SYNOPSYS®

WHITE PAPER

CISO's Guide to Sensitive Data Protection

An application security viewpoint

Table of contents

"Through 2022, privacy-driven spending on **compliance tooling** will increase to more than **$8 billion** worldwide."[1]

One of a CISO's primary responsibilities is to protect their company's important digital assets, which can include corporate intellectual property such as proprietary source code and other patented technology or confidential information. However, because of emerging privacy and regulatory laws and standards, CISOs and data protection officers now also need to protect user data—personally identifiable information (PII), personal health information (PHI), and payment card industry (PCI) data.

These new privacy laws are increasing the restrictions on the use, retention, and geographic residency of user data. This requires many organizations to protect this data and its use both internally as well as with third-party vendors that handle this data. CISOs need to work with their colleagues in data protection, privacy protection, IT infrastructure, compliance, and software development to ensure compliance with these data protection and privacy laws, standards, and guidelines. In addition, the emergence and adoption of hybrid clouds and multicloud services creates new challenges for data security. Other factors—the geographic origin of data, storage location, and user access location points—further complicate what services providers and major cloud infrastructure providers need to do to secure their data.

Consumers are becoming more wary about their personal information and how it is used. The National Conference of State Legislators, citing a report by the Pew Research Center, writes, "More than 80% of Americans say they go online on a daily basis." It adds, " Of those, 28% go online almost constantly and 45% go online several times a day. Consumers are now more aware that businesses, social media sites, and other websites may collect and share their personal information with third parties. They also hear more about security breaches, cyber attacks, and unauthorized sharing of personal information."

Similarly, a survey of 1,000 consumers from the U.S. and the U.K. conducted by Entrust on data privacy showed that "79% of consumers said they're concerned about data privacy, and 64% said that concern has increased in the past 12 months. The top reasons for consumers' heightened concerns were news stories about data breaches and seeing an increase in targeted ads on social media."[2]

"By 2023, companies that earn and maintain digital trust with customers will see **30% more digital commerce profits** than their competitors."[3]

The recent surge in remote work has also resulted in increased worker data privacy concerns. "What we found was that roughly two years ago most companies barely had a privacy team; it was tucked away in a legal office," says Robert Waitman, director of data privacy at Cisco. "But with the shift to remote work because of the pandemic, privacy has become more important, mainly because employees were uncomfortable with the privacy of the tools available and the need for companies to provide a safe workplace."

Digital transformation and the need for application security

Understanding how application security ties into data and privacy protection is essential. With the digital transformation happening in many industries, organizations are compelled to digitize their business web presence to more quickly gain and retain new customers versus their competitors. This is especially true in the financial services industry, healthcare, and e-commerce / retail market segments, where usage of mobile and web applications and websites has increased significantly. However, these websites and applications can also serve as attack vectors for hackers who leverage them as entryways into organizations' databases, which contain sensitive user data that can be monetized on the dark web.

This white paper provides a summary of recent privacy laws and describes how different frameworks and security tools—including application security tools—can help ensure data protection and privacy. Software security services, architecture

analysis, and threat modeling of new systems from both a security and systems engineering perspective are equally important. CISOs should work collaboratively with their heads of software application development, third-party application procurement, and systems engineering to better protect sensitive data against potential cyber security attacks that can lead to costly data breaches. The recent SolarWinds software supply chain breach points to the urgent need for improved DevSecOps processes, secrets management, and sensitive data detection throughout the stages of the software development life cycle (SDLC).

Significant data privacy laws, frameworks, and security standards

Cyber security and privacy frameworks are both integral. Cyber security and privacy frameworks provide methods, processes, and best practices that can help companies better achieve compliance with security standards and data privacy laws. Cyber security frameworks help reduce the risks associated with loss of confidentiality, integrity, or availability; privacy frameworks help reduce risks associated with unintended consequences of data processing. Both are needed in order to reduce the risk of privacy breaches. U.S. cyber security frameworks include the Cybersecurity Framework and Privacy Framework, which provide voluntary guidelines based on existing standards, guidelines, and practices to help organizations better manage and reduce their cyber security risk and individuals' privacy risk. The National Institute of Standards and Technology (NIST) encourages organizations in various market sectors to adhere to these frameworks according to their unique risks, situations, and needs, as they are meant to serve as guidelines.

More specifically, FISMA update NIST 800-37 recommends the use of "automated security tools to continuously diagnose and improve security," with one of the goals being to ensure that security controls are integrated into an organization's enterprise architecture and system development life cycle. In addition, NIST 800-53 includes new security and privacy controls, as well as guidelines to cover areas like mobile and cloud computing, insider threats, application security, and supply chain security for U.S. federal information systems.

Commercial data security standard

PCI Data Security Standard (PCI DSS) is a data security standard that applies to all entities that store, process, or transmit cardholder data. There are specific requirements for software developers and manufacturers of applications and devices used in those transactions. These security controls and processes are essential for protecting all payment card account data, including the primary account number printed on the front of a payment card.

Consumer privacy laws worldwide

The European Union (EU) Data Protection Directive (DPD) regulates the processing and free movement of personal data within the EU. Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) regulates the consent and use of personal data. These were among the first privacy laws to be enacted. But the General Data Privacy Regulation (GDPR) from the EU, which protects consumer data of EU residents, is the law that attracted the most international attention.

Since these laws were enacted, many other countries are putting in place their own additional privacy laws. Here are just a few examples:

- Canada: Personal Health Information Protection Act (PHIPA)
- Australia: Consumer Data Rights (CDR)
- China: Right of Privacy and Personal Information Protection as part of the Cyber Security Law
- India: Personal Data Protection Bill (PDPB)
- Brazil: Lei Geral de Proteção de Dados / General Personal Data Protection Law (LGPD)
- United States: California Consumer Privacy Act (CCPA)

The GDPR covers data protection and privacy in the European Union and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA. It provides guidelines for data transparency, purpose limitation, data minimization, accuracy, storage time limitations, integrity and confidentiality, and accountability by a data controller or data protection officer. The GDPR essentially creates a privacy framework. For example, to comply with Article 25 of GDPR, companies must implement "privacy by design" principles, which state privacy should be considered at every point in the process. The GDPR imposes fines on organizations that don't adhere to its data protection and privacy laws.

"By 2024, more than **80% of organizations worldwide** will face modern **privacy and data protection requirements."**[4]

The CCPA received a lot of attention because it's the first strong privacy regulation in the U.S. It ensures several privacy rights to consumers who live in California, and it affects organizations worldwide that serve California residents. Its main goal is to give California residents control of their personal information and how it is used. To achieve this, it introduces five fundamental rights: The right to disclosure, to deletion, to access, to opt-out, and to nondiscrimination. In addition, CCPA introduces significant fines and sanctions for noncompliance, and is applicable to businesses based in California, and potentially any business offering services to California residents.

Data security strategies and frameworks

Organizations must start by creating a data strategy and framework that meets their business needs. This is especially true for companies that leverage user data as part of their business strategy. This requires coordinating and establishing key corporate metrics and goals for regulatory compliance, data security governance, supporting IT strategy, and tolerance for risk.

Organizations must then do data discovery and data classification, determine access policy, and manage datasets over their entire life cycle within their organization. Data classification requires noting the sensitivity level of files, databases, and emails, and access policy involves indicating which groups or individuals are granted access. Similarly, applications should be classified according to the criticality of the data that resides within them, and whether they are external-facing, internal, or cloud-hosted.

"In 2020, research data from Imperva warned that **'unauthorized transmission of data from organizations'** networks to external destinations soared **93% in 2020**… to 1.7 million incidents by the end of December. It is naïve to think that it is only human access to data that leads to compromise. Over 50% of access requests to databases are coming not from users, but application to application.'"[5]

Defining comprehensive data security policies and adequate implementation resources should be done by a variety of teams within an organization and approved by executive management. After defining the strategy, an organization should select and implement security tools, products, and services that help ensure data and application security.

The end of the traditional perimeter

The traditional data center has gone through many fundamental changes over the years. There once was the concept of a self-contained data center and internal network that was protected at the external-facing boundaries by network and web application firewalls. In this scenario, within the physical building, corporate-owned endpoints were trusted so they could easily access data via the internal network.

With corporate data and applications moving to the cloud, the bring-your-own-devices (BYOD) paradigm, and growing adoption of remote work, the traditional security perimeter has disappeared. Organizations must now face the challenge of defining new security policies to mitigate the risks associated with a perimeter-less network: sensitive data leakage, and data privacy and regulatory compliance breaches.

Identity and context as the new perimeter

With the increasing use of BYOD smartphones and tablets/laptops, and the rapidly growing number of employees working from home, all devices and users must be authenticated and validated before they can access corporate SaaS apps and internal data. There are many security tools that can perform multifactor authentication (including biometrics) or correlate multiple devices with the specific identity of a single user to ensure authorized access and keep out cyber attackers. Other security tools (e.g., SIEMs/UEBAs and CASBs for cloud apps) can use factors such as device location (or IP address), time of day, and volume and types of file downloads to flag anomalous behavior that could lead to data leakage. Critical applications can also be isolated or shielded from unauthorized access.

Compliance with security standards

OWASP Top 10 and OWASP Mobile Top 10

Web applications can serve as a conduit for hackers to gain access to sensitive data. The OWASP Top 10 outlines the 10 most-critical security risk categories for web applications. For example, in a SQL injection attack, hackers try to get access to sensitive data in a database without proper authorization by executing unintended commands through a web input form. Another danger to web applications is sensitive-data exposure. According to Open Web Application Security Project (OWASP), "Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser." Similarly, the OWASP Mobile Top 10 outlines the top risk categories for mobile applications.

Common Weakness Enumeration (CWE) Top 25

The CWE Top 25 is a community-developed list spearheaded by MITRE. This list catalogs the most dangerous software and hardware weaknesses that are often easy to find and exploit, and that can allow cyber attackers to completely take over a system, steal data, or prevent an application from working. The CWE team created the 2020 list by leveraging the common vulnerabilities and exposures (CVE) data in the National Vulnerability Database (NVD), as well as the common vulnerability scoring system (CVSS) scores associated with each CVE. Some of the top 10 weaknesses include both quality issues (e.g., out-of-bounds memory buffer, use after free, out-of-bounds read or write) and security issues (e.g., cross-site scripting, improper input validation, SQLI, cross-site request forgery, and exposure of sensitive information to an unauthorized actor).

CISQ Automated Source Code Data Protection Measure

The Consortium for Information & Software Quality (CISQ) has coordinated a new OMB standard, the Automated Source Code Data Protection Measure. According to CISQ, the measure is "based on a collection of relevant CWEs that can be used to support enterprise and supply chain needs in protecting data, confidential information, intellectual property, and privacy. These CWEs are currently available for use. This new standard is highly relevant to GDPR, CCPA, and Cybersecurity Maturity Model Certification (CMMC) for controlled unclassified information protection."

The standard seeks to spotlight CWEs that can enable data leakage—those that have CWSS technical impacts that allow unauthorized access to read/modify data. CISQ notes that "Scanning code that will run or is running in enterprises (on systems and devices that process or transmit data) would determine if the systems or devices enable data leakage. If so, then such a scan would reveal if the data protection/privacy controls associated with the process assessment were inadequately implemented."

Static application security testing (SAST) tools along with other AppSec tools (e.g., interactive application security testing [IAST], software composition analysis [SCA], and dynamic application security testing [DAST]) can help development teams automate the identification and remediation of security vulnerabilities and weaknesses in the top categories listed by standards, such as the OWASP Top 10 and CWE Top 25.

Thinking like an attacker

Business logic, or application logic, refers to the set of rules that define how an application operates and functions according to a specification. SAST tools can find issues by examining static code, but they often can't easily identify business logic weaknesses—flaws in the design or implementation of an application that allow an attacker to elicit unintended behavior by interacting with the applications in ways that developers never intended.

Flaws in application logic can allow attackers to circumvent these rules. An attacker passing unexpected values into server-side logic could potentially cause, for example, a transaction to complete outside of a normal purchase workflow. A deep understanding of an application's business logic and how attackers can interact with it helps testers model potential attack vectors and perform a more-focused code review.

As stated by OWASP on its wiki, "testing of business logic flaws is similar to the test types used by functional testers that focus on logical or finite state testing. These types of tests require that security professionals think a bit differently, develop abuse and misuse cases, and use many of the testing techniques embraced by functional testers. Automation of business logic abuse cases is not possible and remains a manual art relying on the skills of the tester and their knowledge of the complete business process and its rules."

Threat modeling in the design phase

Creating a threat model helps ensure that business requirements are protected against malicious actors, accidents, or other causes. Performing threat modeling to identify and prioritize potential threats and security mitigations early in the design phase helps prevent security vulnerabilities and weaknesses from being introduced, even before any coding happens.

A threat model usually includes a description, design, or model of the primary concerns; a list of assumptions that can be checked against; potential system threats and actions to be taken for each threat; and a way of validating the model and threats and verifying the success of actions taken. The scope of the threat model needs to be defined, and the model must be based on a deep understanding of what the application does. Architecture diagrams, dataflow transitions, and data classifications are also very useful in the process.

Threat modeling requires close collaboration between people who perform different roles (e.g., security architects, DevOps, and development leads) and who have sufficient technical and risk awareness to agree on the framework to be used during the threat modeling exercise. The variety of perspectives and expertise helps bring awareness of current threats to development teams that may not necessarily have deep security knowledge.

Secrets management is crucial for data security

"By 2021, more than half of organizations using DevOps will be using [**privileged access management**]–based secrets management services and solutions."[6]

In the context of cyber security and IT, secrets are private data or credentials that must be stored securely with tight access control. Typically secrets consist of digital credentials, such as application keys and APIs, encryption keys, PEM files, Oauth tokens, private certificates (SSL, TLS), and passwords (user, system-to-system, and database) that unlock protected resources in tools, applications, containers, and DevOps and cloud-native environments. Secrets provide users and applications with access to resources (e.g., sensitive data, systems, and services) and enable authorized developers to make changes to source code in application development.

There are tools and services (e.g., Hashicorp Vault and AWS Secrets Manager) that enable central management of secrets, manage access control lists of people and machines and what they can access, handle dynamic rotation of credentials, encrypt data at rest and in transit, and generate audit logs. Secrets management is crucial for organizations, regardless of their usage of DevOps, because almost all organizations use digital secrets to some extent.

Secrets such as private keys should not be stored in public repositories of code, although they often are. A recent study from researchers at North Carolina State University found that over 100,000 public GitHub repositories were leaking secret keys, and "thousands of new, unique secrets are leaked every day." There are horror stories about a developer who accidentally checks his AWS S3 key in to GitHub, and although he pulls it within 5 minutes, he still racks up a large bill from bots that crawl open source sites looking for secrets.

Sensitive-data detection: AppSec tools versus secrets management tools

Secrets often consist of sensitive information that a continuous integration (CI) build server (or job) needs in order to complete work. What secrets management tools don't do is scan code to identify secrets or back doors that have been

accidentally left in source code. If discovered by hackers, those secrets and back doors could lead to data breaches. Some companies, such as GitHub, will scan public and private repositories for secrets (e.g., access tokens, API keys, private keys, etc.) and will notify the service providers of credentials that have been committed accidentally, to prevent fraudulent use.

Organizations can also use AppSec tools (e.g., SAST, SCA, IAST, and DAST) that use dedicated security checkers or rulesets to scan their own private code repositories and web apps for secrets and other forms of sensitive data. Application security tools can identify CI workflow-centric secrets that have been accidentally left in code, and they can also automate the detection of other types of sensitive data, such as credit card numbers and user credentials, and whether these types of sensitive data have not been encrypted or inadequately encrypted. These security weaknesses can then be fixed before an application is released to production.

System back doors that allow access to data and processes at the system level include malware, such as remote access trojans. Application back doors are versions of legitimate software that can compromise data, transactions, and whole systems.

Static analysis tools examine applications in a similar way to how attackers look at them. They create a detailed model of the application's data and control flows. Although application back doors are often obfuscated and difficult to detect, static analysis of source code or binaries can identify them as part of a malicious code detection review process. For compiled software or a subverted development tool chain, back door detection may require static binary analysis since the back door only exists after compilation or linking. Frameworks and libraries that are available as binaries also need to be scanned for security vulnerabilities and weaknesses.

A holistic systems security engineering approach

According to Ron Ross, a NIST fellow, adversaries are becoming more sophisticated. After breaching an initial perimeter, they will try to establish a presence in a system, steal credentials, escalate privileges, move laterally across the system, and then attack other systems. An example of this is the recent SolarWinds software supply chain attack, where it is believed that attackers lurked in the company's Office 365 email system for months before compromising their broader Office 365 environment, and later other systems.

In a video interview, Ross said, "The adversary has the advantage; they live in the cracks. We have an Achilles heel that we're building into these new technologies. And this is why I think working in a DevSecOps approach [is useful]. You're looking at agile and DevOps-type processes, you're looking at security across the entire life cycle. And you're working with software engineers, so they can work out some of those bugs and weaknesses and deficiencies early in the process, so they don't become vulnerabilities when they get delivered to you. How can we apply those fundamental security design concepts and principles from NIST 800-160 to the DevSecOps process or agile development … to create lean system security engineering?"[7]

These adversaries look at systems differently than organizations that have a single-dimensional strategy of protecting systems (e.g., implement necessary security controls and frameworks, then wait and do scanning, monitoring, and detection—defend at the perimeter). Adversaries look at it as a system of systems ecosystem—interconnected systems that interact with each other within an organization, and that connects with external systems as well. Ross points out that our definition of a system is broadening to include the supply chain. He advocates for our strategy and tactics to become multidimensional and include systems architecture, systems engineering, and security engineering teams working together from the beginning to define and build more secure systems. These teams need to understand the systems components, how they are put together, how much protection each component has, the information flow between components, how the components interact, where the single points of failure are, the interactions with the supply chain, the automatic updates or patches, and what would happen if there was malicious code in those updates.

In the SolarWinds software supply chain attack, attackers were able to replace source code files in the build process, before compilation, subvert SolarWinds' software development process, and insert a malicious back door into the Orion network monitoring software. After attackers inserted their malware into SolarWinds' software, it was digitally signed by the company and propagated to 18,000 customers via SolarWinds' software update process. The Wall Street Journal reported that the attack gave the hackers potential access to sensitive corporate and personal data. And The Verge reported that "9 federal agencies and about 100 private sector companies were compromised."

Synopsys can help organizations better protect their sensitive data

Synopsys Software Integrity Group offers a broad portfolio of software security services and application security tools that help development teams identify and remediate security weaknesses and vulnerabilities. Organizations can use Synopsys' industry-leading application security tools themselves or supplement their security and development resources with Synopsys' managed services or security program consulting.

Software security services and programs

The Synopsys Architecture and Design practice helps organizations identify missing or weak security controls, understand secure design best practices, and mitigate security flaws that increase the risk of a breach. Security services include security control design analysis, threat modeling, and architecture risk analysis. In addition, Synopsys also offers a Malicious Code Detection (MCD) service as well as security programs (e.g., Building Security In Maturity Model [BSIMM] and maturity action plan [MAP]) that enable organizations to define, build, and manage their own software security initiatives (SSIs).

Synopsys provides continuous access to security testing experts with the skills, tools, and discipline needed to cost-effectively analyze any application, at any depth, at any time. Managed security testing services consist of penetration testing, dynamic application security testing, static application security testing, mobile application security testing, network penetration testing, red teaming, IoT and embedded software testing, and thick client testing.

Intelligent Orchestration for development at the speed of DevOps

Synopsys' Intelligent Orchestration solution enables teams to integrate application security analysis into their DevOps pipelines while maintaining development velocity. Intelligent Orchestration supports Synopsys AppSec tools (e.g., Coverity® SAST, Black Duck® SCA, Tinfoil™ DAST, and Seeker® IAST) as well as managed services (e.g., threat modeling, penetration testing) and third-party tools (e.g., AppSec, GRC, and dashboarding systems). It automatically performs the right security tests at the right time based on user-defined policies, risk profiles, and severity/context-specific code changes that are user-defined in advance. Risk-based vulnerability and weakness reporting ensures that developers need only remediate the most important issues they are assigned to address, all within the issue trackers, development tools, and notification channels that they normally use. Reminders to do manual testing such as threat modeling, manual code reviews, or penetration testing can also be automated based on policies. Developers can integrate security analysis and results seamlessly into their existing development tools and platforms. Application security testing (AST) analytics metrics help identify gaps so that heads of development can understand the effectiveness of their AST and DevSecOps implementation.

A complete suite of application security test tools across the SDLC

Synopsys application security tools have been recognized as leaders in industry analyst reports, such as the Gartner Magic Quadrant for Application Security Testing, The Forrester Wave™: Static Application Security Testing (Q1 2021), and The Forrester Wave™: Software Composition Analysis (Q2 2019). Synopsys products and services help development and security teams build secure, high-quality software faster.

- Coverity SAST. Coverity helps developers find and fix security defects early in the SDLC, with support for 21 languages and over 70 frameworks and template engines. Coverity has security checkers that identify hardcoded credentials, sensitive-data leaks, and unencrypted and inadequate encryption to help ensure compliance with OWASP Top 10 (web and mobile), CWE Top 25, PCI DSS, and other standards, as well as checkers for all the newest data protection measures.
- Black Duck SCA. Black Duck helps teams manage the security, quality, and license compliance risks that come from the use of open source and third-party code in applications and containers across their software supply chain. Black Duck Binary Analysis scans binaries and all associated files (e.g., HTML files, readme files), firmware and containers, and surfaces information leakage data such as forgotten developer credentials, AWS keys, IP addresses, and clear-text passwords.
- Seeker IAST. Seeker helps development, QA, and security teams automate application security testing and identifies vulnerability and weakness trends against compliance standards (e.g., OWASP Top 10, PCI DSS, CAPEC, and CWE/SANS Top 25). Seeker actively verifies that identified weaknesses and vulnerabilities are exploitable. It uses patented technology that can reduce false positives to near zero. And its unique sensitive-data tracking feature automatically detects when user-designated sensitive data is exposed in logs, databases, or files.

- Tinfoil Web Scanner. Tinfoil Web Scanner dynamically checks for over 70 classifications of weaknesses and vulnerabilities, including the OWASP Top 10. It analyzes all facets of your site, logging into any website, including SAML/SSO-authenticated sites. Its sensitive-data content checkers scan for credit card number disclosure, source code repository disclosure, private IP address disclosure, email address disclosure (if an email address is harvestable by bots), and Social Security number disclosure.
- Tinfoil API Scanner. Tinfoil API Scanner detects weaknesses and vulnerabilities in any RESTful API, commonly used in modern web-based applications and sites, including mobile and IoT-connected apps. Tinfoil API Scanner also supports GraphQL APIs, scanning for GraphQL-specific vulnerabilities. It provides specific focus on the context of API authentication and more. Unlike other tools that serve more as a defensive protection mechanism, Tinfoil API Scanner allows you to perform proactive and intelligent fuzzing of your APIs.

Summary

One of a CISO's primary responsibilities is protecting their company's digital assets, and adhering to current and emerging data privacy laws is crucial. Organizations must ensure that their corporate intellectual property and user data (e.g., customer, employee, contractor and/or prospect data) is safe from cyber attacks and data breaches.

CISOs must work with their colleagues in data protection, privacy protection, IT infrastructure, compliance, and software and system development to ensure compliance with data privacy laws.

Because cyber attackers are becoming increasingly sophisticated in their attacks, organizations must secure entire systems of systems, the software supply chain, and software development workflows. Defining and building the design, workflows, and processes that ensure software and system security is essential. Key stakeholders in system architecture, security, software development, and IT infrastructure need to work closely together to perform comprehensive architecture analysis, threat modeling, and holistic system evaluation.

Best practices for securing software development and DevSecOps workflows include secrets management, automated AppSec tools for compliance with industry security standards and sensitive data detection, threat modeling, manual penetration testing of business logic, and customized intelligent orchestration of AppSec tools and services.

As data privacy laws and requirements change over time, the information that's considered sensitive can change as well. Organizations must perform comprehensive data discovery and classification, and know where the data resides, so they can easily find the data when laws change. Organizations should also use AppSec tools that are flexible and can identify multiple types of sensitive data in source code, binaries, and all associated files such as HTML files, readme files, and firmware and containers. In addition, security and DevOps leads should use dynamic IAST tools that enable users to mark user-defined sensitive data types and automatically detect and track whenever this data exposed is exposed in a log, database, or file.

Learn more about Synopsys' Software Integrity Group solutions or request a demo.

About the author

Anna Chiang, CISSP, is a senior manager of product marketing in the Software Integrity Group at Synopsys.

References

1. Gartner, "The State of Privacy and Personal Data Protection, 2020-2022," Aug. 26, 2020.
2. Security Boulevard, "Data Privacy Day: How much do consumers really know about data privacy?", Jan. 28, 2021.
3. Gartner, "The State of Privacy and Personal Data Protection, 2020-2022," Aug. 26, 2020.
4. Ibid.
5. Infosecurity Magazine, "#Data Privacy Day: Leaks and Breaches Soared 93% in 2020," Jan. 28, 2021.
6. Gartner, Gartner Magic Quadrant for Privileged Access Management, Dec. 3, 2018.
7. Tom Field interview with NIST's Ron Ross: "The Adversary Lives in the Cracks," Dec. 23, 2020.

SYNOPSYS®

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

Contact us:
U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com