Enterprise Strategy Group™
by TechTarget

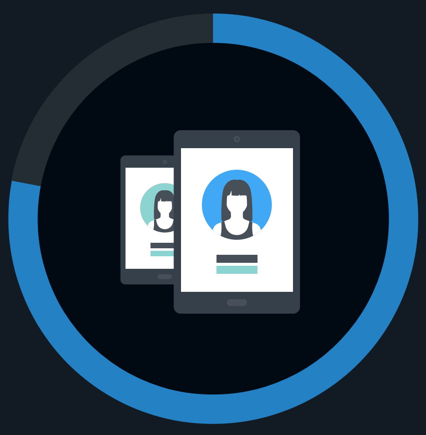
The State of Identity Security

Organizations continue to rely on identities that are susceptible to compromise, abuse, misuse, and theft. Risk is compounded by over-permissive, static access rights that provide little to no visibility into access trends or, most importantly, who is accessing what and how they are doing so. Unfortunately, organizations have been slow to pivot their security programs to an approach that incorporates identities as a foundational aspect of their cybersecurity strategy. TechTarget's Enterprise Strategy Group recently surveyed IT, cybersecurity, and application development professionals responsible for or involved with identity security technologies and processes to gain insights into these trends.

Notable findings from this study include:

82%

of organizations have **faced multiple employee account or credential compromises over the past 12 months.**



78%

of organizations that have had accounts or credentials compromised in the last 12 months report that this led to at least one cybersecurity attack.

66%

of organizations have implemented mandatory passwordless authentication across their workforces.

82%

of organizations believe that on-premises and cloud-resident infrastructures require a different set of identity security policies and technologies.

72%

of organizations report that deployment of identity security tools has taken much longer and/or has been more complex than originally planned.

86%

of organizations are **increasing spending on identity security to reduce the risk of access and permissions vulnerabilities.**

For more from this Enterprise Strategy Group study, read the full research report, ***The State of Identity Security: Opening Doors to the Right Entities and Locking Bad Actors Out.***

LEARN MORE

Source: Enterprise Strategy Group Research Report, *The State of Identity Security: Opening Doors to the Right Entities and Locking Bad Actors Out*, July 2024.