ABC's of SaaS Security

grip

SaaS adoption by enterprises of all sizes and industries is a natural corollary of their ongoing migration to the cloud. Many trends have led to an unprecedented reliance on SaaS that, paired with targeted attacks against identities and credentials, punctuates the serious threats to unguarded SaaS services.

Most business-critical operations have been surrendered to SaaS services, existing entirely outside of IT and security oversight, making traditional controls ineffective. New controls are needed to address these new realities.

Security teams are confronting these challenges by simplifying SaaS security with visibility, risk mitigation, and access control.

Learning the ABC's of SaaS Security is where it all begins.

© Grip Security, Inc. 2023. All rights reserved.

A is for Access

Access is the ability to use the functions of SaaS

SaaS is used to access and control everything in the digital enterprise, including production and security SaaS, IaaS, finance, repositories, and business-led SaaS.

B is for Business-led

By 2030, 85% of SaaS apps will be business-led SaaS

Business-led IT strategy is characterized by business groups identifying and sourcing technology, especially SaaS, outside of IT budgets, selection, support and security oversight.

C is for Classification

Classification relates to the functional components of SaaS services

SaaS security depends on classification to determine acceptable use, risk, authorization, and authentication across the enterprise SaaS layer – from factories and finance, engineering and DevOps, HR and IT – all of it runs on SaaS.

D is for Discovery

SaaS discovery is the process of identifying user-SaaS relationships

Discovery identifies user-SaaS relationships and related risks, including access and credential risks in the enterprise SaaS layer—from the first observed user-SaaS interaction to the present day.

E is for Edge

Edge computing is a distributed computing topology

Edge computing relies on information processing located close to the edge, it is a distributed schema where people produce and consume information, such as SaaS services, apps, and tenants.

F is for Federated IDM

Federated identity management (IDM) provides identity information sharing

Enterprises rely on federated identity management to transfer trust, enabling “single sign-on” for access control to managed SaaS services, while most SaaS apps remain accessible via passwords.

G is for Grants

Grants allow SaaS services to have access to user accounts

The most common form of grant authorization is via Open Authorization (OAuth), which enables a SaaS service to gain access to other SaaS services or user accounts and device information.

H is for Hashing

Hashing is the process of transforming a new value in place of the original

Hashing is a one-way encryption and vulnerable to credential attacks that expose original keys and values like usernames and passwords; hashing is the most common identity protection SaaS services use.

I is for Identity

Identity is the set of characteristics unique to a recognizable individual

Identities are the only enterprise asset security teams can control in relationship to SaaS services. Threat actors know this and continue to attack identities with phishing, vishing, and smishing schemes.

J is for Justification

Justification is a designated status and process to approve SaaS use

Organizations rely on justification processes and approval workflows to review and authorize use of SaaS services for identities or users.

K is for Kit

A kit is a distributed software or instrument for malicious purposes

The most common malicious kits are intended for phishing attacks against identities and credentials, allowing cybercriminals to scale attacks with purpose-built tools.

L is for Login

Login is the procedure to get access to SaaS

Cybercriminals target identities to gain access to SaaS services via simple login from stolen credentials. By accessing the enterprise SaaS layer, threat actors can control SaaS-delivered functions and operations.

M is for Multi-faceted

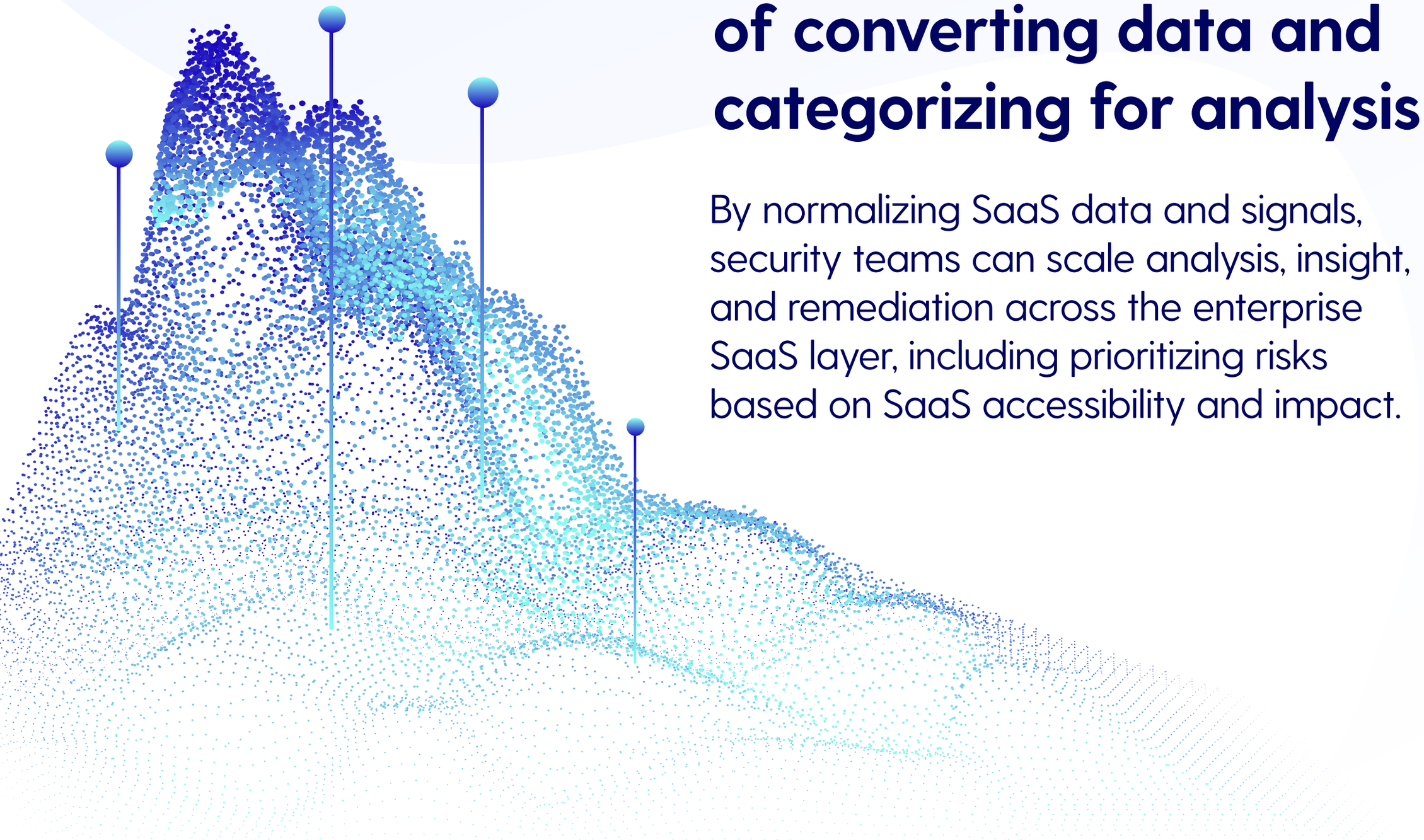
SaaS is multi-faceted with many functions, components, and capabilities

The enterprise SaaS layer is diverse, multi-faceted, and remains the largest shadow threat with an outsized impact — because organizations use SaaS to control and operate everything else.

N is for Normalization

Normalization is the process of converting data and categorizing for analysis

By normalizing SaaS data and signals, security teams can scale analysis, insight, and remediation across the enterprise SaaS layer, including prioritizing risks based on SaaS accessibility and impact.



O is for Offboarding

Offboarding revokes access to SaaS services or decommissions SaaS services for targeted users

On-demand, secure SaaS offboarding removes attacker opportunity to target and exploit credentials and identities; credentials are the top threat target and secure offboarding protects against unauthorized access to SaaS services.

P is for Password

A string of characters, letters, numbers, and symbols to authenticate users to SaaS

Username and password is the most common form of authentication to SaaS services. Over 70% of passwords are duplicates and with the average user having 109 duplicate credentials, identities remain the top attacker target.

Q is for Questionnaire

A sequence of questions to be used when assessing SaaS and other third parties

Questionnaires help enterprises simplify security assessments for third party services, including SaaS, by requesting information to determine business justification and shared risk with the SaaS provider.

R is for Risk

SaaS risk indexing (SRI) enumerates SaaS risk based on accessibility and impact

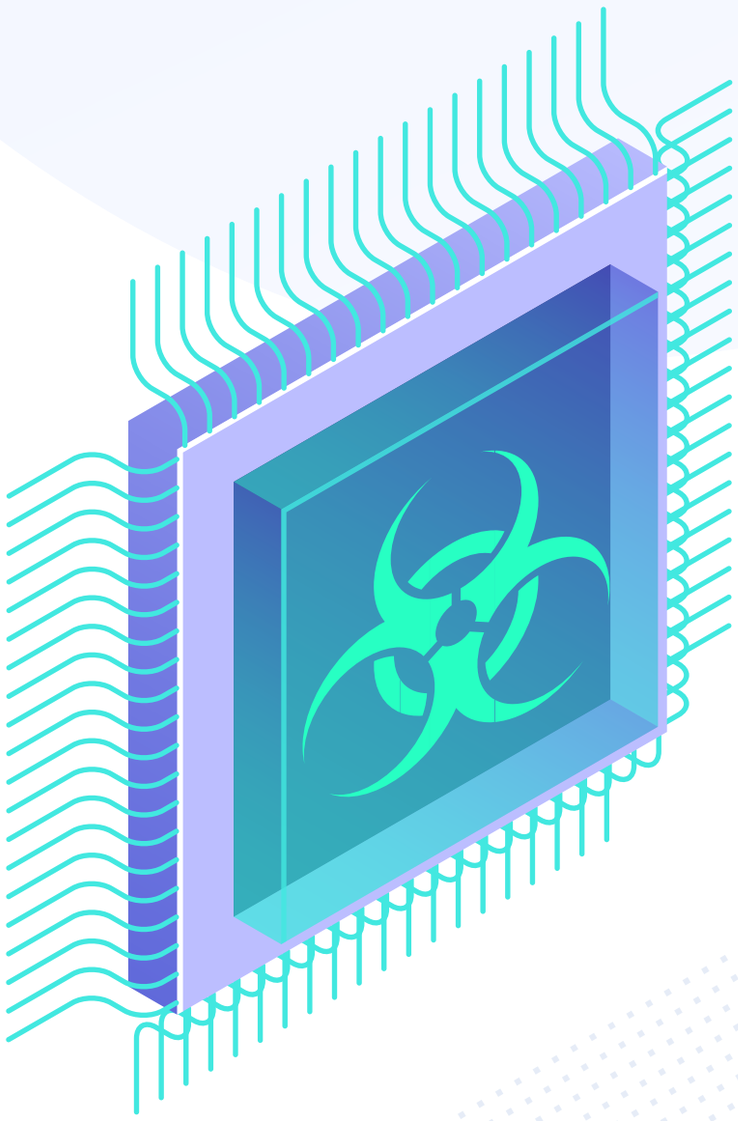
Organizations have unique SaaS service layers, each must be mapped and indexed for risk based on accessibility and functional capabilities to control business and technology operations via SaaS services.

S is for SSCP

SaaS Security Control Plane (SSCP) is an identity-based architectural element for discovering and securing SaaS access

SSCP discovers user-SaaS relationships, risky access, credential exposures, rogue or abandoned SaaS throughout the enterprise SaaS layer. SSCP is characterized by its three distinct capabilities: 1) SaaS discovery, 2) SaaS risk indexing, and 3) SaaS security orchestration and enforcement.

T is for Threat



A scenario, event, or actor capable of adverse impact via unauthorized access to SaaS

Given the unmatched control of SaaS services, access to the enterprise SaaS layer remains the greatest threat – because once an adversary gains access to SaaS, the threat actor is at the controls of the digital enterprise.

U is for Unsanctioned

SaaS services and applications not officially approved are considered unsanctioned

Most SaaS services are unguarded and unsanctioned – including SaaS used for critical functions, security control, DevOps, repositories, business operations, and production systems.

V is for Visibility

SaaS visibility is the result of discovery and graphing user-SaaS relationships

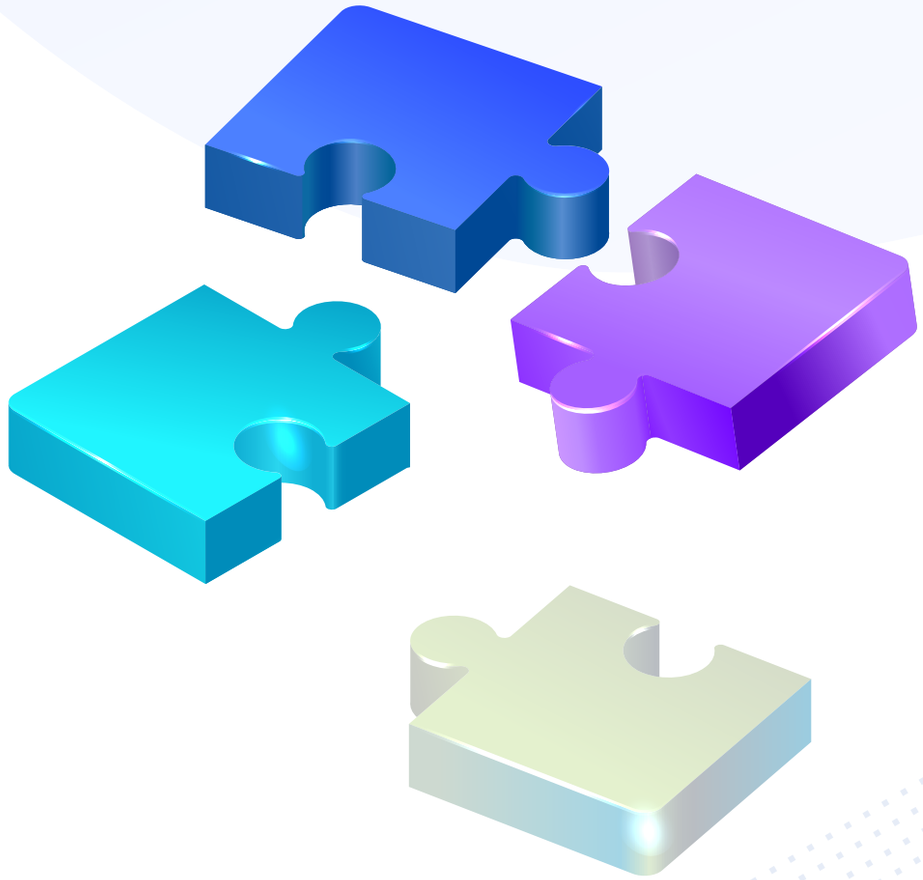
Visibility across the enterprise SaaS layer includes better awareness of SaaS services, users, groups, tenants, and real-world usage, such as authentication methods and control gaps like missing SSO, policy dodging, dangling access, and zombie accounts.

W is for Web Browser

A web browser is a software program for accessing web pages, including SaaS services

Over 90% of SaaS usage occurs within a web browser, whether the user is authenticated with single sign-on (SSO) or username and password. Most identity-based attacks happen within a web browser environment – enticing users to malicious sites posing as legitimate SaaS services.

X is for eXtensions



Extensions are small software modules for customizing a web browser

Often, browser extensions are granted access to sensitive data. Security teams should only grant access for the minimum amount of data an extension needs, creating less exposure if an extension is compromised.

Y is for Yottabyte

A yottabyte is the largest unit of measure for data storage capacity

By 2030, SaaS services are expected to contain at least 1 yottabyte of data. In decimal format, a yottabyte is written as 1,208,925,819,614,629,174,706,176 bytes (or a million trillion megabytes).

Z is for Zombie Account

Zombie accounts occur when users retain unnecessary access to SaaS services

Zombie accounts often result when human users who are authenticated through username and password or SSO leave the organization or change roles. Old credentials, when left unmanaged, are a prime target for attackers.

How Grip Security can help

Security is hard. SaaS security is even harder. Security teams and leaders want to keep pace with the growth of SaaS services that run our digital organizations. But it is hard.

SaaS security is unique because of the velocity of new SaaS being adopted, the decentralized purchasing decision process paired with ever-broadening scope for SaaS to operate business functions and technologies.

Grip created the world's first SaaS Security Control Plane (SSCP). Grip SSCP is an identity-based architectural element for discovering SaaS services and user-SaaS relationships, identifying risky access and malicious or abandoned SaaS services, credential exposures and accumulated risk throughout the SaaS estate – relevant and actionable, tuned to what matters.

Grip SSCP enables organizations to consistently protect their cloud-first reality, characterized by its three distinct capabilities: 1) SaaS discovery, 2) SaaS risk indexing, and 3) SaaS security orchestration and enforcement.

Each of these capabilities align with top concerns of security leaders: visibility, risk, and access control.

Get started with a 10-minute deployment to secure the enterprise SaaS layer.

grip

Grip Security, Inc.
50 Milk Street
Boston, MA 02110

sales@grip.security
@GripSecurity
grip.security

© Grip Security, Inc. 2023. All rights reserved.