Enterprise Strategy Group™ by TechTarget

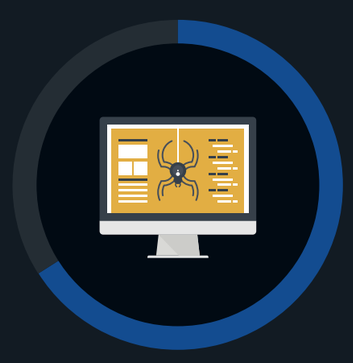
Managing Non-human Identities for an Effective Cybersecurity Program

Modern application architectures with complex relationships and ephemeral resources have resulted in a proliferation of non-human access to communicate and exchange data. Enterprise IT cybersecurity and operations teams are recognizing the risk associated with the large and growing volume of non-human identities. As cloud adoption and automation continue to grow, effective non-human identity management has become essential for maintaining security, facilitating business operations, and supporting digital transformation initiatives. TechTarget's Enterprise Strategy Group recently surveyed IT, cybersecurity, and DevOps, platform, and cybersecurity engineering professionals to gain insights into these trends.

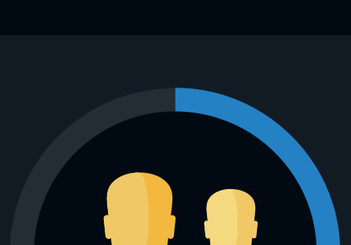
Notable findings from this study include:

For every human identity, organizations estimate there are **20X NON-HUMAN IDENTITIES.**

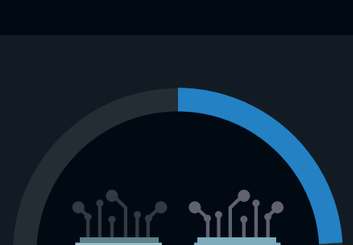
72%
of organizations either know or suspect that they have had non-human identities compromised in the past 12 months.



66%
of organizations have endured at least one successful cyberattack resulting from compromised non-human identities in the last 12 months.



57%
of organizations that suffered a successful attack tied to a compromised non-human identity indicated the event got board-level attention.



Organizations expect
24% GROWTH
in the volume of non-human identities in the next 12 months.

83%
of organizations say they expect to **spend relatively more on non-human identity security over the next 12 months.**

For more from this Enterprise Strategy Group study, read the full research report, ***Managing Non-human Identities for an Effective Cybersecurity Program.***

LEARN MORE

Source: Enterprise Strategy Group Research Report, *Managing Non-human Identities for an Effective Cybersecurity Program,* December 2024.