SECURITY HYGIENE AND POSTURE MANAGEMENT
## REMAINS DECENTRALIZED AND COMPLEX

Security hygiene and posture management has become increasingly difficult because of factors like a growing attack surface, the increased use of cloud computing, and the need to support a remote workforce. These factors can create security vulnerabilities that lead directly to cyber-attacks. Unfortunately, this pattern will likely persist as most organizations continue to approach security hygiene and posture management with point tools, spreadsheets, and manual processes. TechTarget's Enterprise Strategy Group recently surveyed IT and cybersecurity professionals to gain insights into these trends.

Notable findings from this study include:

73%
of organizations report that spreadsheets **remain a key aspect of their security hygiene and posture management strategy.**
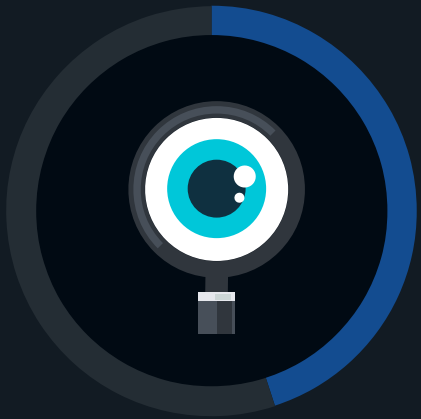
45%
of organizations perform attack surface discovery to reduce the risk of a ransomware attack.
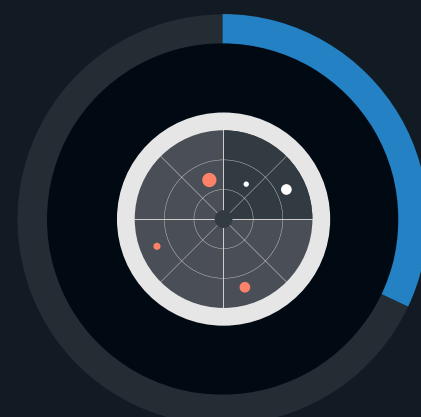
76%
of organizations have experienced a cyber-attack due to the exploit of an unknown, unmanaged, or poorly managed internet-facing asset.

48%
of organizations need more than 80 hours to discover all assets on their external attack surface.

32%
of organizations use at least 11 data sources to discover, track, and inventory IT assets for security hygiene and posture management.

45%
of organizations use penetration testing and/or red teaming reports to reassess security and IT processes and cyber-risk.

49%
of organizations believe that performing continuous security controls validation testing would most improve their security hygiene and posture management.

For more from this Enterprise Strategy Group study, read the full research report, *Security Hygiene and Posture Management Remains Decentralized and Complex.*

LEARN MORE