common strategy for ensuring interoperability and adherence to industry best practices. Real-time threat detection and response mechanisms are integral components of API security solutions to combat emerging threats effectively.

Focus Area: Application Security Testing

Application Security Testing has always been key to cybersecurity, encompassing a broad range of methodologies and tools designed to identify and remediate vulnerabilities within software applications. As software becomes increasingly complex, the importance of application security testing has never been more vital. Both startups and established vendors are actively engaged in this domain, employing various innovative strategies to enhance testing capabilities and mitigate threats, especially zero-day issues.

Startups in application security testing generally focus on one or more combinations of dynamic analysis, static analysis, and interactive application security testing (IAST) technologies to scan application code comprehensively. Automation is obviously central to their strategies, enabling rapid detection of vulnerabilities while minimizing false positives. These startups recognize the need to integrate seamlessly into modern DevOps pipelines, where continuous delivery and deployment are the norm.

Established security vendors also commonly include application security testing suites. AI and machine learning are usually featured, enhancing the accuracy of vulnerability scanning and reducing manual verification. The focus extends beyond traditional applications to encompass modern architectures, including cloud-native and microservices-based systems. These vendors prioritize comprehensive code coverage. Key elements of application security testing strategies include:

1. Scalability: Both startups and vendors recognize the importance of scalability, ensuring that testing tools can accommodate the ever-expanding scope of modern applications. This scalability ensures that large enterprises with diverse application portfolios can efficiently test all components for vulnerabilities.
2. Integration: Seamlessly integrating with development and DevOps workflows is essential. Startups aim for lightweight integrations that do not disrupt existing processes, while established vendors emphasize compatibility with popular development tools and CI/CD pipelines.
3. Comprehensive Coverage: Application security testing must provide holistic coverage, encompassing both legacy and modern application architectures, including web, mobile, and cloud-native environments. Additionally, the ability to assess third-party components and dependencies is vital.
4. Accurate Reporting: Precise reporting mechanisms, including detailed vulnerability descriptions and remediation recommendations, are a hallmark of effective application security testing. Clear reporting aids development and security teams in efficiently addressing identified vulnerabilities.

Application security testing is an evolving field that reflects the increasing complexity of modern software. Startups and established vendors are employing innovative tools and techniques to meet the demand for comprehensive, automated, and accurate vulnerability assessments. As software complexity continues to increase, the role of application security testing remains indispensable in protecting critical data and ensuring the security of applications.

Focus Area: Application Security Posture Management (ASPM)

Application security posture management (ASPM) has emerged as a key component of modern cyber, focusing on proactively monitoring and enforcing security policies within software applications. This discipline enables organizations to maintain a strong security posture, mitigate risks, and swiftly respond to emerging threats. Both startups and established vendors

recognize the significance of ASPM and employ strategic approaches to offer innovative solutions in this domain (perhaps inspired by External Attack Surface Management (EASM)).

Startups entering the ASPM landscape typically provide real-time visibility into an organization's security status, enabling security teams to identify vulnerabilities, policy violations, and anomalies promptly. These startups emphasize automation, utilizing machine learning algorithms for anomaly detection, threat intelligence integration, and adaptive policy enforcement. A central tenet of their commercial strategies is ease of integration with existing security infrastructure, ensuring minimal disruption to organizational workflows.

Established security vendors offering ASPM are characterized by continuous monitoring capabilities, compliance reporting, and risk mitigation features. Integration with Security Information and Event Management (SIEM) systems is standard, allowing organizations to correlate security posture data with broader threat intelligence. Commercial strategies frequently involve subscription-based licensing models, with scalability options for organizations of varying sizes and complexity. Key elements of ASPM strategies include:

1. Real-Time Monitoring: Both startups and established vendors recognize the need for real-time monitoring of applications to promptly detect and respond to security incidents and vulnerabilities as they emerge.
2. Compliance Management: ASPM solutions emphasize compliance reporting to ensure organizations adhere to industry regulations and internal security policies, providing clear insights into areas of non-compliance.
3. Anomaly Detection: Machine learning algorithms play a crucial role in anomaly detection within ASPM platforms. They analyze application behavior to identify deviations from the norm, potentially indicating security incidents or policy violations.
4. Policy Enforcement: Adaptive policy enforcement is integral to ASPM, ensuring that security policies are consistently applied and adjusted in response to evolving threats and organizational requirements.
5. Integration: Both startups and established vendors emphasize seamless integration with existing security infrastructure, including SIEM, endpoint protection, and threat intelligence feeds.

ASPM thus enables organizations to maintain a robust security posture. Startups and established vendors provide real-time insights, automated policy enforcement, and compliance management. As organizations prioritize security posture management to protect sensitive data and maintain customer trust, the ASPM market continues to evolve, offering comprehensive solutions to address emerging security challenges.

Focus Area: Runtime Application Security

Runtime application security platforms focus on the monitoring and protection of software applications while they are executing. It provides organizations with the ability to detect and

mitigate threats as they occur in real-time, ensuring the integrity and availability of applications.

Startups supporting runtime application security often support runtime application self-protection (RASP) technologies, which employ behavioral analysis and artificial intelligence (AI) to detect and respond to threats as they emerge. A key element of their strategies is seamless integration with existing application environments, ensuring minimal performance overhead. They focus on providing real-time visibility into application behavior, anomaly detection, and adaptive threat response mechanisms.

Established security vendors often provide advanced threat detection capabilities, zero-day vulnerability protection, rapid threat response, and scalability. Machine learning and AI technologies play a key role in improving the accuracy of threat detection and response. Key elements of Runtime Application Security strategies include:

1. Behavioral Analysis: Both startups and established vendors recognize the importance of behavioral analysis, which involves continuously monitoring application behavior to identify deviations from the norm, potentially indicating security threats.
2. Zero-Day Vulnerability Protection: Advanced runtime security solutions focus on protecting against zero-day vulnerabilities and previously unknown threats by employing heuristics and AI-driven detection mechanisms.
3. Real-Time Threat Response: Rapid threat response mechanisms are essential, allowing organizations to take immediate action to mitigate threats as they emerge during application runtime.
4. Scalability: Runtime security solutions must be scalable to accommodate the dynamic nature of modern applications and their varying workloads.
5. Integration: Seamless integration into existing application environments, including support for both traditional and cloud-native architectures, is a cornerstone of effective runtime security strategies.

Startups and established vendors are at the forefront of innovation in runtime security, offering solutions that provide real-time threat detection and response capabilities. As organizations increasingly rely on applications for critical operations, the need for robust runtime security continues to grow. The runtime application security market is thus poised for further development and growth.

Focus Area: Software Bill of Materials (SBOM)/Software Compositional Analysis (SCA)

Software bill of materials (SBOM) and software composition analysis (SCA) collectively address the need for software supply chain security. These disciplines enable organizations to gain visibility into the software components and dependencies used in their applications, assess associated vulnerabilities, and ensure a robust and secure software supply chain. In this context, both startups and established vendors employ strategic approaches to provide innovative solutions in SBOM and SCA.

Startups venturing in SBOM and SCA domains tend to focus on developing specialized tools and platforms that facilitate the creation, maintenance, and analysis of SBOMs, especially for open source. These tools integrate seamlessly into development workflows and provide comprehensive insights into software components, their versions, and known vulnerabilities. Startups recognize the importance of continuous monitoring and updating of SBOMs to keep pace with the rapid changes in software supply chains.

Established security often offer capabilities for generating, managing, and analyzing SBOMs. Integration with vulnerability databases and automated risk assessment are integral components of their solutions. Moreover, they emphasize the importance of supply chain risk management and compliance tracking, ensuring that organizations can effectively secure their software supply chain. Key elements of SBOM and SCA strategies include:

1. Visibility: Both startups and established vendors emphasize the need for visibility into software components and dependencies to assess their security posture accurately.
2. Automation: Automation is a central element in SBOM and SCA strategies, enabling the continuous monitoring and analysis of software components and vulnerabilities.
3. Integration: Seamless integration into existing development pipelines and security workflows is crucial to ensure the adoption of SBOM and SCA practices across the organization.
4. Comprehensive Analysis: Effective SBOM and SCA solutions offer comprehensive analysis of software components, including third-party libraries, open-source software, and their associated vulnerabilities.
5. Vulnerability Management: These solutions typically include vulnerability management features, enabling organizations to prioritize and remediate software supply chain risks effectively.

SBOM and SCA have become indispensable in safeguarding the software supply chain. Startups and established vendors are actively innovating in this domain, offering solutions that provide visibility, automation, and comprehensive analysis of software components. As organizations increasingly recognize the importance of securing their software supply chain to prevent supply chain attacks and vulnerabilities due to outdated dependencies, the SBOM and SCA market continue to evolve, offering comprehensive solutions to address emerging security challenges.

Companies and Contributions

The companies listed below emerged as part of our research at TAG. Our goal in listing these fine firms is to provide a starting point for buyers, advocates, stakeholders, and researchers trying to make sense of the commercial landscape for application security as a means for driving toward reduced global cyber risk.

API Security Vendors

1. 42Crunch: Specializes in API security, offering API contract security, runtime protection, and comprehensive testing.
2. Akamai: Akamai includes an API protector as part of its edge security.
3. Akana: Focuses on the provision of API security and management, ensuring secure and optimized APIs.
4. Apigee: Apigee by Google, provides API management and security solutions to help organizations design, secure, and analyze their APIs.
5. APIsec: APIsec Platform offers automated API security testing that can generate and execute thousands of attack scenarios to cover the OWASP and business logic flaws.
6. Axway: Offers API management and security solutions, ensuring the secure flow of data across APIs.
7. Bright Security: Formerly known as Neurolegion, Bright security Offers AI-powered API security solutions, including vulnerability scanning and threat remediation.
8. Cequence Security: API Sentinel offers customers API discovery, risk analysis, and threat protection at the edge of data center or service mesh environments.
9. Cloudflare: Offers API security solutions with DDoS protection, access control, and rate limiting.
10. Data Theorem: Focuses on API security and runtime application security, providing automated security analysis and threat detection.
11. Human Security: Formerly known as PerimeterX, Human Security focuses on API security and bot protection, safeguarding APIs from automated threats.
12. Impelsys: Provides a range of API security solutions with access control and encryption features.
13. Imperva: Provides API security solutions with threat detection, access control, and data protection capabilities.
14. Micro Focus: Fortify is an extensible application security platform that helps enterprises deliver secure code at scale.
15. MuleSoft: Specializes in API integration and management, enabling secure API connectivity.
16. Noname Security: Provides a security platform that allows enterprises to see and secure managed and unmanaged APIs.
17. Ping Identity: Offers identity and access management solutions, including API security, to protect against unauthorized access.
18. Salt Security: Specializes in API security with a focus on API discovery, protection, and threat prevention.
19. Signal Sciences: Formerly Fastly, Signal Sciences focuses on runtime web application security, providing protection against web application attacks and real-time visibility into threats.
20. Traceable: Provides API security solutions with AI-driven threat detection and behavior analysis.
21. Wallarm: Offers advanced API security solutions with AI-driven threat detection and protection.

Application Security Testing Vendors

1. Acunetix: Offers web application security scanning tools with automated vulnerability detection.
2. Checkmarx: Provides application security testing solutions, including static and dynamic analysis.
3. Datadog: Formerly known as Sqreen, provides runtime application security solutions, including real-time threat detection.
4. Detectify: Focuses on automated web application security testing with continuous monitoring.
5. GitLab: Offers an open-source DevOps platform that provides a complete set of tools for software development.
6. GBG Idology: Formerly known as Acuant, the company offers identity verification and document authentication solutions for application security.
7. HCL Software: Offers HCL AppScan, which focuses on application security testing with dynamic and static analysis.
8. Indusface: Offers a product called AppTrana that specializes in web application security and provides managed security services.
9. Invicti: Formerly known as Netsparker, offers automated web application security scanning tools for vulnerability detection.
10. Micro Focus: The company has been acquired by OpenText and offers a solution called Fortify that provides application security testing solutions with static and dynamic analysis capabilities. They also offer WebInspect that provides dynamic application security testing tools for vulnerability assessment.
11. OWASP: Offers ZAP, an open-source web application security scanner for vulnerability testing.
12. PortSwigger: Offers their product called Burp Suite that focuses on web application security testing with features for scanning and manual testing.
13. Contrast Security: Offers a range of interactive and dynamic application security testing solutions.
14. Qualys: Provides application security testing tools and vulnerability management solutions.
15. Rapid7: The company offers a product called AppSpider that specializes in web application security testing with automated scanning and reporting.
16. Synopsys: Specializes in application security testing with static analysis, dynamic analysis, and software composition analysis.
17. Tenable: Provides advanced vulnerability management and application security testing solutions.
18. Veracode: Offers static and dynamic application security testing tools for web application vulnerability scanning.
19. VMWare: Now a part of Broadcom, VMware offers a wide range of virtualization and cloud computing software along with application security testing services.

Application Security Posture Management Vendors

1. AlgoSec: Specializes in advanced network security policy management and compliance tracking.
2. Aqua Security: Focuses on cloud-native security posture management, offering protection for containerized applications.
3. Axonius: Provides asset management and security posture assessment solutions for organizations.
4. Blumira: Offers cloud-native security posture management and automated threat detection.
5. Cyber Observer: Formerly known as XMCyber, Cyber Observer offers security posture management solutions for comprehensive security visibility.
6. CyberSkyline: Specializes in security posture assessment and cybersecurity skills development.
7. CyCognito: Provides external attack surface management and security posture monitoring.
8. Fidelis Security: Formerly known as Cloudpassage, Fidelis Cybersecurity is an integrated, automated network and endpoint detection and response platform. Fidelis is engineered for visibility, designed for response and trusted by the most important brands in the world.
9. Fortra: Provides cloud security posture management solutions for securing cloud infrastructure.
10. Fugue: Focuses on cloud security posture management, ensuring compliance and security in cloud environments.
11. Imperva: Imperva provides a range of web application, database file, and cloud security products for protecting business critical data and applications. The company specializes in insider threat and ransomware protection, DDoS protection and API security.
12. Onapsis: Onapsis provides a behavioral-based approach to detecting anomalies against business critical applications with emphasis on SAP.
13. Orca Security: Provides cloud security posture management solutions for comprehensive visibility and threat detection.
14. Palo Alto Networks: Expanse offers attack surface management solutions to help organizations maintain a strong security posture.
15. Panorays: Provides third-party security posture management, ensuring vendor risk assessment and compliance.
16. Progress: Progress transfer enables the consolidation of all file transfer activities to one system to ensure better management control over core business processes.
17. Reveal Security: Monitor malicious activities in applications and platforms.
18. Mastercard: The RiskRecon platform specializes in third-party security risk management and security posture assessment.
19. SecurityScorecard: Focuses on security ratings and security posture assessment for organizations and vendors.
20. Skybox Security: Focuses on security posture management and risk analytics for complex environments.

21. Synopsys: Provides a cloud-based technology platform for web application security.
22. Tenable: Offers security posture management solutions, including vulnerability assessment and continuous monitoring.
23. UpGuard: Provides cyber resilience solutions, including security posture assessment and risk mitigation.
24. Vulcan Cyber: Offers remediation-focused security posture management, helping organizations prioritize and address vulnerabilities efficiently.
25. Xanadata: Offers security posture monitoring and threat detection solutions for organizations.

Runtime Security Vendors

1. Aqua Security: Focuses on container security, including runtime protection for containerized applications.
2. Contrast Security: Offers runtime application security solutions with real-time protection and attack visibility.
3. CrowdStrike: Offers industry-leading endpoint protection and runtime threat detection solutions.
4. Datadog: Provides runtime application security solutions with AI-driven threat detection and protection.
5. Data Theorem: Focuses on API security and runtime application security, providing automated security analysis and threat detection.
6. F5: Focuses on cloud security monitoring and runtime threat detection for cloud-native applications.
7. Fortinet: Specializes in security orchestration, automation, and response, including runtime security incident management.
8. Imperva: Built into the application runtime environment, RASP is capable of detecting and preventing attacks real-time.
9. Signal Sciences: Focuses on runtime web application security, providing protection against web application attacks.
10. Sysdig: Focuses on container security and runtime threat detection for containerized environments.
11. Uptycs: Provides cloud-native security and compliance solutions, including runtime security monitoring.
12. Wallarm: Provides runtime application security solutions with AI-driven threat detection and protection.
13. ZeroNorth: Specializes in risk-based vulnerability orchestration, including runtime threat analysis.

Software Bill of Materials (SBOM) and Software Composition Analysis (SCA) Vendors

1. Anchore: Syft is an open-source tool for generating software bill of materials (SBOM) documents.
2. Checkmarx: CXsca specializes in software composition analysis for identifying open-source vulnerabilities.

3. Cybeats: SBOM Studio is an enterprise-class solution that helps users understand and track their third-party components that are an integral part of their software.
4. Dependency-Track: An open-source platform for tracking and analyzing application dependencies and their vulnerabilities.
5. Finite State: Finite State provides software bill of materials (SBOM) solutions in support of SCA and security objectives.
6. Flexera: Offers software composition analysis solutions for managing software vulnerabilities.
7. GitHub: GitHub's Dependabot provides automated dependency updates and security checks for open-source projects. Retire.js is another popular and familiar open-source tool from GitHub for identifying JavaScript library vulnerabilities.
8. GitLab: Dependency Scanning is part of GitLab's DevSecOps platform, providing dependency scanning capabilities.
9. Gramma Tech: GrammaTech's Binary Software Composition Analysis Tool analyzes the actual code that will run, not build the environment.
10. Insignary: Insignary SCA is designed to support the security and compliance of open-source code to reduce supply chain risk
11. JFrog: Focuses on DevOps and provides solutions for artifact management and software composition analysis.
12. Karamba Security: Karamba Security VCode software identifies, prioritizes, and mitigates security gaps in the software image, specifically third-party modules.
13. Mend: Specializes in open-source software security and provides SCA tools for vulnerability detection.
14. NodeSource: NodeSource provides visibility into application behavior and overall system health with performance metrics.
15. NPM: Specializes in Node.js package management and offers tools for dependency analysis.
16. OWASP: The Offensive Web Testing Framework (OWTF) includes software composition analysis features for web application security.
17. Qwiet.AI: I-SCA checks for attacker relevancy to tell whether a known vulnerability can be accessed by dataflows from the surface of the application.
18. Snyk: Provides developer-focused SCA solutions, helping organizations identify and remediate vulnerabilities in open-source components.
19. Sonatype: Offers software composition analysis solutions, including dependency scanning and vulnerability management.
20. Synopsys: Black Duck offers software composition analysis tools for managing open-source component risks.
21. Veracode: Provides SCA solutions for identifying and mitigating open-source component risks.

About TAG

TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations in cybersecurity,

artificial intelligence, and sustainability to enterprise teams, government agencies, and commercial vendors.