Scrut Automation

SaaS Platform Security
Done Right

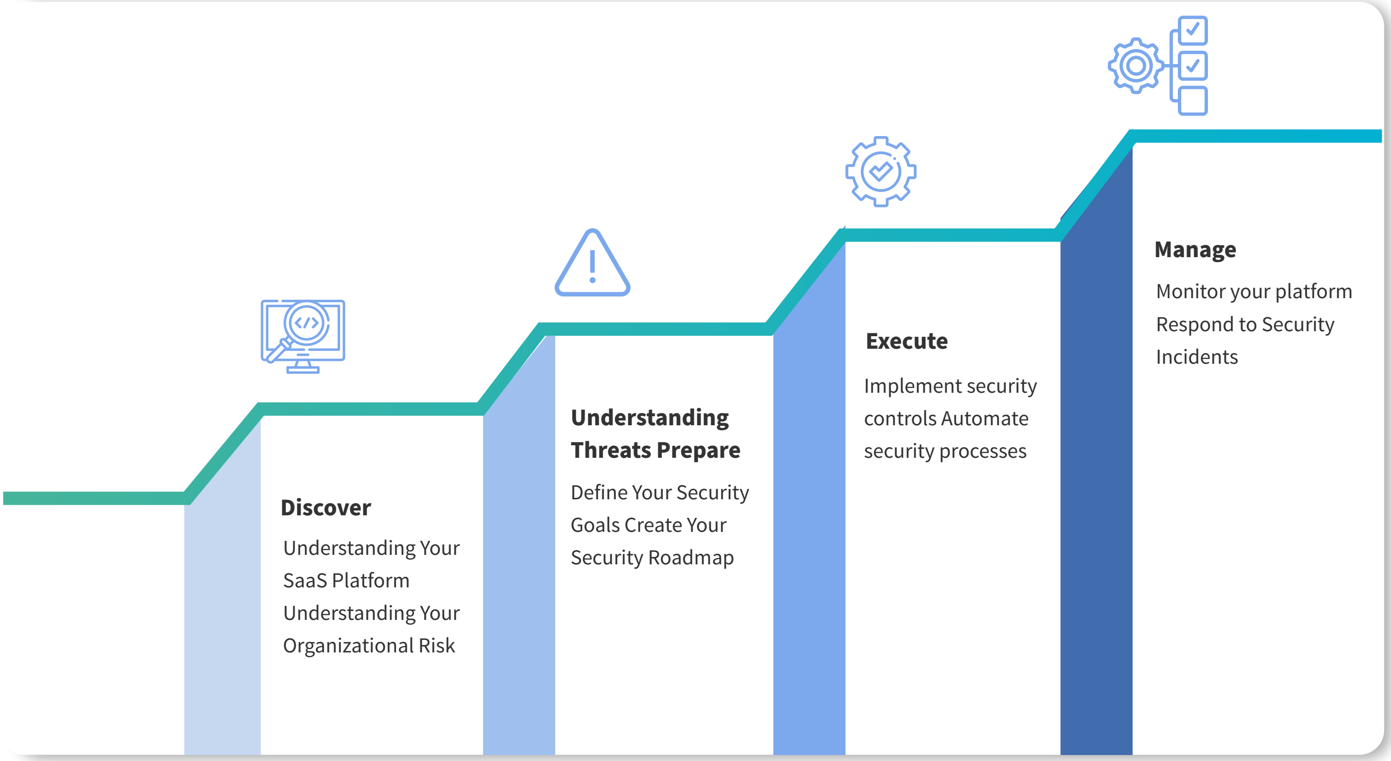
Creating a SaaS Security Program in 4 Easy Steps

Clients put their trust in SaaS platforms when they incorporate these platforms into their IT infrastructure. These organizations often share sensitive data, maintain multiple user credentials, and integrate with servers, databases, and cloud environments to reap a SaaS platform's benefits. Maintaining that trust means SaaS providers must do everything they can to secure their software platforms and keep customer data safe.

> **As third-party supply chain cyberattacks rise, organizations expect stronger security standards from the SaaS platforms they adopt.**

SaaS platforms need a comprehensive security program to ensure the platform—and the customer data it contains—remains secure. As vendor risk management strategies drive more companies to vet third-party platforms, platforms without a defined security program are certain to lose users.

Thankfully, creating a security program for SaaS platforms doesn't have to be hard. Here's a simple blueprint you can follow to create a security program that keeps your company and customer data secure.



Discover

Understanding Your SaaS Platform Understanding Your Organizational Risk

Understanding Threats Prepare

Define Your Security Goals Create Your Security Roadmap

Execute

Implement security controls Automate security processes

Manage

Monitor your platform Respond to Security Incidents

Discover

Discovering what to cover in your SaaS platform's comprehensive security program includes reviewing three areas: your platform, your company's overarching organizational risk, and relevant threats.

Understanding Your SaaS Platform

Many organizations that develop SaaS platforms rejoice when they learn cloud providers offer a shared responsibility model for security. However, these companies often underestimate their role in that shared responsibility, leaving their SaaS platforms open for exploitation.

Work with your DevOps team to better understand your platform and how it's developed. Most companies developing SaaS platforms don't know they're responsible for protecting all the data, containers, applications, and configuration information stored within the cloud provider's accounts. You'll also need to conduct a regular risk analysis to ensure that new code deployments don't create or expose security gaps.

Conduct a comprehensive risk assessment of all the information within your cloud accounts to get a comprehensive view of the platform's security needs.

You'll also need to conduct a regular risk analysis to ensure that new code deployments don't create or expose security gaps.

For SaaS platforms that have already launched, part of the information stored in your cloud accounts is data from your customers. Your organization is responsible for keeping all integrated data secure, so it's crucial to confirm all clouds are configured correctly, including clouds that contain your application, the data your platform produces, and the data your customers provide. Many SaaS platforms cater to customers across multiple industries, which means your organiza-

Understanding Your Organizational Risk

Complete an organizational risk assessment to find what security risks outside the cloud may impact your platform or customer data.

Detecting security gaps within your organization can help prevent a malicious actor from infiltrating your platform code.

It may seem like the organizational risk isn't relevant to your SaaS platform's security program, but understanding your organization's procedures is essential to secure your platform. For example, knowing the security procedures that DevOps follows can help expose gaps that a team monitoring the application itself might miss. Ensuring that DevOps security processes are sound can help prevent cyberattacks like the notorious SolarWinds breach, where a routine update pushed out to SolarWinds software customers contained malware.

Understanding Threats

Reviewing your platform risk assessment alongside your organizational risk assessment will reveal security vulnerabilities and potential threats that your security team must be aware of. Make a record of security vulnerabilities that need to be addressed and create controls to monitor known vulnerabilities closely.

Known threats—or threats security teams have already seen and know how to address—should be included in your security program. Include information about how to identify these threats, what controls are in place to mitigate them, what actions DevOps is taking to close the security gap, and the procedure security teams should follow to control the threat.

To address unknown threats, create a procedure for documenting new threats detected and the efforts taken to fight those threats.

You should also include a process for regularly performing platform risk assessments to discover new vulnerabilities exposed by new code deployments.

Prepare

With your risk assessments in hand, you're ready to create a security plan. Every SaaS platform security plan should define your security goals for the platform and a roadmap to achieve those goals.

Define Your Security Goals

Creating and implementing relevant security controls takes extensive time, money, and resources, so it's important to define which platform security goals to most closely align with overarching business goals.

Knowing the most pertinent threats to your SaaS platform and reviewing your platform infrastructure can reveal security gaps.

Your security goals should equally address managing and reducing vulnerabilities at all infrastructure levels, strengthening data security, and meeting regulatory compliance standards.

You can also consider goals like implementing a zero-trust security framework or automating compliance reporting.

Define achievable short-term and long-term security goals to make the best use of your security budget while introducing stronger controls.

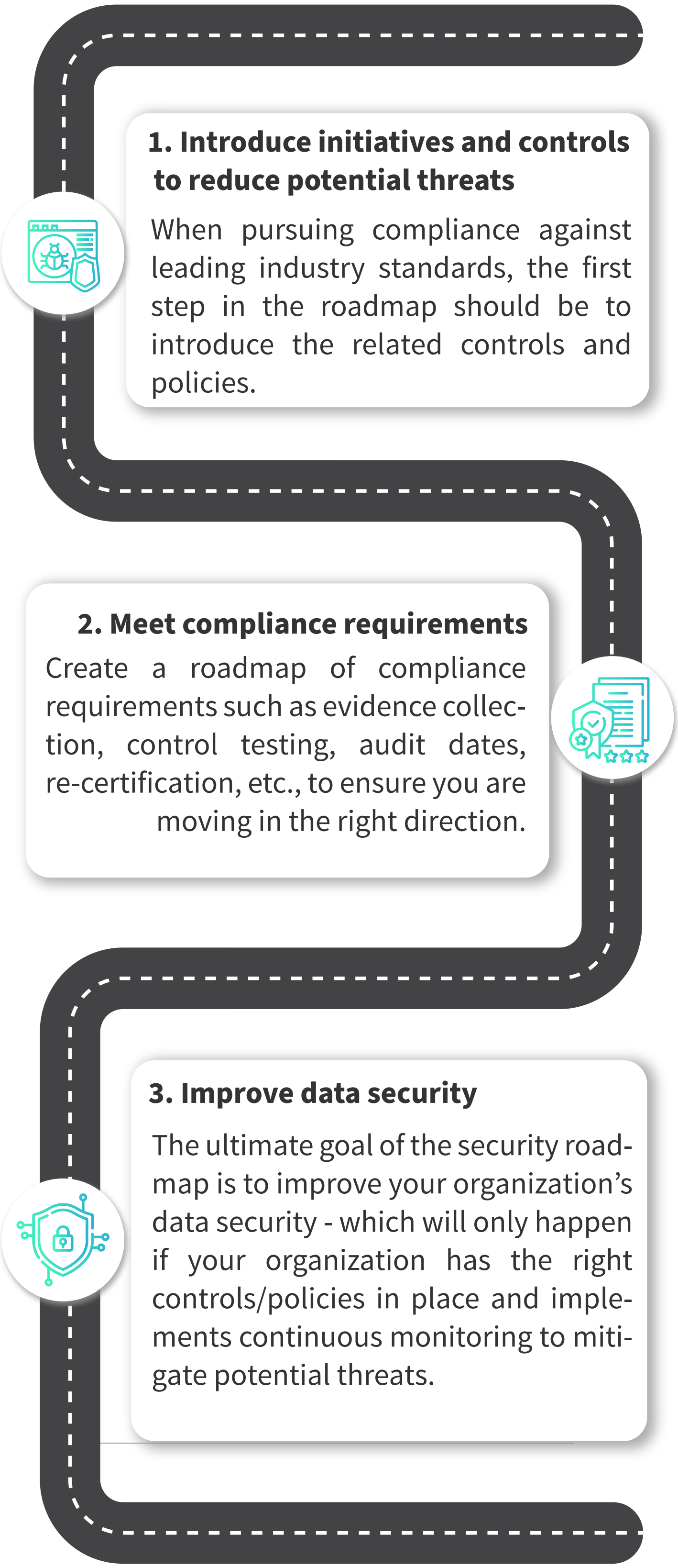
Create Your Security Roadmap

Once you've defined your security goals, you can design a security roadmap to achieve those goals. Often, the roadmap can involve which initiatives and controls to introduce first to reduce potential threats, meet compliance requirements, and improve data security. This security roadmap can also help guide DevOps priorities by defining which security gaps to address first with new code deployments.

For example, achieving SOC 2 or ISO 27001 certification may involve a long process of introducing controls, creating procedures and policies, and drafting other documentation.

Along with goals for designing these components, teams should include target audit dates and compliance dates in their security roadmap, too.

Roadmaps should provide a comprehensive account of your security team's priorities and budget for the future. However, it's easy to get overzealous when defining security roadmaps. Always remember to consider the time you'll need to spend on compliance reporting and auditing or testing new controls to ensure your security roadmap reflects your team's realistic bandwidth.



1. Introduce initiatives and controls to reduce potential threats

When pursuing compliance against leading industry standards, the first step in the roadmap should be to introduce the related controls and policies.

2. Meet compliance requirements

Create a roadmap of compliance requirements such as evidence collection, control testing, audit dates, re-certification, etc., to ensure you are moving in the right direction.

3. Improve data security

The ultimate goal of the security roadmap is to improve your organization's data security - which will only happen if your organization has the right controls/policies in place and implements continuous monitoring to mitigate potential threats.

Execute

Security goals and an implementation roadmap defined what security controls to prioritize to secure your SaaS platform. Now that you have a plan, it's time to get started on the most essential security controls and capabilities to support your SaaS product.

Implement security controls

While you may have introduced some security features in your SaaS platform's initial design, you still need to create controls to ensure those safeguards continue to function properly. Security teams for SaaS platforms will typically introduce different security controls first, depending on which compliance requirements apply to the data the platform collects and stores. Many compliance standards define certain controls companies must have in place to manage their data, so these controls are a good place to start with implementation.

For some controls, your organization may work with a dedicated vendor solution. Your security team must evaluate relevant vendors on the market and find the best fit for your SaaS platform.

It's common for a vendor solution to overlap and cover multiple security controls that may be required for compliance. Then, your team will need to roll out these new solutions and test controls to ensure they're operating properly.

As your team implements new controls on your security roadmap, it's important to document what controls you're implementing and the procedures for testing or maintaining that control. Some compliance certifications will require this documentation to show adherence to their standard.

Automate security processes

Some controls and processes are best managed with automation. Security automation can help stretch your security budget and allow your security team to focus on more strategic work.

> **Some security processes need to be predefined before they can be automated, like the procedure for de-provisioning access to a former employee**.

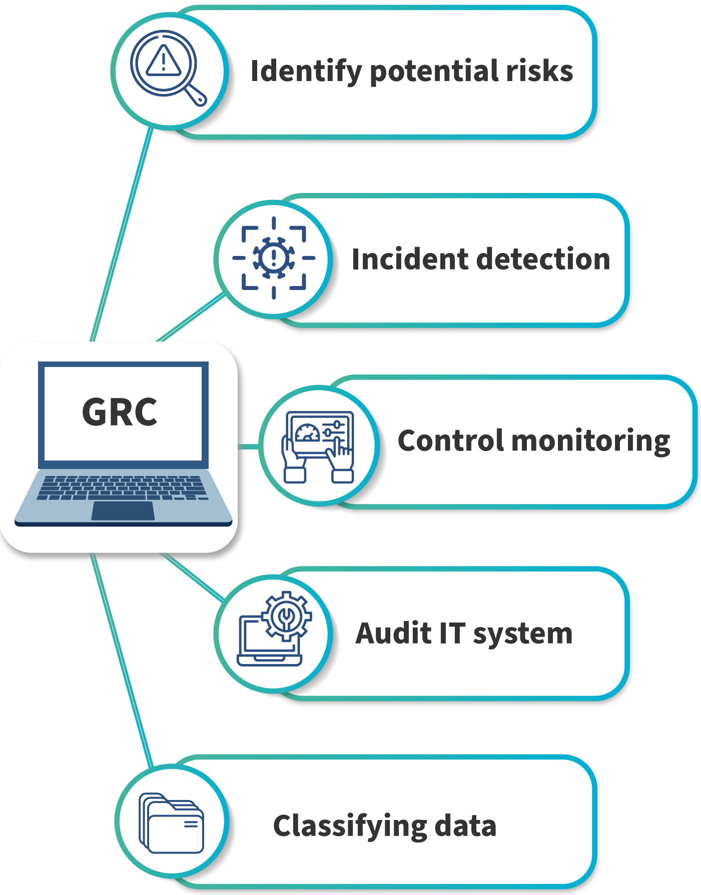
Others, like incident detection, rely on machine learning to identify irregular patterns and alert the security team of a potential threat.

Governance and compliance tasks are frequently automated to reduce the manual workload and reduce the risk of human error. Auditing IT systems and reporting to regulatory bodies manually can take security teams thousands of hours each year. Meanwhile, automatically discovering and classifying data can provide more accurate reports while saving time and resources.

In today's cybersecurity environment,

> **There's no way a security team can manage all their IT infrastructure manually**.

Teams rely on automation to streamline monitoring, maintain visibility across their infrastructure, and prioritize the most important security threats.



Manage

As your team continues implementing controls and automating processes from your security roadmap, they must also manage real-time security for their live SaaS platform. While automation and controls work in the background, teams must track the success and efficacy of their controls by monitoring the platform and responding to security incidents.

Monitor your platform

Even the most sophisticated security controls benefit from a human perspective, and security teams must continuously monitor and optimize their controls to reduce the risk of a breach. Putting these controls in place allows security operations teams to monitor performance and behavior across their organization's IT infrastructure, so teams can detect and investigate a potential breach quickly.

Monitoring your SaaS platform involves not only looking for incidents. It also includes

Scanning for vulnerabilities within your IT environment, testing existing controls to ensure they're working ongoingly, and detecting new risks and threats.

monitoring tools produce notifications for security operations teams, and responding to those notifications can help teams prioritize their daily work and direct DevOps on changes needed to make the platform more secure.

Respond to Security Incidents

Automation alone is not enough to keep your SaaS platform safe. While automated controls can address some potential threats directly, many require hands-on investigation once they've been detected through automated scans or real-time monitoring.

These controls and monitoring tools work by sending notifications to security teams to inform them of abnormalities within their IT environment and prompting them to investigate the abnormality. Using these tools,

Security teams can detect potential threats, discover the cause of the threat or the security gap at risk, and mitigate the impacts of the threat before it becomes a breach.

Strong controls and relevant tools can offer significant support with the

Decreasing mean time to detection and mean time to resolution

two key performance indicators security teams often measure as part of their goals. Plus by responding to security incidents, your team can identify more known threats and mitigate those threats by upgrading your SaaS platform. Organizations should maintain detailed documentation about the security issues they experience and update their controls, policies, and procedures to standardize responses to known threats.

Some incidents may not be discovered right away, which means data may have been exposed or compromised. Security tools can also help your team identify what systems and data have been compromised and automatically remediate breaches. Automated remediation also allows your team to do their due diligence by communicating with customers or regulatory bodies when data is exposed.

your team identify what systems and data have been compromised and automatically remediate breaches. Automated remediation also allows your team to do their due diligence by communicating with customers or regulatory bodies when data is exposed.

Strengthen Your SaaS Platform's Security Program with Scrut Automation

When you're creating a comprehensive security program for your SaaS platform, you want to make sure it's done right the first time. That's why so many companies spend countless hours interviewing vendors to find the best fit for their platform. Setting up strong security controls is critical to protect you and your customers' data, and you rely on best-in-class tools to help you mitigate risk and avoid breaches.

Tools like Scrut Automation.

At Scrut, we offer a smart and radically simple way to manage all your governance, compliance, and risk controls. Our innovative platform allows companies like yours to manage and monitor all your security controls in one place, so you know your SaaS platform is secure. Plus, Scrut automatically maps your data to applicable regulatory standards like SOC 2, HIPAA, ISO 27001, GDPR, PCI DSS, and CCPA, saving your team thousands of hours on compliance auditing and reporting.

Your security operations team has enough to keep track of. Leave the compliance controls to Scrut. Schedule a demo today and discover how Scrut can strengthen your SaaS platform's security program.