


# CHALLENGES IN SECURING AN OVERABUNDANCE OF COMMUNICATION AND COLLABORATION TOOLS



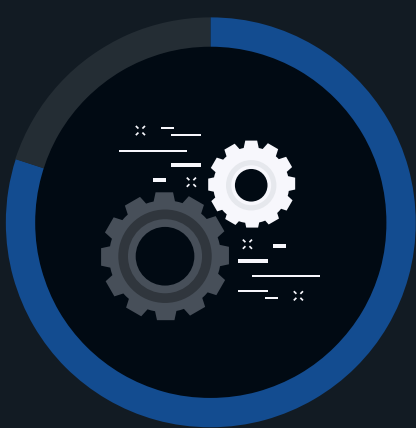
As more workers collaborate virtually, many organizations now depend on additional digital communication tools beyond email. Unfortunately, these new collaboration tools provide attackers the opportunity to engage with humans and evade automated cybersecurity controls. TechTarget's Enterprise Strategy Group recently surveyed IT and cybersecurity professionals involved with securing enterprise communication and collaboration technology and processes to gain insights into these trends.

Notable findings from this study include:



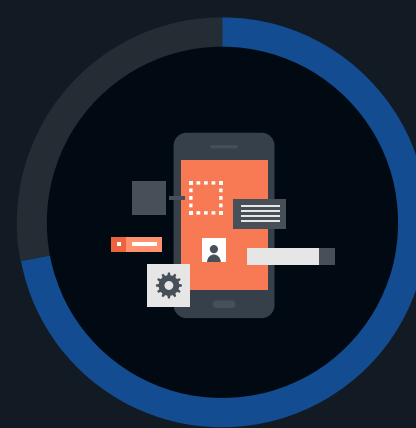
**38%**

of organizations believe that email is the communication and collaboration tool that is **most vulnerable** to threat actors.



**80%**

of organizations expect to add third-party controls to address gaps in native email security capabilities.



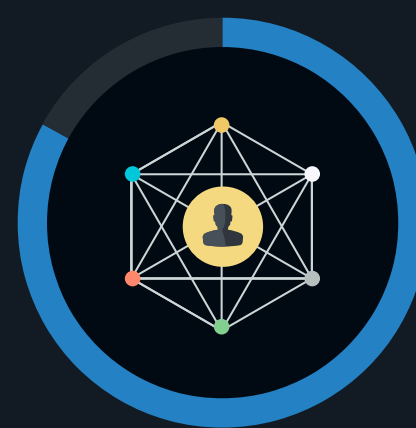
**72%**

of organizations report frequent socially engineered attacks involving multiple electronic communication channels.



**41%**

of cybersecurity teams have **limited or no involvement** in securing communication and collaboration tools.



**83%**

of organizations say securing their communication and collaboration channels is a top priority.



**67%**

of organizations are concerned that attacks leveraging communication and collaboration tools (other than email) to **evade security controls** are threatening their environment.

For more from this Enterprise Strategy Group study, read the full research report, *Challenges in Securing an Overabundance of Communication and Collaboration Tools*.

[LEARN MORE](#)