Identity Security that Stops Breaches

Continuously Managing Permissions and Identity Risks

The Identity Security Challenge:
Maintaining a Secure and Compliant Posture

Security practitioners face a constantly changing and expanding attack surface – digital identity. This expansion extends beyond traditional employee identities to include third parties, contractors, machine identities, and APIs, all introducing new challenges in maintaining a secure and compliant posture. Additionally, the challenge is often compounded by the absence of effective access management systems that can quickly and accurately handle the provisioning and deprovisioning of access permissions.

75% of cloud security failurs by 2023 will result from inadequate management of identities, accesses, and priveleges.

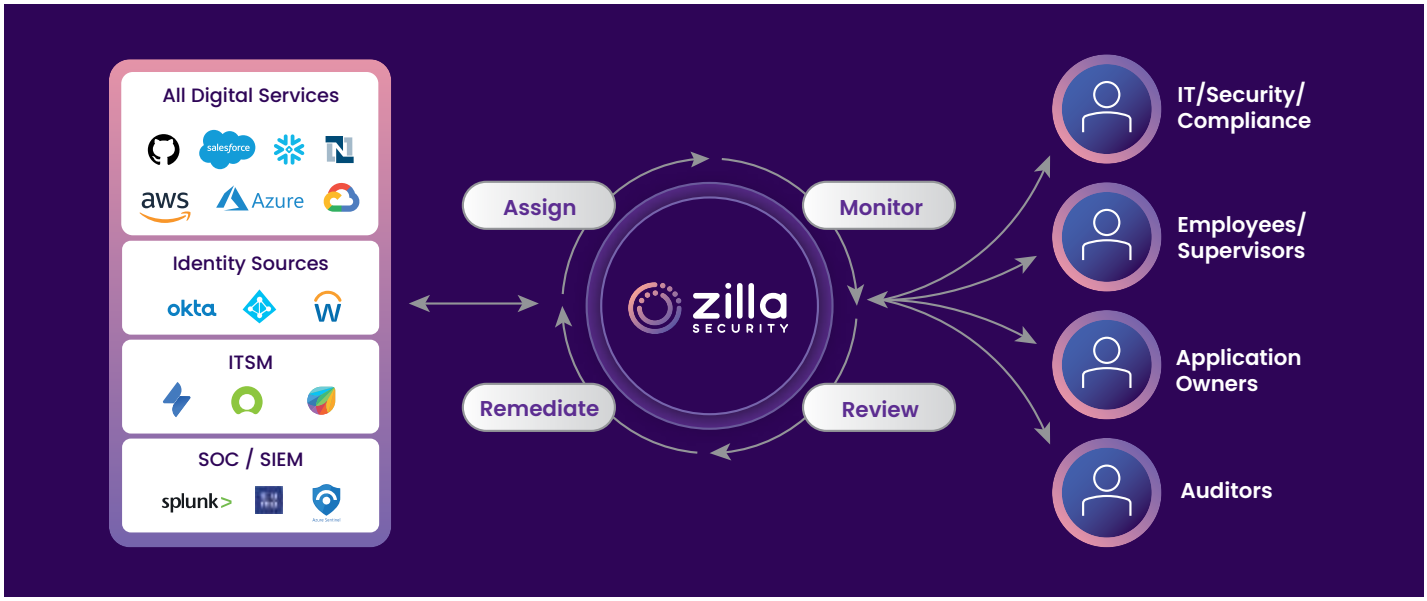
GARTNER 2021, MANAGING PRIVELEGED ACCESS IN CLOUD INFRASTRUCTURE

A deep analysis reveals that an alarming majority of modern breaches are predominantly driven by excessive permissions and misconfigured access settings.

Critical questions surface: Do third parties have privileged access to AWS? Are permissions being granted without proper approvals? Is sensitive HR data left publicly accessible? Issues such as rogue service accounts in HR systems like Workday, developers' access to customer data, and privileged accounts not protected with multi-factor authentication (MFA) are pressing. Additionally, there is the risk of terminated employees retaining access to sensitive financial applications like Snowflake, Oracle NetSuite, and Salesforce.

The Zilla Identity Platform:
The Intelligent Control Center

The Zilla Identity Security Platform assigns, monitors, and remediates user permissions across your organization's digital landscape - cloud, SaaS, and on-premise applications and services. It provides a centralized and comprehensive view of who has access to what, and enables near-time insights and actions.



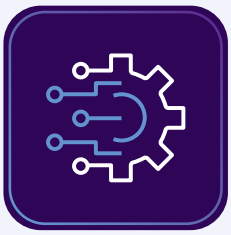
Zilla Secure reduces potential internal and external threats by ensuring least-privilege access. It uses automated security policies to identify, remediate, and prevent identity and access risks by continuously monitoring your SaaS and cloud configurations.

Zilla Comply streamlines the user access review process by automating tedious manual tasks. It enforces Segregation of Duties by identifying and flagging toxic rights combinations and simplifies audit preparation with complete and accurate compliance evidence.

Zilla Provisioning makes access rights management easy, fast, and secure, ensuring that user permissions are assigned correctly and revoked as needed through an automated, auditable process. It delivers system-verified access provisioning and allows organizations to leverage existing ITSM investments.

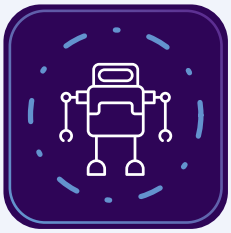
Why Choose Zilla Security?

Comprehensive coverage across all cloud, SaaS, and on-prem apps



More integrations than anyone else in the industry

Fastest time to value and rapid deployment measured in weeks



Unmatched automation that reduces manual efforts up to 75%

Simple and intuitive user experience for novices and experts alike

What Our Customers Say

> With Zilla's help, over 90% of our access review tasks became automated.
>
> TaL Hornstein,
> CISO, Hippo Insurance Services

> Zilla is not just a tool but a partner in our growth. Their forward-thinking approach ensures we are prepared for the challenges of tomorrow while addressing the needs of today.
>
> Christopher Callahan
> CISO, Weichert Companies

About Zilla Security

Zilla Security is an identity security platform that combines identity governance and cloud security. Our SaaS platform is the only service that delivers no-code integration across all environments, SaaS and home-grown applications, cloud platforms, and on-premises systems to automate access security and compliance and deliver a comprehensive system of record for user, machine, and API identities.

To learn more, visit zillasecurity.com.