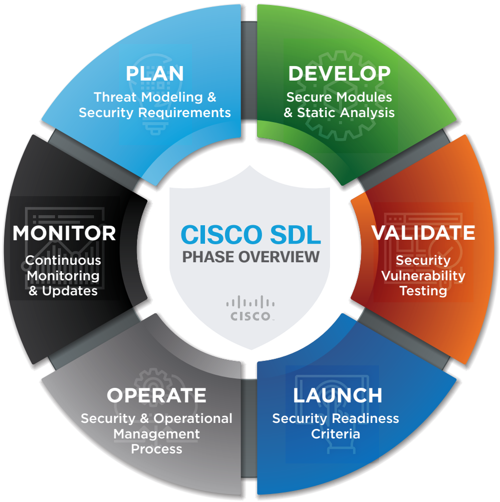
Cisco Secure Development Lifecycle

Securing Cisco Technology

Organizations need the comfort of knowing the technology they depend on is secure. To help instill this confidence, Cisco infuses security and privacy awareness into the entire development process. We call this the Cisco Secure Development Lifecycle (Cisco SDL).

Cisco SDL follows a secure-by-design philosophy from product creation through end-of-life. Because the security landscape always evolves, so does Cisco SDL. We constantly review the latest known security and privacy attacks and make sure that our technology can defend against them.


PLAN
Threat Modeling & Security Requirements
DEVELOP
Secure Modules & Static Analysis
MONITOR
Continuous Monitoring & Updates
CISCO SDL
PHASE OVERVIEW
VALIDATE
Security Vulnerability Testing
OPERATE
Security & Operational Management Process
LAUNCH
Security Readiness Criteria

Let’s explore the Cisco SDL core processes:

- **Plan** – security and privacy controls and risk assessment
- **Develop** – secure modules and static analysis
- **Validate** – security vulnerability testing
- **Launch** – security and privacy readiness
- **Operate** – security and operational management
- **Monitor** – continuous monitoring and updating

Plan

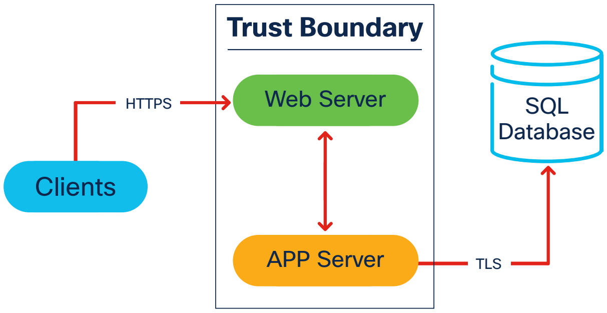
Cisco strives to build security and privacy into our technology at the start rather than bolt it on afterward. Creating secure technology begins by incorporating fundamental security and privacy concepts in the planning phase. Basic security concepts such as reducing the attack surface, controlling risk, and applying defense-in-depth techniques are crucial and should be well thought-out before any code is written. Basic privacy concepts such as processing personal data under legal stipulations and managing data subject rights must also be adhered to.

We conduct a gap analysis and risk assessment to establish the product’s security and privacy posture compared with Cisco and industry standard baseline requirements. This analysis serves as our security reference throughout the development process.

Threat Modeling

Threat modeling helps us better understand and prioritize security risks and expose potential design vulnerabilities. The model identifies trust boundaries, relationships, and inflection points where the data or system might be compromised. After potential vulnerabilities and threats are identified, we develop strategies to minimize the risk.

Cisco invests heavily in threat modeling tools, enabling our developers to apply the latest threat models throughout the development lifecycle. For example, we can address new points of entry, adjustments in trust boundaries, and other changes that might introduce vulnerabilities or threats. These actions result in a more accurate view of the security posture.



Cloud Security

Cloud-based technology presents a dynamic set of challenges that need to be addressed upfront. Following Cisco's cloud security strategy, we develop cloud-based technology in accordance with industry certifications such as SOC 2 Type II, ISO 27001, or FedRAMP. This strategy, devised in cooperation with a leading auditing firm, helps us comply with certification audits and address related security and privacy measures in a single development workflow.

Privacy Assessment

Cisco believes privacy is a fundamental human right and takes rigorous steps to handle data properly. Our engineering teams conduct a privacy impact assessment, which results in a privacy data sheet for each product. The privacy data sheet is a living document that specifies information such as the minimum data that should be collected and how long data should be retained. It also defines which controls are necessary to meet Cisco's privacy policies and to process data globally.

We continually re-evaluate privacy controls against a variety of governmental laws and regulations to make sure Cisco products comply with local requirements in the markets for which they are developed.

Develop

Cisco developers are directed to use secure coding standards, build threat-resistant code, and follow other standard security best practices. Our engineering teams use state-of-the art tools, libraries, and mature frameworks throughout the development process. We use hardening technologies such as Address Space Layout Randomization (ASLR), Object Size Checking (OSC), and XSPACE where appropriate. We also integrate image signing and trust anchor modules.

Secure Code Repositories

Our code resides in secure and restricted source control repositories. Cisco engineers can peer review each other's code, which helps prevent defects, minimize security weaknesses, and promote team collaboration and knowledge-sharing.

Common Security Modules

We use a series of Cisco-vetted, common security modules to help assure our technology is threat resistant. These centrally maintained modules focus on deterring the many ways attacks can penetrate your infrastructure, from controlling buffer overruns to protecting encrypted data.

Using common security modules, we can manage and complete upgrades quickly and efficiently. If a vulnerability is discovered in OpenSSL, for example, we can expediently update the CiscoSSL module instead of relying on hundreds of teams having to patch OpenSSL independently. In this instance, our product teams build against the vetted CiscoSSL module.

Code Analysis

During development, each Cisco product and solution undergoes frequent checks for vulnerabilities. We use several sophisticated static code analysis tools, such as Coverity and SonarQube, to analyze source code for buffer overflows, dangerous input, out-of-range numbers, and other security issues.

Product teams run updated scans of new software releases to review discoveries and address high-priority security issues before delivering the release. This approach is especially important in an ever-changing and sophisticated threat landscape and in a continuous integration / continuous delivery (CI/CD) development environment.

Security Training

Secure product design and development require an ongoing commitment to personal and professional improvement. All Cisco employees receive internal security training. Development and test teams undergo multilevel security education. The Cisco Security Space Center is an education program for our engineers, imparting fundamental security-oriented training and a multistep curriculum that raises an engineer’s security and privacy knowledge.

Validate

In the validation process, we test Cisco products to help identify and mitigate common security defects. The Cisco SDL security testing regimen incorporates industry-leading protocol tests, commonly used open-source tools, and sophisticated application test methods.

Vulnerability and Penetration Testing

Cisco SDL vulnerability testing improves the resiliency of our products against probes and attacks. Our development teams combine protocol robustness testing applications, commercial tools for common attacks and scans, and web application scanning tools to detect security defects in a consistent and repeatable manner.

Dedicated penetration testing and security risk assessment engineers are also available to help identify and resolve potential security weaknesses. Cisco performs In-depth security architecture evaluations and forensics as well as Red Team attack simulations where appropriate and employs third-party penetration testing when needed.

Third-Party Software Compliance

Cisco software images are digitally scanned for third-party commercial or open-source components. These components are inventoried to form a centrally registered software bill of materials (BOM) that we check for license and versioning. We also review the software BOM for known vulnerabilities, and a centralized team sets up alerts when component anomalies are detected. These alerts enable engineering teams to quickly patch the affected code.

Privacy Control Validation

Privacy and data protection controls are validated as required per policy. Controls such as assessing changes in data and its classification and processing, assuring data is properly encrypted and backed up where applicable, and making sure deletion mechanisms are in place are verified by the development teams before release.

Privacy data sheets and data maps enable our customers to understand what data is processed in our offering as well as the processing environment when Cisco is the processor. This data is made available to customers via the Cisco Trust Portal.

Launch

Security and Privacy Readiness

Our pre-launch criteria help us manage security risk and prepare products for customer use. The criteria detail critical security and privacy controls and track a product's status throughout the development process.

The Cisco Product Security Incident Response Team (PSIRT) is the official communications channel between Cisco and our customers. If a high-priority or critical security defect exists in an on-premises or cloud product, the PSIRT takes appropriate action to control the risk, including preventing release.

Operate

After a product has been thoroughly validated and passes Cisco's readiness criteria, we officially launch it. But security does not stop there. For on-premises products, security is continuously updated through maintenance releases that undergo all or a portion of the Cisco SDL, depending on the release type.

After a product launches, the Cisco PSIRT works with cloud and on-premises product teams to address critical security events.

Cisco cloud products maintain strict operational governance, employing mechanisms such as continual hardening, security control updates, and built-in security guardrails like identity and account management. Automated vulnerability testing, scheduled security reviews and assessments, periodic penetration testing, and disaster recovery planning are all part of a cloud product's operational governance.

After a cloud product is released, we maintain privacy controls. Controls for managing data retention periods, performing cross-border transfers, and sharing data between functional groups and third parties are designed in by default. These controls align with legal stipulations and the purpose for which the data was collected or created.

Monitor

Today's dynamic threat landscape requires not only multiple layers of defense, but also continuous security monitoring. The Cisco Computer Security Incident Response Team (CSIRT) monitors all Cisco-maintained data centers and hosted services, constantly evaluating logs from across our infrastructure. The team employs multiple monitoring tools and techniques such as Cisco Secure Malware Analytics (Threat Grid) and Cisco Secure Network Analytics (Stealthwatch) to detect and respond to threats quickly.

Cisco is active in threat intelligence organizations, with groups like Cisco Talos Intelligence often leading the way. Through Cisco Talos, we share actionable information about the latest threats and vulnerabilities with the broader security and Internet community. Our active participation helps us track security defects found both internally and in the field, and helps ensure those defects are promptly addressed and fixed.

We also continually assess, monitor, and improve the security of our value chain throughout the lifecycle of our products and solutions. See Value Chain Security for details on how Cisco protects against tainted and counterfeit solutions, the misuse of intellectual property, and more.

Developing Trustworthy Technologies

Building trustworthy products and solutions requires baking security into the design and development process. We implement security holistically across the entire product lifecycle. At Cisco, security and trustworthiness are not afterthoughts. They are vital elements designed, built, and delivered from the ground up. Visit The Trust Center for further details.