



# INSIDE THE MIND OF MODERN ADVERSARIES

SANS, in partnership with Bishop Fox, surveyed 280 ethical hackers to gain insight into the mind and methods of modern adversaries – including what works and what doesn't. For more insights into our hacker analysis, [tune into our webcast!](#)

# TIME TO BREAK INTO AN ENVIRONMENT



**57%** of hackers say it takes less than 5 hours to break into an exposed environment.



n = 247

# TIME TO COMPLETE AN END-TO-END ATTACK

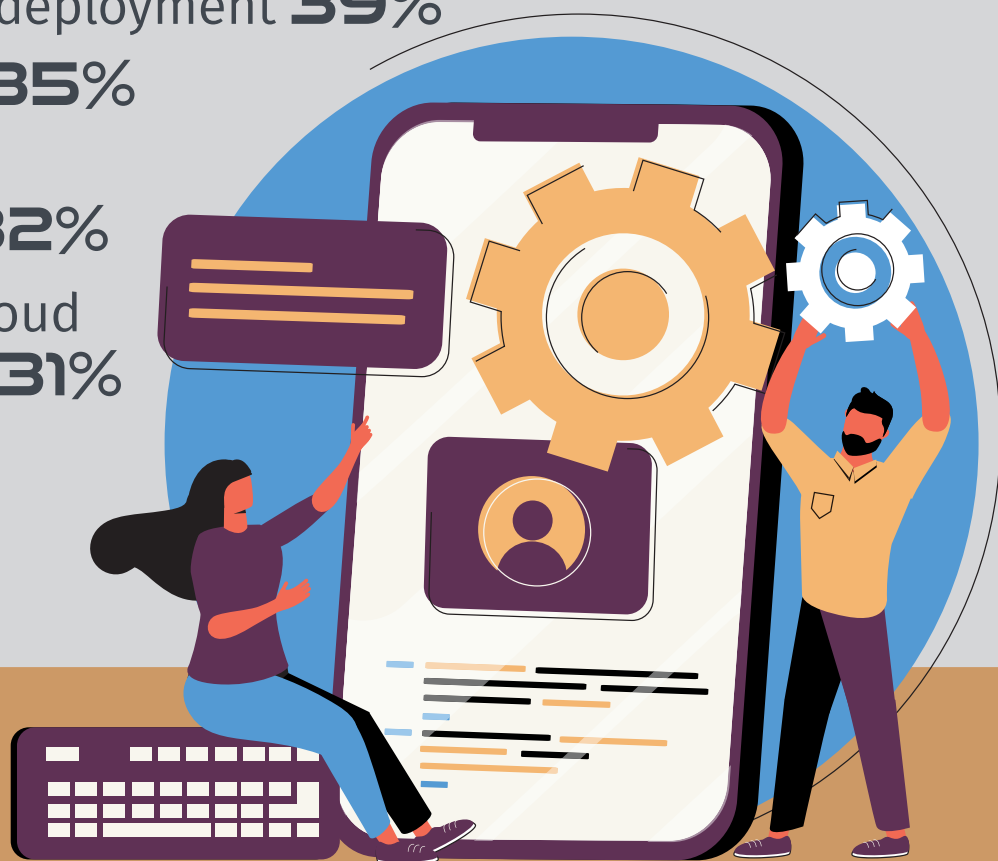
**44%** of hackers can complete an end-to-end attack in 20 hours or less (breach perimeter, gain access to targets, and potentially exfiltrate data).



# TOP FACTORS THAT LEAVE COMPANIES VULNERABLE

Top five factors making attack surfaces vulnerable to compromise:

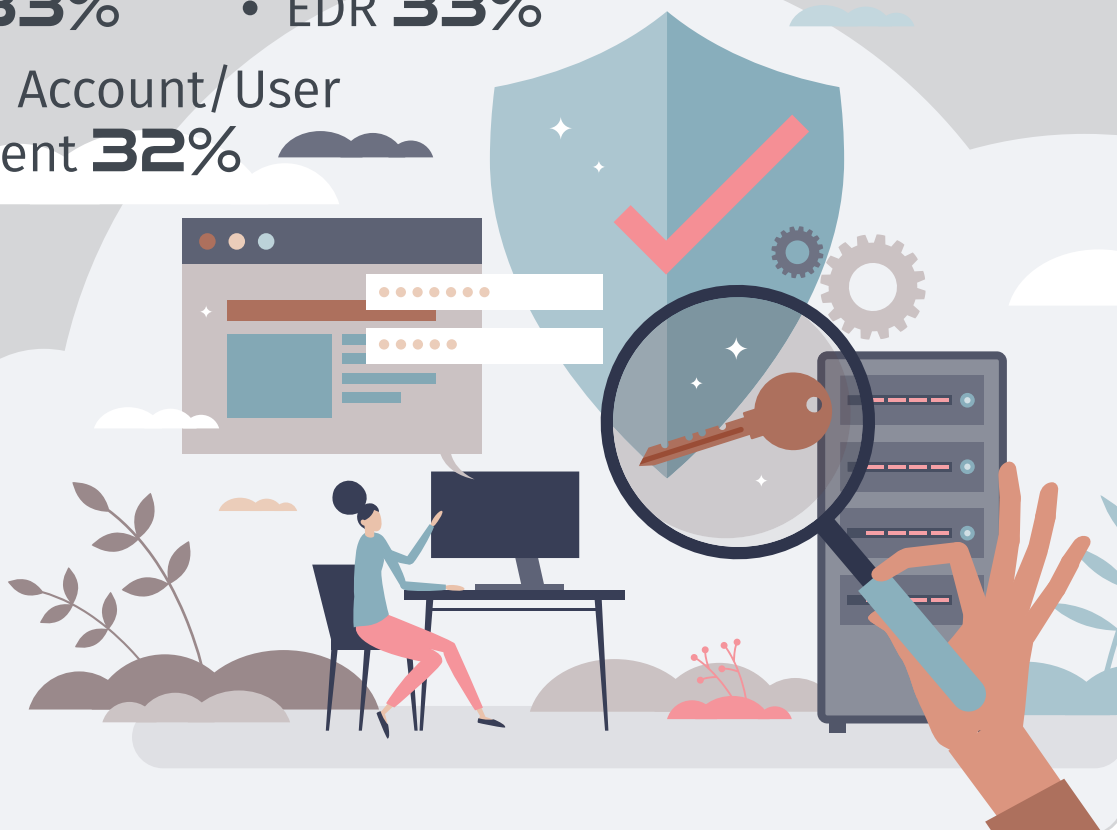
- Third-party connections **40%**
- Increased pace of application development/deployment **39%**
- Remote work **35%**
- Mergers and acquisitions **32%**
- Adoption of cloud infrastructure **31%**



# CHALLENGES TO PENETRATE AN ENVIRONMENT

Leading challenges hackers face when penetrating an environment:

- MFA **48%**
- Patching **42%**
- Firewall **33%**
- EDR **33%**
- Privileged Account/User Management **32%**



# GREATEST ROI FOR HACKERS

Top three attack vectors that offer hackers the greatest return on investment (ROI) include:

- Social engineering **32%**
- Phishing **17%**
- Web application attacks **9%**

