Scrut Automation

Security Best Practices For Startups

Scrut Automation

Contents

Abstract

Security is super important in today's complex business environment due to the increasingly mobile/hybrid nature of the modern workforce, a continuously evolving technology stack, and the pervasiveness of cyber attacks and malicious hackers looking to exploit vulnerabilities in corporate IT environments. **It is even more important for startups since they may prioritize faster time to market over cybersecurity and compliance requirements as they race to grow their user base and become profitable.**

Not having time, funding, or resources is no excuse to skip or gloss over security measures. A lightweight approach to security will drastically increase the chances of a breach and jeopardize the successful launch and adoption of your product/service. This ebook outlines 10 security best practices for startups to shore up vulnerabilities within their IT ecosystem and provide a solid foundation for building an effective startup security plan.

Control User Access to IT Resources

Controlling access to IT resources is a critical part of enterprise security strategies and is foundational to a security-centric culture. Deploying an Identity Access Management (IAM) solution is a great way for startup founders to control user access to IT assets whether it's databases, networks, files (in on-prem or cloud storage), applications, reports and analytics, devices or IT equipment, etc. The ideal IAM solution should have the following capabilities:

- Audit logging, insights, and reporting
- Automated user and resources provisioning/de-provisioning via secure protocols
- Single sign-on (SSO)
- Policy-driven user groups
- Customizable security policies
- Secure user authentication and authorization
- Centralized directory for storing user data across on-premises and cloud resources
- Flexible enough for hybrid workforces (in-office, remote, and mobile)
- Assign user access using the principle of least privilege
- Put systems in place to track users' information and system activity
- Ensure that only privileged users can access personally identifiable information (PII)
- Ensure role redundancy in the case of an emergency

Did you know?

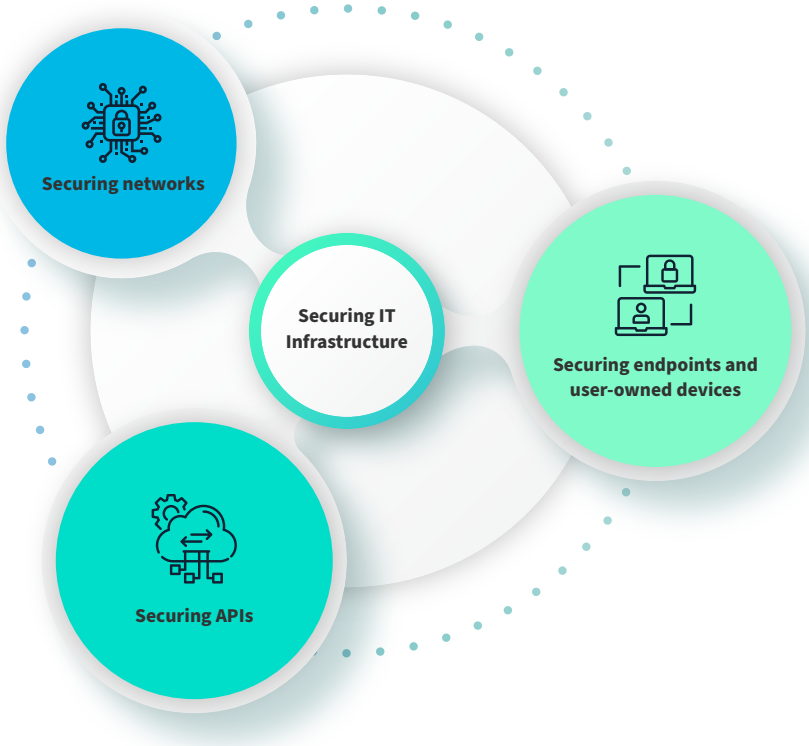
- ABAC (account-based access control) - uses policies to set permissions from attributes
- RBAC (role-based access control) - uses predefined roles that explicitly dictate varying levels of permissions

Key takeaways:

Implement a robust identity and access management policy.

Control user access to key assets through an Identity Access Management (IAM) tool.

Secure IT Infrastructure



Securing endpoints and user-owned devices

A great way for founders to secure IT infrastructure and efficiently manage all endpoints and user-owned devices within the startup environment is by leveraging security tools and creating security policies that facilitate the following

- Create a unified ecosystem that seamlessly manages devices and users, regardless of location or operating system.
- Turn on disk encryption for all devices and machines
- Ensure that all network-connected devices are visible and trackable
- Enforce screen locks after a short period of inactivity
- Automate device updates and patching using a patch management tool
- Require multi-factor authentication login for all devices
- Assign each user device to a policy-governed device group
- Restrict sharing of user devices, especially in remote and hybrid work environments.

Securing APIs

Since APIs often connect the logic of business apps to user data, they are an attractive attack vector for cybercriminals. If the right security measures aren't in place, hackers can execute SQL injection, cross-site scripting (XSS), and Man-in-the-middle (MitM) attacks on vulnerable APIs to gain access to a startup's infrastructure. Securing APIs will involve

- Building a thorough inventory of all APIs
- Analyzing and mitigating API data exposure
- Using TLS to encrypt traffic
- Deploying a web application firewall
- Using proven protocols for authentication procedures
- Validating all inputs

Securing networks

With the seemingly limitless expansion of traditional network perimeters, there's a real need for stringent, software-driven security for network access and usage. Startups must ensure that their central networks are protected with modern multi-layered safeguards to block attacks from virtually all vectors.

A private VPN is a popular option for enterprises looking to secure remote connections to their IT infrastructure. Many startups also opt for cloud directories that use RADIUS, SAML, LDAP, or other authorization/authentication protocols to secure remote access to resources.

These protocols should prohibit network access from unprotected and public WiFis and also enforce conditional access policies that relax or enforce multi factor authentication based on the particulars of the login attempt. VLANs can also be used to segment the network and provide access to only users with the proper network access permissions while next-generation firewalls can be deployed to facilitate application-level inspection and intrusion prevention.

Key takeaways:

- Secure end-point devices and user-owned/BYO devices.
- Assess API data exposure, and Identify and secure vulnerable APIs.
- Protect central networks with modern multi-layered safeguards.

Enable data security

Business owners prioritize data security to protect business data everywhere from devices and endpoints to networks, servers, on-prem systems, across the web, and in the cloud. The first step towards securing sensitive data is **putting in place a data collection and retention policy** that establishes the procedures for data management and protection. This includes when and how data is collected and retained, who can access the data and the types of data to be encrypted.

Savvy startups go a step further to encrypt and back up their data. This helps to maintain its confidentiality and integrity. **Encrypting data at rest and in transit adds an extra layer of safety** that prevents malicious actors from exploiting stolen data, even when they successfully breach networks. This encryption should protect data how ever, whenever, and wherever it is accessed. This means the use of HTTPS, TLS, SSL, SSH, and other security protocols for data transmission.

It's also a great idea to **deploy a data loss prevention platform** that uses proven techniques and reliable technologies to automate the tracking of sensitive business data. These platforms monitor the transmission of data and can prevent the illicit transfer of data from corporate networks to unauthorized entities.

Key takeaways:

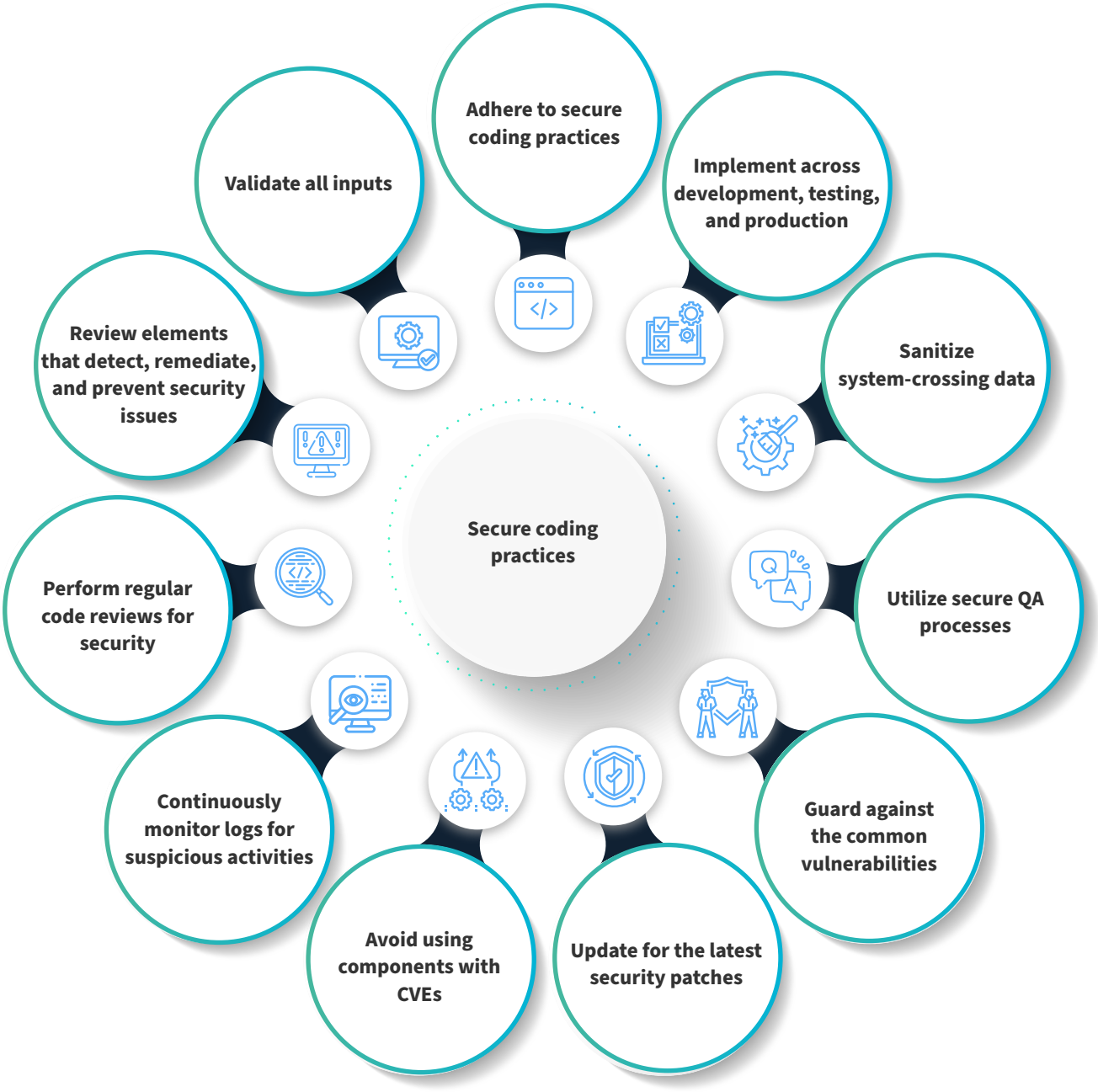
- Implement a robust data management and retention policy.
- Encrypt data at rest and data in transit using relevant protocols.
- Deploy a data loss prevention platform (DLP) to track sensitive business data.

</> Implement secure coding best practices

It's virtually impossible to protect digital products from every possible attack vector due to the large number of latent vulnerabilities within platforms, languages, and systems. Rather than expend time and resources towards fixing every potential vulnerability within the code, it's best to protect what matters the most and safeguard against well-known attacks and potential zero-day hacks.

Secure coding is a software engineering best practice that can save startups a lot of headaches by preventing security bugs and vulnerabilities from creeping up within their code. Secure coding practices include:

- Validating all inputs, especially from external data sources.
- Write code while adhering to secure coding standards and practices.
- Sanitize system-crossing data, especially those passed on to complex subsystems.
- Use effective quality assurance processes including source code audits, penetration testing, and fuzz testing.
- Protect APIs from injection attacks.
- Focus on guarding against the more common vulnerabilities such as those in the OWASP top 10.
- Update all dependencies using the latest security patches.
- Avoid using packages and libraries with known vulnerabilities i.e. CVEs.
- Enable logging and continuously monitor them for suspicious activities.
- Perform regular code reviews...reviewers should pay particular attention to sections of code that deal with payments, authentication, authorizations, transmission/storage of PII and other sensitive business/personal data, etc.
- Ensure the accuracy of technical elements that detect, remediate, and prevent security issues.
- Implement secure coding practices at every phase including development, testing, and production.



Engineering teams should also perform vulnerability tests, execute automated source code analysis, and develop applications with a security-first mindset.

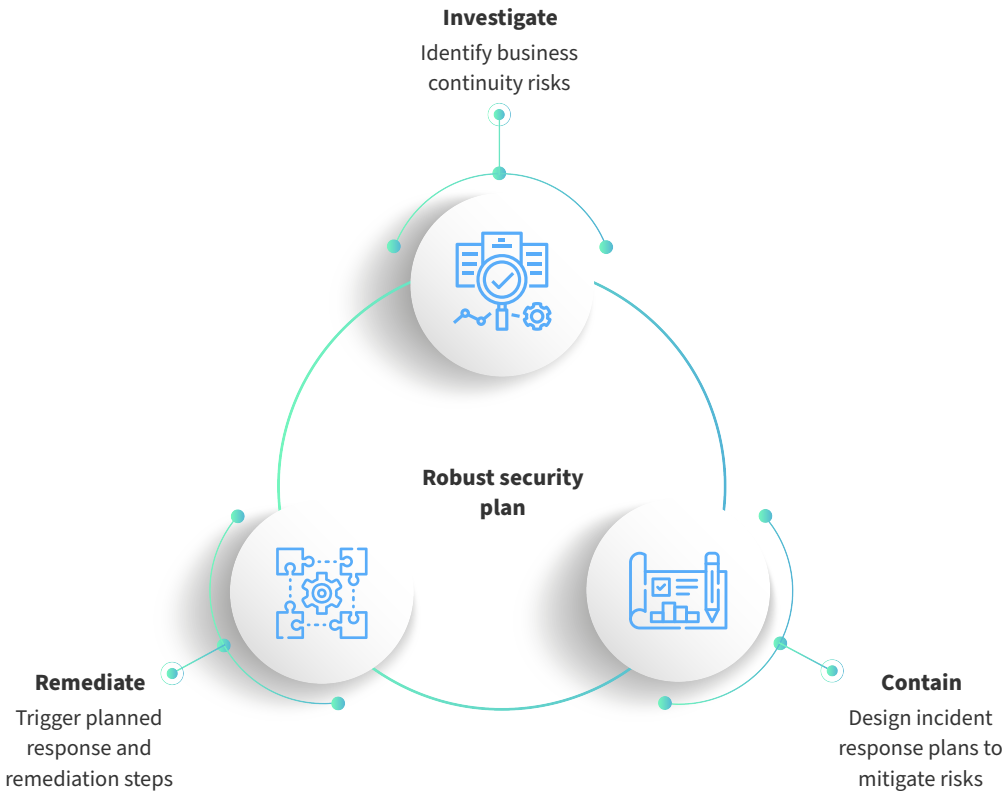
Key takeaways:

- Shift Left - implement secure coding practices.
- Build security-first mindset in engineering teams.

Design a security plan /BCDR Policy

Despite an organization's best efforts, malicious attackers can launch sophisticated attacks that bypass the best cyber defense mechanisms and cause a data breach. Aside from cyber attacks, disasters and emergencies also pose a security risk to business operations. Savvy startups **design security plans and BCDR policies** to mitigate the impact of such disasters. These policies contain contingency plans in the event of a data breach to ensure business continuity and operational viability in the aftermath of a cyber attack.

The first step towards designing a BCDR plan involves **identifying and understanding business continuity risks.** Risk assessments can help pinpoint vulnerabilities within IT systems, identify potential cybersecurity threats and root out factors that could result in disasters/downtime. Management can then **design incident response plans** to mitigate the repercussions and reduce the prevalence of these threats.



An incident response plan views security threats and data breaches as inevitable and details response steps to be triggered in the event of a breach. This includes investigation, containment, and remediation procedures. Having a dedicated incidence response (i.e. BCDR) team can make this easier. The plan should detail how employees can ascertain the criticality of security events and escalate to the proper channels when necessary.

Key takeaways:

Design security plans and BCDR policies to mitigate the impact of cyber-incidents

Allocate clear accountability for executing incident response plan

Educate and train employees

After deploying the latest cybersecurity tools, startups can still be vulnerable to security risks if their employees routinely click on suspicious links and ignore security protocols. **Employees are often the weakest link in any cybersecurity strategy.** However, they can easily become the strongest asset in a startup's security arsenal with the proper training.

A data breach will occur when employees, contractors, and third parties with privileged system access aren't adequately trained on how to identify and respond to red flags that indicate a phishing attempt or a potential security attack. Most phishing attempts can be prevented if employees know what to look out for. With studies showing that **human error causes over 90% of cybersecurity breaches**, startups must provide employees with heightened cybersecurity training and awareness to avoid errors that can result in data breaches and disrupt business operations.

Organizing regular security training on how to recognize and report phishing, social engineering attacks, and other security vulnerabilities will help employees and other users avoid human-driven security risks. For better results, **make cybersecurity training a core part of the employee onboarding process.** This ensures that employees are well acquainted with the organization's security protocols from the very onset and start off on the right foot (security-wise).

Key takeaways:

- Create role-based security training programs for employees
- Conduct trainings during onboarding, with bi-annual refreshers, and as need arises

Effective device updates and password management

An effective way to prevent unauthorized access or theft of IT resources is to design password management policies to ensure that only authenticated users' (across remote, on-prem, or hybrid work environments) can securely access said resources. These policies should facilitate the following:

- Create stringent complexity requirements.
- Ensure periodical password rotation.
- Prohibit password sharing.
- Enforce MFA, minimum length (12 characters or more), and password uniqueness (for instance, the use of passphrases).
- Avoid users sharing accounts or passwords (this is particularly important in startup environments looking to reduce expenditure on licensing costs).
- Deploy password managers to help users create unique passwords for each user account - without having to remember them.
- Store users' passwords with a cryptographic hash and salt the hash.
- Simplify user provisioning, de-provisioning, and logins by deploying SSO (this enables users to sign in to all their accounts with one set of credentials).

Also, regularly updating systems is a great way to keep phishing, ransomware, and other cybersecurity attempts at bay. Old versions of firmware, software, and hardware systems don't have the latest security patches and this leaves them vulnerable to ever-evolving threats.

Key takeaways:

Implement strong password management policies and tools to execute these policies.

Regularly update all your systems to ensure you have the latest security patches.

Implement Zero Trust Security Principles

Zero trust enables a layered, software-driven security approach that safeguards IT infrastructure by verifying everything and trusting nothing. Authorized access to IT resources is granted only when the network path, device, and user identity have been thoroughly vetted by passing through multiple layers of security. This principle should apply to both company- and employee-owned devices.

Although BYOD can help boost employee productivity, satisfaction, and engagement levels, they introduce another layer of complexity when it comes to the security of a startup's IT ecosystem. These devices can become a security concern when there are weak/inadequate BYOD policies in place or employees become lax in adhering to BYOD requirements. An effective BYOD policy should :

- Protect devices by requiring multi-factor authentication and preventing the download/installation of unsafe applications.
- Keep an accurate inventory of all such employee devices.
- Limit the type of data employees can access based on their access privileges and designated roles.
- Facilitate remote wiping of sensitive information in case of theft or when employees leave the organization.
- Prohibit employees from connecting to Wifi in public places.
- Prevent the transfer/download of sensitive business to device physical storage or unauthorized external mediums such as USBs, etc.

Key takeaways:

Implement a layered, software-driven security approach to safeguard IT infrastructure.

Introduce secure usage of devices in BYOD policies.

Set up an IT asset inventory system

An IT asset inventory system helps startup founders track every hardware and software asset within their IT infrastructure. This helps them to stay ahead of the security concerns each asset brings to the table as well as avoid the creep of "shadow IT". Else, a data breach may occur and incident response teams will be scrambling to understand the source of the attack and identify the threat vector or vulnerability that allowed attackers to gain access to their infrastructure.

Aside from taking stock of all on-prem and cloud systems/devices, auditing the SaaS stack is a great way to keep track of the apps that expose startup employees to phishing attempts and cyber attacks. **On average, employees use eight SaaS apps, and companies with fewer than 50 employees deploy as many as 40 SaaS apps.**

Every one of these apps represents a slew of potential vulnerabilities. Periodically auditing the SaaS stack helps startups understand how many of these apps are used by employees and the level of risks they represent. With this knowledge, startups can review each app's security capabilities and ascertain if the benefits are well worth the risk of adding it to their IT infrastructure.

Key takeaways:

- Build and monitor a comprehensive list of all hardware and software assets.
- Regularly audit your SaaS stack, usage and potential

Build a strong security culture

Fast-growing startups need to balance the need for speed, agility, and faster time to market with security and regulatory compliance. A seamless blend of operational security, infrastructure security, and applications security is ideal for virtually all IT environments. While deploying a versatile tableau of technology-based security solutions will ensure adequate protection, focusing on people and processes can deliver unbelievable returns.

Since a large percentage of data breaches have been attributed to human error (rather than flaws in technology), **a security-first approach to operational workflows is key.** This can be done by infusing security into the startup's workplace culture and educating customers about account takeover fraud which cybercriminals can use as entry points to search for exploitable vulnerabilities. This is especially true for startups with SaaS and other digital product offerings.

Outsource to a trusted MSSP or a dedicated security resource/professional
Startups may find it difficult to dedicate time and resources to building a security product that's tailored to their unique security challenges. Off-the-shelf solutions may also be costly and lack features that are required to safeguard the startup's unique IT stack and operational workflows.

Many companies handle this by outsourcing all or part of their security operations. While it's advisable to use in-house talent to design an effective security strategy that safeguards your product's software architecture and codebase, there are a lot of benefits to outsourcing the rest of your security requirements. Companies can avoid having to make large upfront investments in building unique security products by outsourcing security needs to an MSSP or a dedicated security resource/professional.

Key takeaways:

- Build a top-down security culture, with leaders enforcing the importance of security.
- Leverage MSSPs for managing security processes in case of lack of right resources.vulnerabilities.

Wrapping Up

While this is not an exhaustive list, the above best practices will help reduce the chances of cyber attacks, plug vulnerabilities within networked systems and make it extremely difficult for malicious actors to gain a foothold in your startup's IT environment.

With cybercriminals increasingly targeting corporate databases/networks to steal valuable business data and compromise IT systems, startups need to proactively protect their digital assets from malicious attacks by beefing up their security infrastructure. However, investing in security is hard, even for established companies, and can be particularly difficult for startups.

Fortunately, Scrut solves this conundrum by delivering everything startups need for securing their IT ecosystem and staying compliant in one platform. With Scrut, you can automate risk assessment and monitoring, build unique risk-first infosec program, effortlessly manage multiple compliance audits, and demonstrate trust with your customers – all from a single window.