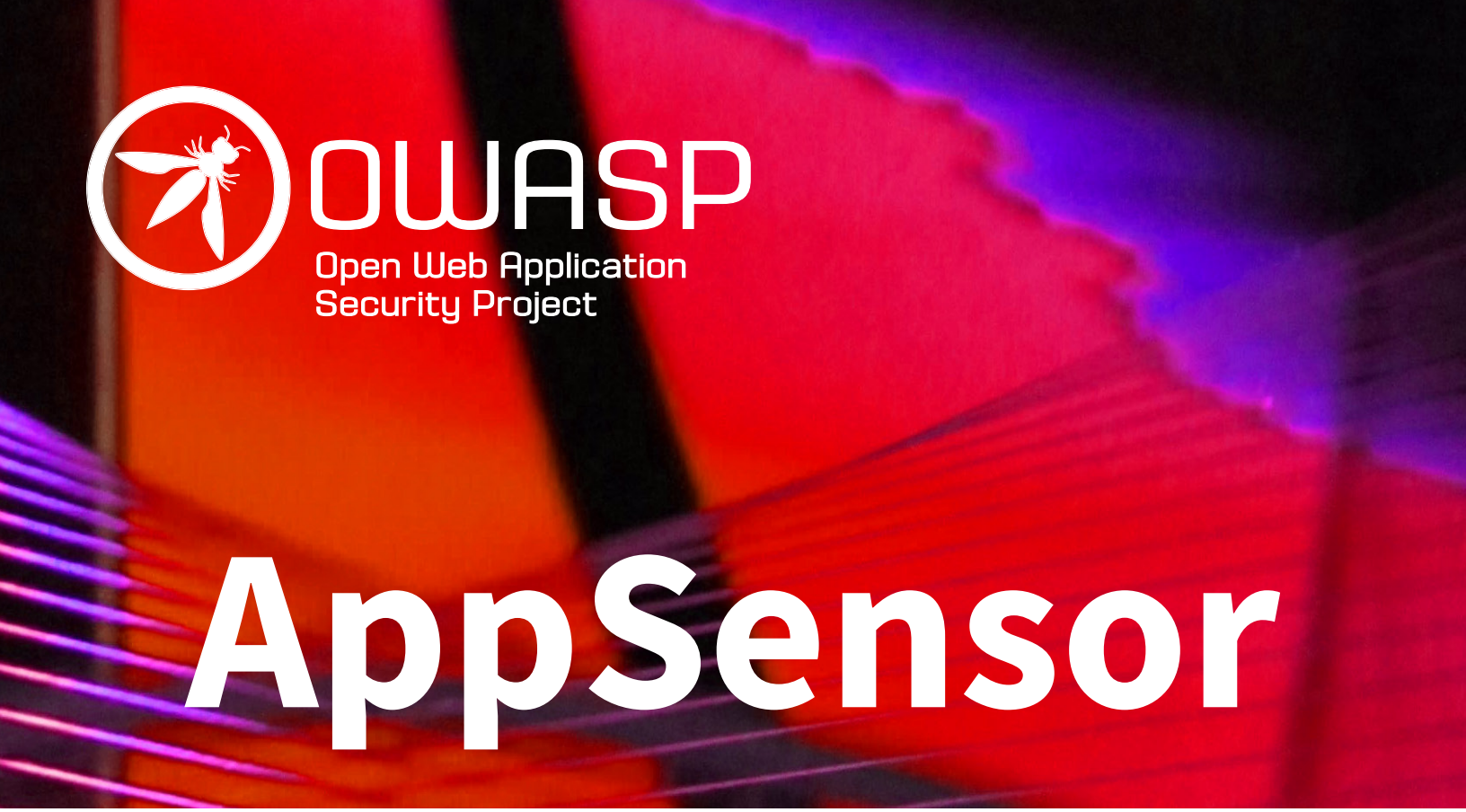


AppSensor

CISO Briefing

OWASP AppSensor CISO Briefing v2.0
Application-Specific Real Time Attack Detection and Response

AppSensor CISO Briefing

AppSensor defines a conceptual framework, methodology, guidance and reference implementation to design and deploy malicious behavior detection and automated responses within software applications. AppSensor instrumentation and telemetry is a deeply integrated proactive approach, originally defined in 2008, with major updates in 2014 and 2015. This briefing document was created to provide senior managers with knowledge about how this forward thinking technique could be utilised as part of application security risk reduction within their organizations. The subsequent pages describe:

- **Defending applications** **2**
- **The application approach** **4**
- **Benefits** **6**
  - **Lower information security risk**
  - **Improved compliance**
  - **Reduced impact of attacks and breaches**
  - **Increased system survivability**
- **Enterprise ready** **8**
  - **Extremely low false positives**
  - **Intelligence driven security**
  - **Low system resource overhead**
  - **Machine-speed response**
- **Next steps** **10**
- **Additional AppSensor resources** **11**
- **Further information** **12**

The OWASP AppSensor Project is a community driven initiative that provides free open source reference materials and code for organizations to define or develop their own application attack detection and response implementations – specific to their own business, applications, environments and risk profile – building upon existing standard security controls.

Defending Software Applications

The security of our applications and services is of paramount importance. Internet connected applications play a role in every aspect of our lives and the operations of society. From financial and medical, through everyday personal and business interactions, to important infrastructure, applications process an immense amount of critical information every single day.

> ***"When asked about their key impediments [to detection and response], visibility is directly implicated as a key issue for respondents, 39% of whom cited lack of visibility into application, underlying systems and vulnerabilities as their overall top impediment to attack detection and response (20% indicated that it was their number 1 impediment)"***
>
> Analytics and Intelligence Survey, SANS Institute, Oct 2014

Despite the importance of these systems, we are yet to integrate advance defenses in many applications. The attackers have determination and are backed by criminal organizations, activist groups, nation states, private enterprises and more. These attackers have the funding, tools and time to infiltrate critical applications. Every day attacks are launched to inspect and probe applications searching for weaknesses and vulnerabilities. The sad reality is that nearly every application is completely blind to these attacks until it is too late.

> ***"Other elements of the Pentagon's strategy include developing 'active defenses' – technologies that detect attacks and probes as they occur, as opposed to 'defenses that employ only after-the-fact detection and notification'"***
>
> Bloomberg Business, Feb 2011

Organizations may place false trust in antiquated defenses such as signature based detection of generic attacks that are trivially bypassed by attackers every day, or reactive log review which is usually too late. We need more. We need a better approach. We need a defense that understands the custom nature of the application – how business logic works, how access control is enforced, and all of the unique aspects of the application. The defense we need must not only detect generic attack techniques, but also custom attacks targeting an application's specific design and architecture.

But advanced detection alone is not enough. The path forward requires a defensive

system that can identify a malicious attacker before they find and exploit a vulnerability. This approach requires the ability to detect and contain an attacker while they are probing for vulnerabilities throughout the application. The response must be swift and fully automatic to eliminate the threat from the application. Reactive analysis by humans is too slow. By the time a human sees an attacker, the attacker will already be gone, along with the critical data they have compromised.

> ***"The future of application defense is a system that can understand custom attacks against an application, correlate them against a malicious attacker, and react in real-time to contain and eliminate the threat. This defense is OWASP AppSensor."***
>
> AppSensor Guide, May 2014

OWASP AppSensor is an open source project created through the contributions of security experts with years of experience assessing, securing and breaking the security systems of applications for financial systems, government bodies, businesses and major organizations around the world.

In 2012 Gartner outlined an emerging security technology in this area, which it named runtime application self-protection (RASP), that is a closely related concept to AppSensor. Gartner's RASP product category currently focuses predominantly on vendor-offerings, and as such touches less on the opportunities available of deeper code-level integration within applications, described and implemented by AppSensor. Organisations can instrument their own applications and build an analysis engine, or use existing event monitoring systems and network security devices, or build upon the AppSensor reference implementation.

> ***"Runtime application self-protection (RASP) is a security technology that is built or linked into an application or application runtime environment, and is capable of controlling application execution and detecting and preventing real-time attacks."***
>
> Gartner, Apr 2012

Detect and Respond to Attacks From Within the Application

Organizations are concerned about protecting their applications, the application users, and related data. The concept of AppSensor is to reduce the risks to these assets by detecting malicious activity within applications. AppSensor is designed to detect activities such as malicious users probing or attacking the application, and to stop them before they can identify and exploit any vulnerability.

> ***"Make application self-protection a new investment priority, ahead of perimeter and infrastructure protection... We believe that by 2020, 25% of Web and cloud applications will become self-protecting, up from less than 1% today."***
>
> Joseph Feiman, Gartner, Sep 2014

This objective is possible because many software vulnerabilities can only be discovered as a result of trial and error by an attacker. Adding AppSensor to an application gives that application the ability to respond to attack attempts by intervening early (oftentimes almost immediately), and blocking those attempts. This approach, if successfully implemented, would make it economically infeasible to attack that application. AppSensor can be used to perform attack determination, real-time response and attack blocking.

It can help to protect software applications against:

- Skilled attackers probing looking for weaknesses
- Misuse of valid business functionality
- Propagation of application worms
- Data scraping and exfiltration
- Application-layer denial of service (DoS)
- As yet unknown attack methods and exploits.

AppSensor is not an application security magic bullet. AppSensor helps defend securely designed and developed applications. It is not a shortcut to deploy security controls. AppSensor will not do these for you. It depends on rigorous input validation practices at every point in the application.

Dynamic defense

In the same way that users are benefitting from responsive design in user interfaces and bandwidth utilization with concepts like progressive enhancement, mobile first and graceful degradation, applications themselves should, and can, alter their normal

deterministic behavior and posture in a predefined manner when under attack to defend themselves, their data and their users. For example, automatically disabling a feature which is being misused until investigations are completed.

> ***"Moving Target – Enables us to create, analyze, evaluate, and deploy mechanisms and strategies that are diverse and that continually shift and change over time to increase complexity and cost for attackers, limit the exposure of vulnerabilities and opportunities for attack, and increase system resiliency"***
>
> National Science and Technology Council, 2011

The application advantage

Detection is undertaken at the application layer where, unlike infrastructure protection devices, the software application itself has access to the complete context of an interaction and enhanced information about the user. The application knows what is a high-value issue and what is noise. Input data are already decrypted and canonicalized within the application and therefore application-specific attack detection is less susceptible to advanced evasion techniques. When appropriate detection points are selected, a very high degree of confidence in attack identification can be achieved, which means the signal can be trusted - this will not be a tool your analysts ignore due to false positives.

High accuracy

AppSensor does not detect software weaknesses or vulnerabilities. Instead it detects users trying to find vulnerabilities. Implementing AppSensor is like defining a whitelist for a subset of application functionality, and noting exceptions to this whitelist (for the functionality/entry points included). Only a sufficiently sized small subset that covers the highest risks, or the most common things done by attackers is needed. AppSensor does not need to detect everything or know about every attack vector.

> ***"The AppSensor project is well-aligned with U.S. Federal Government initiatives for software assurance, especially efforts researching and advancing security technologies like active defenses (with real-time response engines)."***
>
> Resilient Software, US Department of Homeland Security, 2011

Benefits For Organizations and Users

AppSensor is a scalable proactive security approach that detects attackers not vulnerabilities, is application-specific not generic, does not use signatures or try to predict anything, allows applications to adapt in real-time to an identified attacker and thus reduces the impact of an attack.

> ***"[Traditional network defences] do not provide application-specific protection, and if these are all an organization is relying on for application defense, the applications are dangerously exposed and the organization probably does not have insight as to whether the applications are really under attack."***
>
> Michael Coates, AppSensor Project founder, 2015

The most common use cases for deploying AppSensor are:

- Identifying attacks (e.g. application or data enumeration, application denial of service, system penetration, fraud)
- Responding to attackers, including prevention
- Monitoring users (e.g. call center, penetration testing lab)
- Maintaining stability and availability (e.g. application worm propagation prevention)
- Attack intelligence information sharing (e.g. industry verticals, security community).

Application-specific attack detection and response is a comprehensive adaptive approach that can be applied to applications throughout the enterprise. It reduces the risk of unknown vulnerabilities being exploited. The benefits can include:

- Intelligence into whether your applications are under attack, how, and from where
- Certainty due to an extremely high degree of confidence in attack identification
- Fast and fluid responses, using application and user specific contexts
- Protection for software vulnerabilities that you are unaware of
- Defends against future unknown attack methods
- Early detection of both unsuccessful and successful attempts to exploit vulnerabilities
- Insight into users' accidental and malicious misuse
- Information enrichment for conventional network-based intrusion and attack detection systems.

The approach helps to defend organizations (e.g. increased system security, enhanced

data protection, insight into attacks, identification of attempted espionage) and their application users (e.g. privacy protection, malware infection prevention).

> ***"Gartner Group estimates that by 2020, 60% of enterprise information security budgets will be allocated for rapid detection and response approaches, up from less than 10% in 2013."***
>
> Gartner, May 2013

It greatly increases the visibility of suspicious events and actual attacks. This can provide additional information assurance benefits such as lowered information security risk for data and information systems, improved compliance and reduced impact of attacks and breaches, leading to increased system survivability.

> ***"Technology advances and software security program maturity present an opportunity to significantly improve application security by treating the organization's Web infrastructure and IT infrastructure as an ecosystem filled with information that can be mined to determine specific threat trends that are unique to the ecosystem."***
>
> BITS Software Assurance Framework, Financial Services Roundtable, 2012

In turn, these can provide improved service levels and resilience, and competitive advantage. Architects and developers, who have the most knowledge about the intent of an application and its inner workings, can use the techniques described in this guide to build more robust applications that can defend themselves, by adapting the failure response to minimize the impact of the attack, and provide valuable insight into application usage for other systems and processes.

> ***"Some [financial institutions] also have implemented measures to turn off access to certain parts of their online sites, such as search functions, when DDoS activity is detected. These precautions, and others, have helped ensure sites are not completely taken offline by an attack, experts say."***
>
> New Wave of DDoS Attacks Launched, BankInfoSecurity.com, Mar 2013

Enterprise Ready

Although AppSensor capabilities can be built into single applications, a single instance of AppSensor can support multiple client applications.

> ***"Vendor recommended security controls and compliance requirements leave huge gaps in application security… The biggest gap and most pressing need is that most monitoring systems do not understand enterprise applications. To continuously monitor enterprise applications you need to collect the appropriate data and then make sense of it."***
>
> Securing Enterprise Applications, Securosis, 2014

Greater benefits are achievable by developing an enterprise-wide approach that supports:

- Applications deployed across clustered servers
- Distributed applications
- Cloud-based infrastructure monitoring and cloud hosted applications
- Applications where a significant part of the business logic is external to the application (e.g. a mobile app that communicates with a central server)
- Analysis across multiple applications using SSO account correlation.

Further attack detection points and alternative response options can be achieved when AppSensor integrates with existing monitoring systems and network defences:

- Event data from other systems to AppSensor as input, providing a more complete picture for AppSensor to make decisions and give other systems additional options for response (e.g. databases, file integrity monitoring systems, anti-virus systems, web application firewalls, network firewalls)
- Attack data from AppSensor to other systems, sending AppSensor data out to enrich other those (e.g. centralised logging and monitoring, reporting)
- AppSensor using other systems as part of the response giving additional options (e.g. CRM, fraud monitoring/detection systems, network firewalls).

Extremely low false positives

AppSensor does not attempt to identify all malicious behaviour. Instead it is used to determine the intent of a user, and identify them as an attacker based on specific high-confidence signals. This leads to an extremely high confidence level in the identification of someone as an attacker.

Intelligence driven security
Apart from defending an organization's applications, the context-rich live application attack data gathered should be used to augment information from other sources in threat intelligence systems. The attacker identification information is invaluable in first line operational security. Existing SIEM and other technologies suffer from an overload of security alerts, and organisations have insufficient resources to tune the systems producing the alerts or validate the alerts. The high-quality information from application intrusion detection is immediately actionable and can be correlated with other event data for the same sources. For organisations without central collection and analysis, AppSensor's highly-attenuated attack data can be a useful early step down the road to threat intelligence.

Low system resource overhead
AppSensor is best implemented within authenticated parts of applications. And unlike traditional application event with its significant platform overhead, AppSensor-like detection only requires a sub-set of malicious activity to be captured. That is sufficient to determine the intent of a user. Thus the additional overhead in processing and communication by a properly designed system is extremely minor.

Machine-speed response
AppSensor provides the ability to monitor in real time, and respond dynamically to attacks based on a flexible pre-defined risk-based strategy. This clouding and distortion of an attacker's observations, affects decisions and impedes actions, and thus can inhibit an adversary's capacity to adapt to this changing environment. AppSensor can be used to change aspects of the application to make it much more difficult for an attacker to be able to identify, target and successfully attack a system. For example, response actions might proxy the attacker to a honey pot, or alter or disable functionality. Some AppSensor implementations have chosen to select responses randomly to confuse attackers further.

> ***"In cyber operations, speed favors the side which has gained the initiative and successful maneuver allows an attacker or defender to get inside their adversaries' decision cycles and move more rapidly than they can react. Speed is a double edged sword in cyberspace. Actions happen at machine speeds, but reactions tend to happen at human speeds since reactions usually require some form of analysis and the involvement of a decision maker."***
>
> 4th International Conference on Cyber Conflict, 2012

Next Steps

Development
AppSensor is about implementing measures proactively to add instrumentation and controls directly into an application in advance so that events are centrally analyzed, using all the knowledge about the business logic and the roles & permissions of users, responding and adapting behavior in real time. It bridges development and operations. The fundamental requirements are the ability to perform four tasks:

- Detection of a selection of suspicious and malicious events
- Use of this knowledge centrally to identify attacks
- Selection of a predefined response
- Execution of the response.

A complete reference implementation exists which can be used free of charge as is, or as inspiration for an organisation-specific custom approach. Comprehensive guidance has been written on how to implement AppSensor-like systems (see the AppSensor microsite, AppSensor Introduction for Developers, and AppSensor Guide listed in Further Information). The planning stages are probably the most time-consuming aspect of implementing AppSensor.

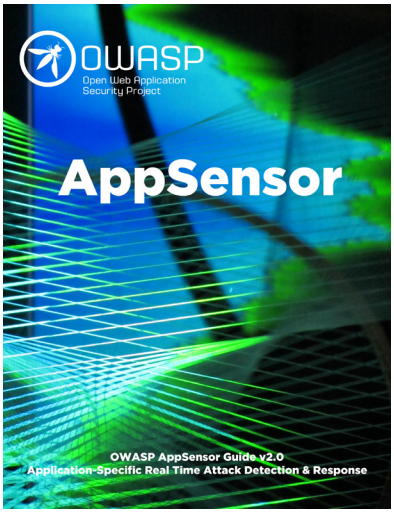
Acquisition
If software development is outsourced or offshored, the information in the AppSensor Guide can be used to specify appropriate AppSensor capabilities.

Vendor products and services
Network firewalls, application-aware firewalls, traffic/load balancers, anti DDoS systems, web gateways, network IDS/IPS, DLP, web application firewalls (WAFs) and other filters/guards are often cited as providing defense to applications, but they have no knowledge of custom application knowledge or insight into the context of user's actions. A growing number of vendors promoting products and services with application-specific AppSensor-like capabilities is anticipated.

> ***"The [AppSensor] approach is especially suited to software applications with high information assurance requirements such as in the defense, critical national infrastructure, and financial service sectors to protect against cyber espionage, fraud, business logic abuse, tampering, and theft"***
>
> CrossTalk, The Journal of Defense Software Engineering, Sep 2011

Additional AppSensor Resources

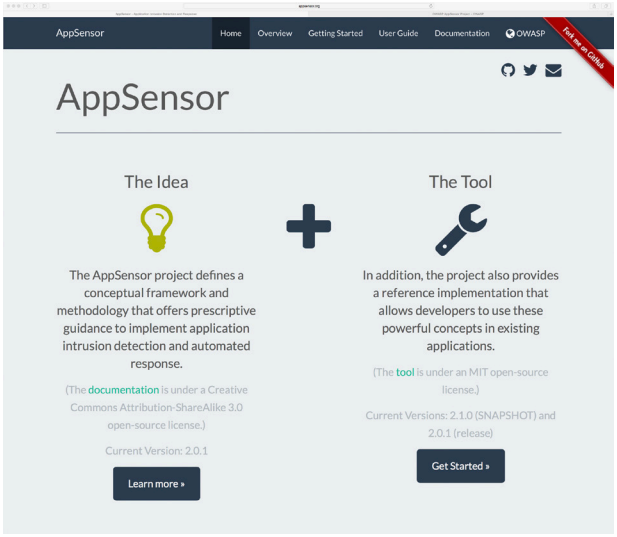
AppSensor Introduction for Developers
2015
PDF and AI, 2 pages, US-letter and A4



AppSensor Guide v2.0,
2014
DOC, PDF and hardcopy, 203 pages, quarto

The Journal of Defense Software Engineering
Vol. 24, No. 5, Sep/Oct 2011
PDF, 5 pages

OWASP AppSensor Project wiki site
2008-2015
https://www.owasp.org/index.php/OWASP_AppSensor_Project



AppSensor microsite,
2014-2015
http://www.appsensor.org

About OWASP

AppSensor is a flagship OWASP project.

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. You will find everything about OWASP on or linked from our wiki at https://www.owasp.org. OWASP does not endorse or recommend commercial products or services, allowing our community to remain vendor neutral with the collective wisdom of the best minds in software security worldwide. Other OWASP guidance Chief Information Security Officers may find of particular use are listed below.

Application Security Guide for CISOs
Guide that seeks to help CISOs manage application security programs according to CISO roles, responsibilities, perspectives and needs.
https://www.owasp.org/index.php/Application_Security_Guide_For_CISOs

CISO Survey and Report
Report on an annual survey allowing senior managers to compare their organizations with others on important application security issues.
https://www.owasp.org/index.php/OWASP_CISO_Survey

Open Software Assurance Maturity Model (SAMM)
Guide to building security into software development. SAMM enables organizations to self-assess their security assurance program and build roadmaps to improve.
http://www.opensamm.org

Application Security Verification Standard
Standard providing a basis for testing web application technical security controls as a metric, as guidance and during procurement.
https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

Secure Coding Practices - Quick Reference Guide
Application security requirements in the form of a compact checklist suitable for procurement and design processes.
https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide

OWASP AppSensor CISO Briefing
Detect and respond to attacks from within the application

AppSensor is a flagship OWASP project. The flagship designation is given to projects that have demonstrated strategic value to OWASP and application security as a whole.

The microsite and project URLs are:

http://www.appsensor.org
https://www.owasp.org/index.php/OWASP_AppSensor_Project

AppSensor CISO Briefing
Version 2.0 (30th March 2015)