imperva

CAPABILITY BRIEF

Protecting Against Software Supply Chain Attacks

Cyberattackers are infiltrating open source and embedded software libraries to get around layered security controls. As their use and automated patching grow more efficient, security teams lose all ability to differentiate between beneficial and unwarranted new application behavior. As the vast majority of security tools only block known, malicious behavior, emerging attacks can go undetected for months by using new tactics, malware, or drop servers. A new, proactive approach to blocking unexpected application behavior is necessary to protect your organization.

Be prepared for the next Sunburst - Legacy controls aren't enough

Attackers have targeted the software supply chain to evade the many controls that need to know specific vulnerabilities or signatures for malicious behavior:

- Application scanning tools, both SAST and DAST, are unlikely to identify compromised third party software embedded in your applications.
- Perimeter tools, such as next-gen firewalls, are easily deceived by seemingly innocuous traffic from applications until the signatures are published.
- Endpoint security is often blind to application attacks as they rarely need to touch user devices in the early stages.

Addressing software supply chain risks requires runtime analysis and protection that restricts applications to "expected" behavior. Only by blocking unexpected activity, do you ensure prevention of novel supply chain directed attack tactics, such as establishing C2 to a remote server or exfiltrating data from a compromised application's database.

The NIST organization recognized how many security controls fail to address this challenge and determined that only runtime protection prevents these stealthy attacks. For this reason, NIST SP 800-53 Revision 5, includes Runtime Application Self-Protection (RASP) as a recommended control [SI-7(17)] to respond to emerging threats from the software supply chain.

Emerging attacks can go undetected for months. A new, proactive approach to blocking unexpected application behavior is necessary to protect your organization.

Imperva RASP blocks supply chain attacks before they're known

Imperva RASP applies a positive security model to an application's internal behavior and only permit activity that should occur. It not only protects the application, but the entire stack; including third party libraries, open source dependencies, and the application runtime. By running inside the application, Imperva RASP disrupts an attacker's ability to run arbitrary code, establish outbound network connections, move laterally inside the network, and read sensitive files. It is this precise prevention approach that stops software supply chain attacks missed by traditional detection tools.

SSDLC
RASP is part of the app throughout SSDLC

Embed Security
RASP plugin attached from the start

Hardened APP
Applications are secure by default

Data Analytics
Local Outlier Factor for insights in SIEM/Analytics platform

Even once vulnerabilities related to backdoors are published, it is often infeasible to remediate on production servers until a scheduled maintenance window arrives. Imperva RASP shields the application from exploit to ensure the application runs safely until a patch is possible. This layered approach of preventing unexpected behavior and shielding known vulnerable systems is why RASP is recommended for organizations that need to easily deploy protection against supply chain attacks.

Easy to enable, easy to manage

Imperva RASP deploys in minutes, is completely air-gapped (no inbound/outbound network connectivity), and requires no signature updates. RASP is woven directly into the deployment process so applications are safely pushed to production without delay. By easily snapping into an application without requiring any code changes, Imperva RASP is a fast and easy way to mitigate risks in even the most complex software supply chains.

IMPERVA RUNTIME APPLICATION SELF PROTECTION (RASP)

Block unexpected application activity without hindering operations

Protect applications from zero-day attacks

No learning or signature updates required

Protects entire stack - including third-party and open source dependencies

Recommended in **latest NIST standard**

Learn more about Imperva Runtime Self Protection (RASP) at +1.866.926.4678 or online at imperva.com

Imperva protects the data of **over 6,200 customers from cyber attacks** through all stages of their digital transformation.