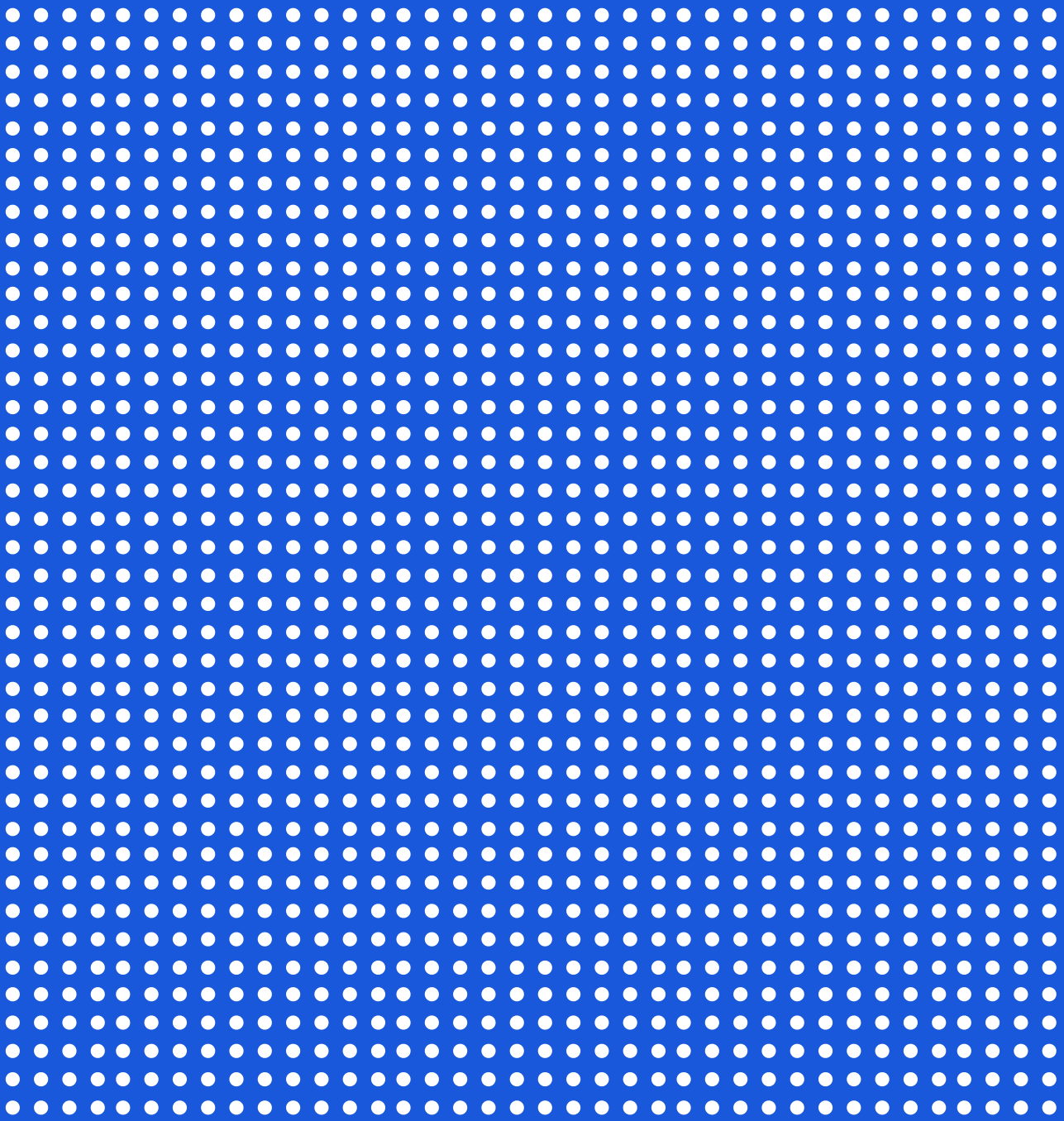
Securitypage.fyi

resmo



Security Page Guide

Table of Contents

1 Introduction

2 Why Security Pages Matter

3 Security Communication Best Practices

4 Security Page Inspirations

5 Resmo

6 Conslusion

Introduction

This guide is created to help you set up your security page that follows generally accepted best practices. The information provided can help clarify concepts, ensure consistency, and meet the **established standards across security pages**. It contains information on some pillars for a minimum viable, secure product and what to cover on a security page.

Why Security Pages Matter

Security is just as important to developers and end-users as it is to the IT staff that runs the servers. End-user education can be a massive part of what makes or breaks a security program.

Educating your users on best security practices—along with tips for spotting phishing emails, avoiding malware, patching vulnerabilities, and otherwise protecting sensitive information—should be a top priority for any organization.

1

Increases Sales

Security landing pages possess a **close to direct impact on increasing sales**, especially for businesses that rely on an online presence like the SaaS or e-commerce industry.

In the face of cybersecurity threats, including phishing attempts, data leakage, and hacking, the modern consumer wants to know if they can trust a business before making a purchase of even a small kind.

Having a clear security landing page on your site that prospects can easily access **eliminates doubts** and assures them that the company is secure enough to make an online purchase. Consequently, this results in a rise in your bottom line.

2

Multiplies Signups

Companies that gather their security efforts on a dedicated web page can see a boost in their signup rates. The logic behind this increase is simple.

Whenever a consumer needs to achieve something online, whether it's buying an item, getting a service, or downloading an ebook, they find themselves in a decisive moment–to give up data in return or not to give up data.

A security page **helps companies build that trust right from the start** and encourage signups.

3

Speeds Up the Sales Cycle

Traditionally speaking, a customer follows through a sales pipeline and progresses through different customer journey stages. In that respect, a security page holds power to **make a trustworthy company image** as the first impression on the customer.

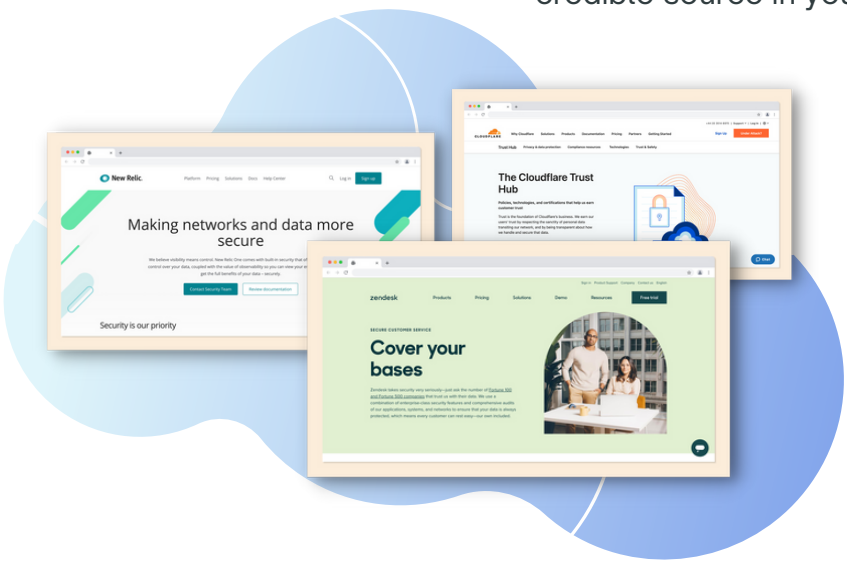
This shortens the sales cycle and helps push the customer through the sales pipeline, adding up your bottom line.

4

Doubles up Business Credibility

Needless to say, trust is the cornerstone of a business' healthy relationship with customers. This applies to both B2B and B2C companies. One of the most appropriate ways to acquire that trust is to use your business front effectively–that being your website.

By presenting your security and compliance efforts on a security page, you can **build up customer trust** and position yourself as a credible source in your industry.



5

Helps Standing Out Among Competitors

Though security posture is an integral part of a brand image, many businesses skip the advantage of letting people outside the company know about it.

Creating a security page that overviews your company's security posture, compliance, and efforts lets you get ahead of your competitors since customers tend to do business with trustworthy companies.

Security Communication Best Practices

1. **Display** Compliance frameworks

A security compliance framework is a set of rules that an organization must follow to ensure that it's taking the right steps to protect its systems, networks, and data. A compliance framework typically includes some or all of the following:

- **Protecting** and monitoring network infrastructure, servers, and applications
- **Monitoring** user activity and data to detect suspicious behavior
- **Enforcing** security policies and access procedures
- **Responding** to reported violations in a timely manner

Displaying compliance frameworks on security pages provides a clear understanding of the company's commitment to data protection. While the complied frameworks vary depending on the industry, common ones include SOC, ISO, HIPAA, FedRAMP, and PCI DSS.

Leading companies typically showcase the badges of some of these frameworks on their security pages to assure the customer that the company is **compliant** with industry standards.

2. **Mention** Identity and access management (IAM)

Identity and access management (IAM) is the practice of controlling access to systems by requiring users to identify themselves to gain entry. An IAM policy controls who can access what systems and actions they can perform.

There are many aspects to identity management;

- **Defining** the identities users will use within your organization (user provisioning)
- **Ensuring** that each user authenticates successfully with your network (user authentication)
- **Accessing** resources from a single sign-on (single sign-on) experience.

Highlighting a product's identity and access management capabilities on a security page is crucial to reassure users that their data will be protected. Some of the commonly highlighted IAM capabilities include:

Single Sign-On

A single sign-on often called SSO for short, is an authentication process that allows users to log in to multiple applications and websites with a single username and password.

Why do businesses choose SSO?

- **Fewer login credentials:** Your account credentials are stored in a secure database that only the company can access.
- **Better security:** A centralized database is more difficult to hack than individual databases because it's harder to get unauthorized access.
- **Improved performance:** SSO saves human intervention by handling the authentication for you.

Access Control

Access control is a method used to prevent unauthorized access to resources. It can be applied to the operating system, application, or both. Access control is a **powerful extra security layer** for protecting data and applications from attack and abuse.

While there are various ways to manage access, common methods include role-based, request/approval, and attribute-based. Industry leaders typically apply access control frameworks like ISO 10181-3.

Two-factor authentication (2FA)

Two-factor authentication, also known as two-step verification, is a **security measure** used to protect data and account information. For example, using a password and a mobile phone number or text message as a second factor can help ensure that an account is secure.

Multi-factor authentication (MFA)

Multifactor authentication (MFA) is a security solution that combines two or more factors to help **reduce the risk of unauthorized access** to your accounts. It can be SMS-based authentication, audio-callback user verification, or a one-time password generator (OTP).

3. **Present** data protection efforts

Typically, companies dedicate a section on their security page to essential data protection measures they take, such as Audit Logging, Backup, and Disaster Recovery policy, and data encryption at rest and in transit.

Encryption

Data encryption is the process of encoding your data in a way that makes it unreadable without the proper key. It is essential to mention data encryption on a security page in order to **reinforce customers' trust** in data privacy. Typically, it is highlighted as data encryption in transit and at rest.

Data loss prevention (DLP)

Data loss prevention (DLP) is the practice of **protecting sensitive data from theft** and unauthorized access by ensuring the integrity of sensitive data through automated and manual controls.

4. **Provide** vulnerability reporting methods

It is essential to provide method/s to report security vulnerabilities and inform users about your disclosure policy and vulnerability management program. These methods vary based on the company; however, companies typically give a gist of disclosure policy on their security page along with the reporting method. These methods can be **bug bounty programs** or r**eporting through email**, or both.

Pro Tip: Create an email address specific to security contact such as *security@example.com*.

5. **Outline** product security features and best practices

Security pages can be beneficial in promoting your platform, company, or product since they **build trust in the customer**. As a common practice, SaaS platforms, for example, list a summary of their product security features and best practices that customers can use and follow.

Furthermore, many cloud-based platforms apply a **shared security model**, which puts some responsibilities on the customer side while the provider maintains some. Therefore, these platforms often instruct customers on data and privacy protection measures, such as using a strong password and enabling 2FA, which they can take and the company-side responsibilities.

6. **Link** to additional security resources

Even the most extensive security page cannot cover every single detail about a company's privacy policy, compliance, and security posture. That is why it's essential to **provide quick links to additional resources**, such as whitepapers, datasheets, docs, separate compliance, transparency reports, and privacy policy pages.

7. **Inform** about internal Security Measures

Internal security measures are **taken against data compromise** due to employee ignorance, facility break-in, or similar conditions. These measures might include:

- Employee training
- Employee hardware and software security
- Physical security of relevant facilities
- Limiting sensitive data sharing
- Having a proper response plan for intruders

8. **Explain** cloud security measures

Cloud security forms the most vital part of the security of cloud-based platforms. Industry leaders typically use a set of technologies to **prevent data compromise** and unauthorized access. These include physical control, restricting access by implementing firewalls, and network security control.

9. **State** subprocessor and vendor management policy

Vendor management is the process of evaluating the risk a vendor poses to your company then taking steps to mitigate that risk.

It is necessary for two reasons:

- You need to **protect your own data and systems**. If a vendor suffers a breach, your company could also be at risk.
- You may have an obligation to **protect client data and systems**. Many clients require you to undergo regular third-party assessments as part of their vendor qualification processes.

For these reasons, providing information about your vendor management system and **the scope of data you share with third-party vendors** on the security page or through a link to a related page is essential.

10. Add CTA buttons to encourage signups and sales

Promoting your products and services or encouraging signups on the security page is advantageous as these pages increase customer trust. While most companies typically use the CTA buttons both above the fold and at the bottom of a security page, some only include CTA buttons at the bottom. Additionally, calls to action for free trials and contacting sales are commonly used.

11. Highlight authentication and password policy

Password policy covers password authentication methods in addition to single sign-on (SSO). These include:

- Passwords consisting of at least 64 characters
- Not limiting the permitted characters to be used in passwords
- Providing an email verification upon a password change request
- Requiring both current and new passwords for a password change

12. Mention privacy policy and regulations

Including a quick link to the company's privacy policy page is common for optimal security pages. However, some platforms skip building a separate privacy policy page and address the issue on the security page.

Furthermore, when mentioning data privacy, it is essential to support your posture with widely-accepted privacy regulations like **GDPR** or **EU-US Privacy Shield**.

13. **Assure** on incident management

A security incident is an event or event series that violates an organization's information security policies, threatens the **confidentiality, integrity, or availability of data or systems**, or poses a risk to business operations. Incidents can involve malware, viruses, insider threats, and other types of cyberattacks.

Security incident management is an integral part of any organization's cybersecurity plan. It ensures that an organization knows what to do when systems don't work as expected, whether an attacker or a technical glitch causes that issue.

14. **Inform** about backup and disaster recovery

Companies that manage and store data must have a Disaster Recovery Plan as a standard security best practice. They should maintain and regularly test it. Likewise, making a **secure backup of all data** to a different location and automating the backup process adds an extra layer of security.

15. **Detect** and get alerted on vulnerabilities

Most companies store their data on the cloud and implement different vendors into their workflows. These leave many of them vulnerable to data compromise, loss, and security threats of varying degrees.

One optimum solution to such issues is using a continuous cyber asset visibility platform like Resmo to **gain insight into all your SaaS and cloud assets** from a single platform, make queries, set rules, and get alerted in real-time.

Security Page Inspirations

Zendesk

Zendesk's security landing page is more of an all-in-one page covering the platform's compliance, security, privacy, and legal notices and efforts.

See full review →

Datadog

Datadog's security page compiles security, data protection, compliance efforts, and vulnerability reporting documentation on a single page. In general, Datadog addresses product, physical, and corporate security.

See full review →

Canva

The spotlight of Canva's security page is on its security features such as data encryption, global CDN, SSO, and MFA options. While the page, by and large, is brief, Canva's bug bounty program stands out with a CTA button to learn more.

See full review →

Auth0

Auth0's security page is a compilation of security, privacy, and compliance at Auth0. Overall, it covers compliance certification and attestation badges, GDPR compliance, Auth0's security capabilities, and a downloadable whitepaper.

See full review →

Webflow

Webflow approaches the security page in whitepaper format. The page divides into five main sections starting with Webflow's Information Security Program and continuing with other security-related topics like internal security measures and compliance certificates and reports.

See full review →

Security Page Inspirations

New Relic

New Relic covers all the highlights about product security, FAQ, links to additional resources, and compliance certifications. Product security capabilities focused on the page include data encryption, authentication, and access management.

See full review →

Snyk

Synk has a brief, security, and compliance-combined page. The page provides information about compliance certifications and attestations, including ISO and SOC and GDPR compliance.

See full review →

Gremlin

Gremlin's security page consists of three tabs; overview, practices, and docs. The overview is the primary page. It showcases badges of security frameworks, regulations, and certifications, as well as two calls to action buttons directing users to download security FAQs or see security practices.

See full review →

Zapier

Zapier addresses security and compliance issues as a branch of their help documents. The compliance certifications displayed on the page are SOC 2 Type 2 and SOC 3, linked to related reports.

See full review →

Notion

Notion's security page combines security, privacy, compliance as well as a sales prompt. The page provides info about the data protection practices they undertake, such as data encryption and the hosting platform they use (AWS.)

See full review →

Security Page Inspirations

Splunk

Splunk covers all security, compliance, data privacy information, certifications, and principles on its security page with additional tabs for detail pages such as Compliance and Security Portal.

See full review →

Cloudflare

Cloudflare's security page is a unification of Privacy & Data Protection, Compliance, Technologies, and Trust & Safety, all given under Trust Hub. Overall, they focus on privacy, technologies, policy, and certifications.

See full review →

PagerDuty

PagerDuty has a brief security page, highlighting its disclosure page, security whitepaper, compliance certifications, and short sections explaining security at PagerDuty from aspects like Payment Processing and Incident Management.

See full review →

Dropbox

Dropbox's security page emphasizes its data protection capabilities and focuses on bilateral responsibility by mentioning the best practices for users to protect their own data and accounts.

See full review →

Zoom

Zoom's security page highlights how it protects user data and privacy with measures including 256-bit Advanced Encryption Standard (AES) and optional end-to-end encryption.

See full review →

Security Page Inspirations

Figma

Figma's security page goes an extra mile on page design, which only makes sense since it is a design tool. Though the page is mainly about security at Figma, the platform also encourages users to sign up, leveraging its security features and compliance.

See full review →

Slack

Slack's security landing page catches the eye with a hero section call-to-action button that leads users to a data sheet expanding on the security and compliance at Slack.

See full review →

Atlassian

Atlassian's security page has a single CTA button in the hero section to channel concerned readers to the All Security Practices page. Then follows a section that is divided into three sub-headings with brief explanations about main security issues and how the company deals with them, such as Platform network security.

See full review →

GitHub

In general overview, GitHub's security landing page exhibits security highlights from different aspects like the Platform, Products, Features, and Customers. While the page itself doesn't give much insight into GitHub security features, there are links to related pages.

See full review →

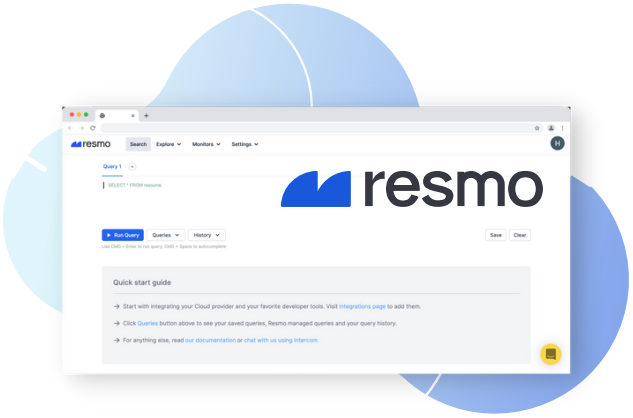
Shopify

Shopify has one of the briefest security landing pages, which adopts a serious tone and design. There are no buttons or showcase of compliance certifications, but only highlights of PCI, Privacy, SOC, and Transparency Report with a paragraph under each.

See full review →

A powerful way to observe and preserve your cloud security: Resmo

Resmo is a **continuous cyber asset visibility solution** for cloud and SaaS assets. With its seamless integration capabilities to cloud stacks, including GitHub, Slack, Jira, and AWS, you can gain deeper insights into potential security vulnerabilities from a single platform.



Here is a breakdown of *how Resmo reinforces your security posture.*

1

Set up rules to continuously assess conformance.

With Resmo, you can add custom security rules for your integrated cloud and SaaS platforms to configure their severity, remediation, and queries to be continuously evaluated.

2

Make queries and gain insights.

Select from ready-to-use queries ranging from **AWS accounts without IAM passwords policy** to **Google workspace users without a recovery email;** check all your resources' potential security risks and best practices on a single page.

3

Receive notifications on rule breach.

Resmo notifies you in real-time when there is a breach of your configured rules. This way, you will save your security team's time and work efficiently on what matters.

Get a demo

Conclusion

More and more websites, services, and products are choosing to comply with industry standards. More than likely, this will be driven by an increase in the number of data protection incidents, forcing organizations to **prove their compliance to rebuild trust with customers**.

In that respect, modern consumers and employees demand more transparency from companies they do business with, so having an informative security page helps build trust and credibility. By following these guidelines, you will be able to **sketch out your security landing page structure and present your security efforts** to customers in the most concise and effective way possible.

Contact

Securitypage.fyi by Resmo
1401 Pennsylvania Ave. Ste 105,
Wilmington, Delaware 19806, USA
www.resmo.com
contact@resmo.com