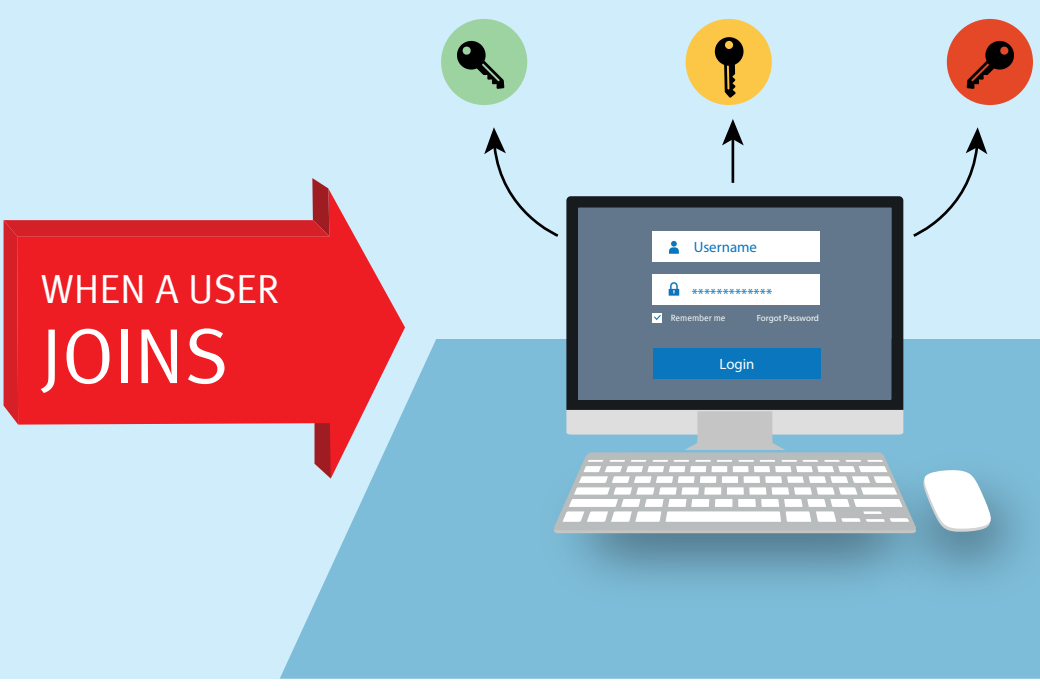
Without RSA: Security Chaos

RSA

Vulnerabilities in the Identity Lifecycle



Users created with excessive privileges, leading to an expanded attack surface.

People are initially created in IT systems, and granted access.

Risks not aligned with overall corporate risk guidelines (GRC).

No visibility or control of dormant accounts, leading to security and compliance risk.

People actively use IT systems to perform their jobs.

Users access rights grow over time, and are never analyzed or revoked.

Users obtain access through "tribal knowledge" or informal processes – without InfoSec or management oversight, resulting in security policy violations.

People's access needs change. This is most commonly a need to obtain new access to perform new duties.

Access changes are not validated – allowing malicious attackers to perform privilege escalation undetected.

Users often retain access to SaaS systems, opening the door to a data breach.

People no longer need access. Most commonly, this is due to an employee leaving the company. But it also applies to other user populations (contract employees, partners, suppliers, and even customers) whose access must be turned off.

No ability to reliably or quickly detect when user access should be deactivated – so user accounts are left active indefinitely.

With RSA: Identity Sanity

RSA

Close security gaps and vulnerabilities with RSA Governance and Lifecycle. Users only have access to what they need, when they need it.

WHEN A USER
JOINS

Reduced attack surface area.

Third-party access is created efficiently and correctly, with appropriate levels of access.

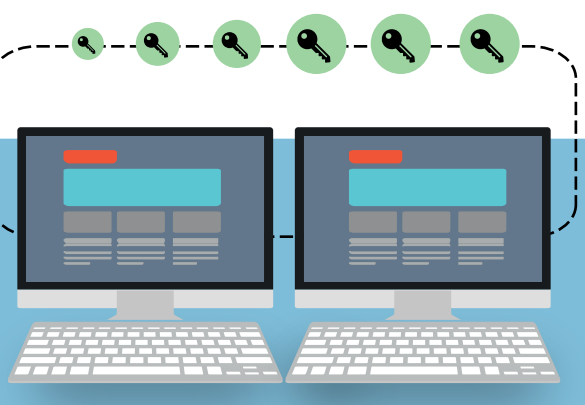
Enforces “principle of least privilege”.

Provisioned access with username and password

WHEN A USER
USES

Stale accounts are prevented (and remediated), improving compliance and security.

Regular access reviews ensure that user access (especially privileged accounts) meet security policies.



WHEN A USER
MOVES

Automated change validation ensures that all user access changes are accounted for.

Centralized and streamlined portal for users to request access, and automated workflow for easy management review.

WHEN A USER
LEAVES

Intelligently manages deactivation of accounts, so as not to impede business productivity.

Disables both on-premise and SaaS accounts.

Key feature:
Unauthorized change detection

Immediately highlight any unauthorized changes and stop malicious privilege escalation.

USER A

Access request

Pending change queue

Access approved

MALICIOUS USER

Privilege escalation

ACCESS CHANGE NOT IN QUEUE? DENIED!