SYNOPSYS® (https://synopsys.com/) (www.synopsys.com/)

Software Integrity Application Build

Support (https://community.synopsys.com/) About Us (/company.html)

Platform (/software-integrity/polaris.html) Solutions Contact Sales (/software-integrity/contact-sales.html)

Tools & Services Customer Success

Partners (/software-integrity/partners.html) Resources

Blog (/blogs/software-security.html)

Security Risk Assessment

Threat modeling best practices (/software-integrity/resources/white-papers/threat-modeling-best-practices.html)

Table of Contents

Definition

A security risk assessment identifies, assesses, and implements key security controls in applications. It also focuses on preventing application security defects and vulnerabilities. Carrying out a risk assessment allows an organization to view the application portfolio holistically—from an attacker's perspective. It supports managers in making informed resource allocation, tooling, and security control implementation decisions. Thus, conducting an assessment is an integral part of an organization's risk management process.

How does a security risk assessment work?

Factors such as size, growth rate, resources, and asset portfolio affect the depth of risk assessment models. Organizations can carry out generalized assessments when experiencing budget or time constraints. However, generalized assessments don't necessarily provide the detailed mappings between assets, associated threats, identified risks, impact, and mitigating controls.

If generalized assessment results don't provide enough of a correlation between these areas, a more in-depth assessment is necessary.

The 4 steps of a successful security risk assessment model

1. **Identification**. Determine all critical assets of the technology infrastructure. Next, diagnose sensitive data that is created, stored, or transmitted by these assets. Create a risk profile for each.
2. **Assessment**. Administer an approach to assess the identified security risks for critical assets. After careful evaluation and assessment, determine how to effectively and efficiently allocate time and resources towards risk mitigation. The assessment approach or methodology must analyze the correlation between assets, threats, vulnerabilities, and mitigating controls.
3. **Mitigation**. Define a mitigation approach and enforce security controls for each risk.

4. **Prevention**. Implement tools and processes to minimize threats and vulnerabilities from occurring in your firm's resources.

What problems does a security risk assessment solve?

A comprehensive security assessment allows an organization to:

- Identify assets (e.g., network, servers, applications, data centers, tools, etc.) within the organization.
- Create risk profiles for each asset.
- Understand what data is stored, transmitted, and generated by these assets.
- Assess asset criticality regarding business operations. This includes the overall impact to revenue, reputation, and the likelihood of a firm's exploitation.
- Measure the risk ranking for assets and prioritize them for assessment.
- Apply mitigating controls for each asset based on assessment results.

It's important to understand that a security risk assessment isn't a one-time security project. Rather, it's a continuous activity that should be conducted at least once every other year. Continuous assessment provides an organization with a current and up-to-date snapshot of threats and risks to which it is exposed.

At Synopsys, we recommend annual assessments of critical assets with a higher impact and likelihood of risks. The assessment process creates and collects a variety of valuable information. A few examples include:

- Creating an application portfolio for all current applications, tools, and utilities.
- Documenting security requirements, policies, and procedures.
- Establishing a collection of system architectures, network diagrams, data stored or transmitted by systems, and interactions with external services or vendors.
- Developing an asset inventory of physical assets (e.g., hardware, network, and communication components and peripherals).
- Maintaining information on operating systems (e.g., PC and server operating systems).
    - Information about:
        - Data repositories (e.g., database management systems, files, etc.).
        - Current security controls (https://www.synopsys.com/software-integrity/software-

security-services/software-architecture-design/security-control-design-analysis.html) (e.g., authentication systems, access control systems, antivirus, spam controls, network monitoring, firewalls, intrusion detection, and prevention systems).
- Current baseline operations and security requirements pertaining to compliance of governing bodies.
- Assets, threats, and vulnerabilities (including their impacts and likelihood).
- Previous technical and procedural reviews of applications, policies, network systems, etc.
- Mapping of mitigating controls for each risk identified for an asset.

What industries require a security risk assessment for compliance?

Most organizations require some level of personally identifiable information (https://www.lifelock.com/learn-identity-theft-resources-what-is-personally-identifiable-information.html) (PII) or personal health information (PHI) for business operations. This information comes from partners, clients, and customers. Information such as social security number, tax identification number, date of birth, driver's license number, passport details, medical history, etc. are all considered confidential information.

As such, organizations creating, storing, or transmitting confidential data should undergo a risk assessment. Risk assessments are required by a number of laws, regulations, and standards. Some of the governing bodies that require security risk assessments include HIPAA (https://www.synopsys.com/glossary/what-is-hipaa.html), PCI-DSS (https://www.synopsys.com/glossary/what-is-pci-dss-compliance.html), the Massachusetts General Law Chapter 93H 201 CMR 17.00 regulation, the Sarbanes-Oxley Audit Standard 5, and the Federal Information Security Management Act (FISMA).

Organizations often question the need for compliance and adherence to these regulations. At Synopsys, we feel that an organization is required to undergo a security risk assessment to remain compliant with a unified set of security controls. Controls that are implemented and agreed upon by such governing bodies.

In fact, these controls are accepted and implemented across multiple industries. They provide a platform to weigh the overall security posture (https://www.synopsys.com/software-integrity/software-security-services/software-architecture-design/security-control-design-analysis.html) of an organization.

Governing entities also recommend performing an assessment for any asset containing confidential data. Assessments should take place bi-annually, annually, or at any major release or update.

Resources to manage your AppSec risk at enterprise scale

SYNOPSYS

2023 Software Vulnerability Snapshot

A Three-Year Analysis of the 10 Most Common Web and Software Application Vulnerabilities

CyRC

Synopsys Security Testing Services and Synopsys Cybersecurity Research Center

Software Vulnerability Snapshot

Learn about the 10 most common web and software app vulnerabilities

Download the report (/software-integrity/resources/analyst-reports/software-vulnerability-trends.html)

DARKReading

WHITE PAPER

Managing Risk at Scale: How to Gain Visibility, Quiet the Noise, and Secure Applications Across the Enterprise

Sponsored by

SYNOPSYS

Managing Risk at Scale

Learn how to gain visibility and secure your apps across the enterprise

Download the white paper (/software-integrity/resources/white-papers/scale-enterprise-application-security-program.html)

synopsys

Consolidation Is More Than Tools:
Three Steps to Improving AppSec Program
TCO and Risk Posture

More software, more tools, more risk

Organizations are seeing steep increases in the amount and speed of code being written, and as a result, they need solutions to address the subsequent increase in application security (AppSec) risk. When teams are working to innovate at the speed of business, they face challenges securing their applications without impeding that velocity.

To address this increased security risk, firms are adding multiple point tools throughout their software development life cycle (SDLC). However, increased tooling adds complexity to the SDLC, which slows down development teams and creates resource inefficiencies. And despite all these tools, businesses still struggle to gain actionable risk insight. Too many tests, too many tools, and too many findings get in the way of shipping software quickly. In a budget conscious economy, this is why you're hearing so much right now from business and software leaders about security tool consolidation.

Consolidation needs to be about more than just tools. By consolidating the effort required to implement and manage your AppSec program, and consolidating the insights gained across tools, organizations can address the growing complexity, diminished risk management, and resource inefficiencies that raise total cost of ownership (TCO). What organizations are looking for is a way to stop duplicating effort across teams that are using multiple, and often diverse, security tools. Consolidation can help you do that. Here are some ways to get started.

Consolidate effort

Most development teams have tools and processes they're accustomed to and want to keep using. On the micro level of a single team, this might make sense, but when you multiply teams by business units, and business units across an entire enterprise, you can wind up with hundreds of different tools enforcing inconsistent AppSec policies across your organization. This leaves your risk data scattered in a way that makes it nearly unusable.

That's why inserting a layer of abstraction between your development teams and your security tools is a good way to begin harnessing this proliferation. By inserting this layer, you can achieve three core goals for your AppSec program:

- Your development teams don't need to learn multiple UIs—they can continue working with the tools they already know.
- Your AppSec team can implement standard and consistent policies across the multitude of point tools being used across your organization.
- All your security tools are run through a single abstracted tool, providing a consolidated view into what was tested, what was found, what was fixed, and what your overall risk is at any point in time.

synopsys.com | 1

Improve your AppSec program TCO and risk posture

Three steps to consolidate your effort, insight, and tools

Download the guide (/software-integrity/resources/ebooks/improve-appsec-program-tco-risk-with-consolidation.html)

Questions about application security?

Contact us (/software-integrity/contact-sales.html)

(https://www.synopsys.com/)

Corporate

About Us (/company.html)

Careers (/careers.html)

ESG (/company/environment-social-governance.html)

Inclusion & Diversity (/careers/inclusion-diversity.html#present)

Investor Relations (https://investor.synopsys.com/overview/default.aspx)

View our Office Locations (/company/contact-synopsys/office-locations.html)

Contact Us (/company/contact-synopsys.html)

Learn

Blogs (/blogs.html)

Press Releases (https://news.synopsys.com/)

Newsroom (/newsroom.html)

What is EDA? (/glossary/what-is-electronic-design-automation.html)

What is Application Security? (/glossary/what-is-application-security.html)

Legal

Privacy (/company/legal/privacy-policy.html)

Trademarks & Brands (/company/legal/trademarks-brands.html)

Products

Application Security (/software-integrity.html)

Semiconductor IP (/designware-ip.html)

Verification (/verification.html)

Design (/implementation-and-signoff.html)

Silicon Engineering (/manufacturing.html)

Resources

Solutions (/solutions.html)

Services (/services.html)

Support (/support.html)

Community (/community.html)

Academic & Research Alliances (SARA) (/academic-research.html)

Manage Subscriptions (https://online.synopsys.com/contact-form-subscription-center.html)

Software Integrity Agreements (/company/legal/software-integrity.html)

Security (/company/legal/vulnerability-disclosure-policy.html)

Copyright (/company/legal/copyright.html)

Follow

𝕏 (https://twitter.com/synopsys) in (https://www.linkedin.com/company/synopsys) (https://www.facebook.com/Synopsys/) ▶ (https://www.youtube.com/user/synopsys) (https://www.instagram.com/synopsyslife/?hl=en)