Enterprise Strategy Group™ by TechTarget

Securing SaaS Ecosystems

Organizations have shifted from using a few discrete cloud applications to supporting an entire ecosystem around SaaS. Because these applications often house sensitive data, it is critical that security teams ensure they are properly configured, malware and compromised users are detected, and data is protected, all while controlling access from a range of both internal and third-party users. TechTarget's Enterprise Strategy Group recently surveyed IT and cybersecurity professionals involved with securing their organization's SaaS applications to gain insights into these trends.

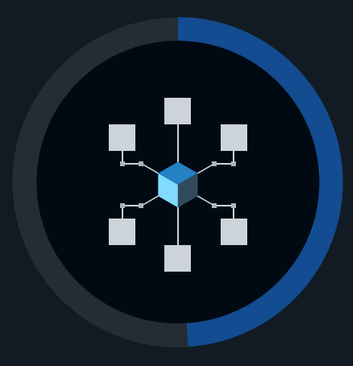
Notable findings from this study include:

73%

of organizations say ensuring the **safe usage of SaaS applications is a top three cybersecurity priority.**

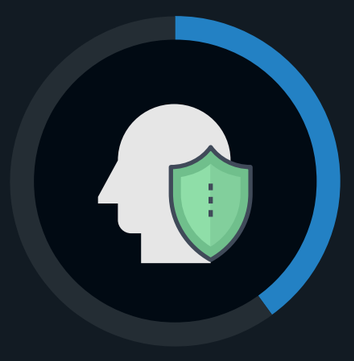
64%

of organizations say improving the speed of SaaS application misconfiguration discovery and remediation is important.



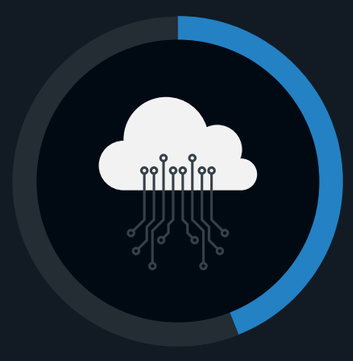
49%

of organizations say they would consider an enterprise browser for securing third-party or unmanaged device access to SaaS applications.



40%

of organizations say they would prefer to consume SaaS security as part of a cloud access security broker or SSE solution.



44%

of organizations say they would prefer to consume SaaS security from a unified, dedicated SaaS security platform.

98%

of organizations say the use of **unsanctioned SaaS applications is a challenge.**

For more from this Enterprise Strategy Group study, read the full research report, ***Securing SaaS Ecosystems.***

LEARN MORE

Source: Enterprise Strategy Group Research Report, *Securing SaaS Ecosystems,* September 2024.