DataGames

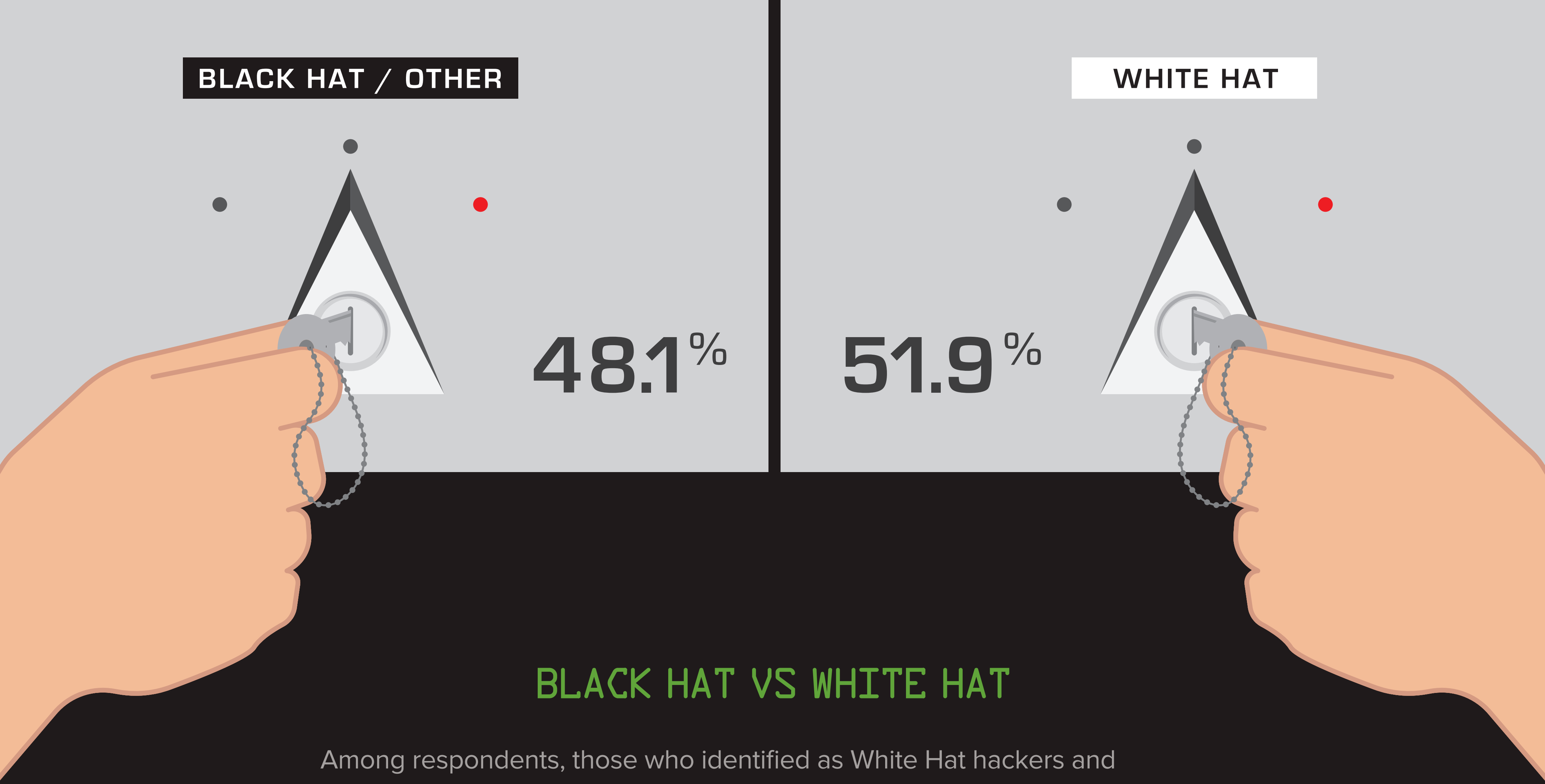
bitglass

Security Blind Spots According to Experts

The advent of cloud and mobile data access has created new arenas in which competing parties battle to exploit and close security gaps. The two feuding groups are Black Hat and White Hat hackers. White Hat hackers use their skills for ethical purposes, while Black Hat hackers pursue their own nefarious ends.

As technologies evolve, enterprises are faced with new challenges around securing data while enabling employee productivity. As such, tapping into the insights of the experts, those deeply familiar with the security landscape, can prove invaluable.

In a survey of over 100 Black Hat 2017 attendees, Bitglass uncovered the infosec community's perceptions of security gaps and enterprise readiness.



BLACK HAT VS WHITE HAT

Among respondents, those who identified as White Hat hackers and those who did not were evenly split. Respondents self-categorized into two groups, White Hat and Black Hat / Other. An average of 80.6% of respondents had some experience working in corporate IT—this includes individuals who self-identify as White Hat, Black Hat, or “Other”.

80.6% of survey respondents worked in corporate IT in the past

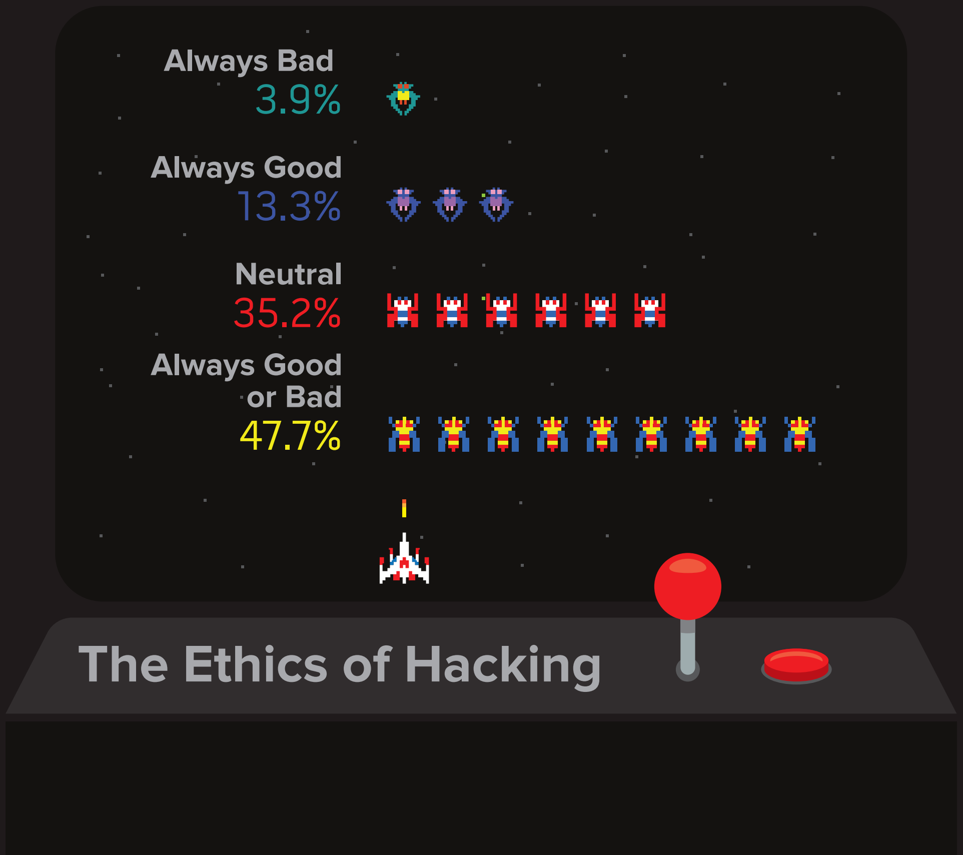
WHY THEY PLAY THE GAME

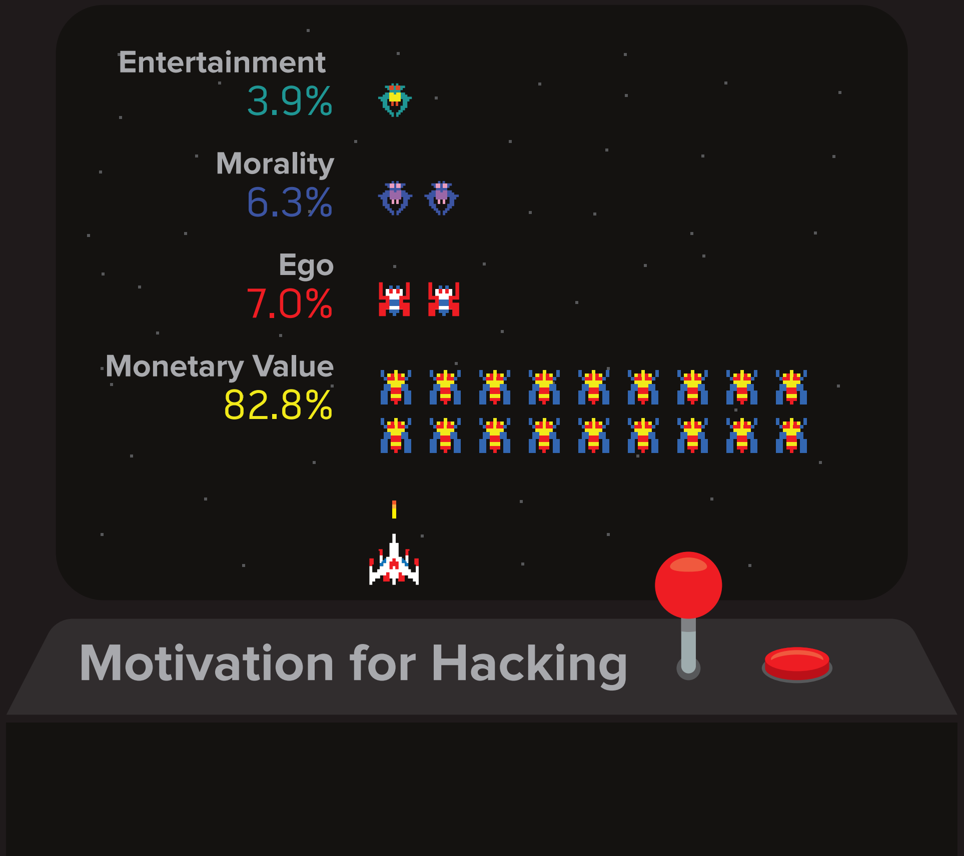
When asked about the moral implications of hacking, experts' responses were largely polarized. More than half (64.8%) of those surveyed believe hacking is always good or always bad. Only 35.2% believe hacking to be inherently neutral.

17.1% of experts believe there is no moral ambiguity in hacking

Whether it's through ransomware or selling credentials and files to malicious parties, stealing data can be very lucrative. This is evidenced by the reality that some White Hat hackers leave their IT jobs to become Black Hat hackers.

For the vast majority (**82.8%**), monetary gain is the primary motivation behind hacking





HOLES IN THE MISSILE DEFENSE

According to the experts, password-protected documents are the least effective security tool (33.3%). At 19.4%, face recognition was rated as the worst tool six times more often than fingerprint authentication—an interesting insight in light of the iPhone X's shift to face-recognition security. In all, the perceived inadequacy of these tools suggests that additional, advanced capabilities like user and entity behavior analytics (UEBA) must also be used.

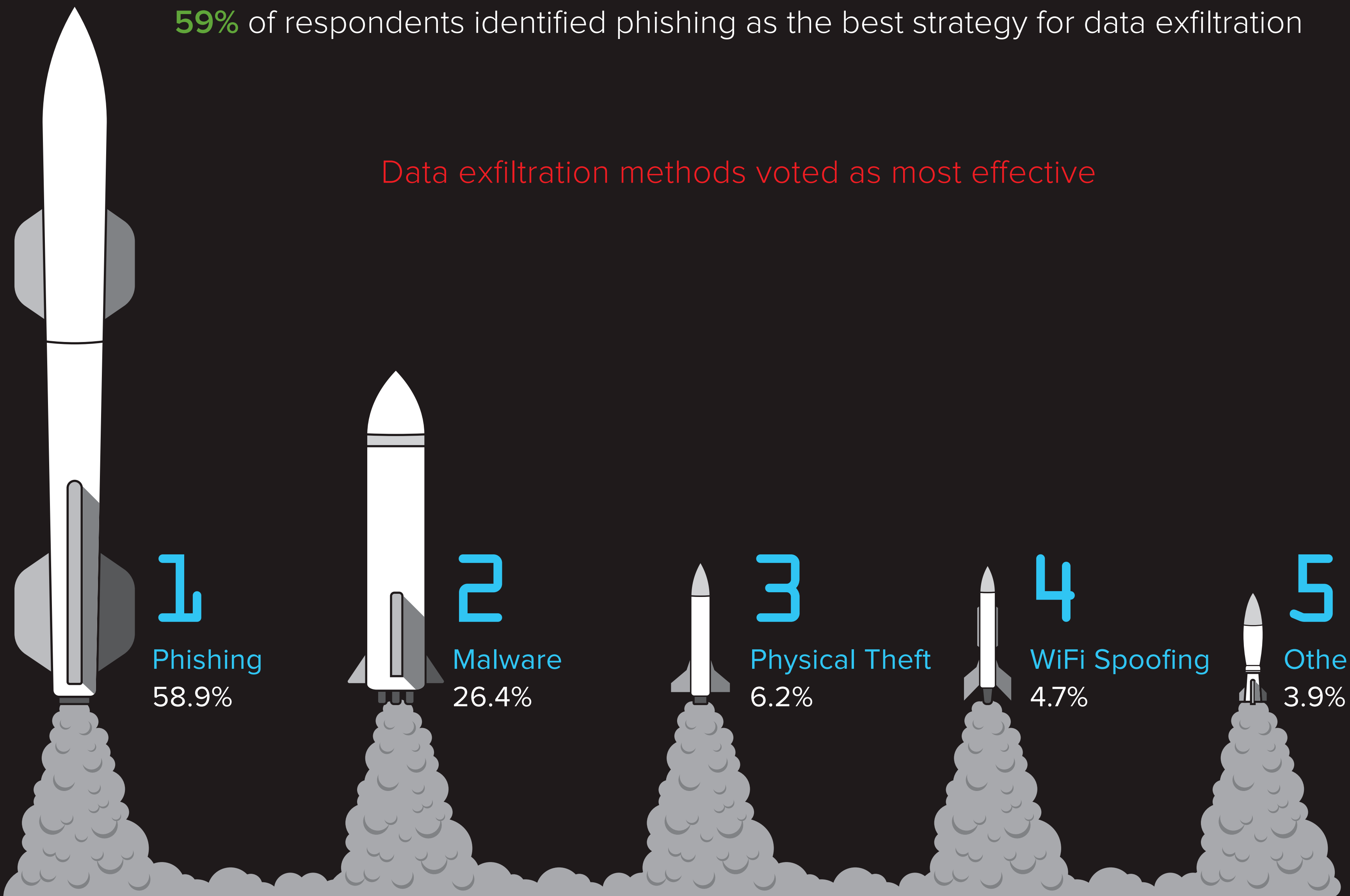
Security tools voted as least secure

1	Password-Protected Documents	33.3%
2	Face Recognition	19.4%
3	Access Controls	15.5%
4	MDM	11.6%
5	Network Firewalls	11.6%
6	Other	5.4%
7	Fingerprint Authentication	3.1%

THE TOOLS OF WAR

Both groups ranked data exfiltration methods in the same order. 59% of respondents identified phishing as the best strategy—human error and ignorance will always be exploitable. Understandably in light of recent attacks, malware and ransomware ranked second at nearly 27%. Security solutions must defend against malware through advanced threat protection (ATP) and prevent data theft and human error through data leakage prevention (DLP).

59% of respondents identified phishing as the best strategy for data exfiltration



Data exfiltration methods voted as most effective

Largest Data Blind Spots

61.2%
Unmanaged Devices

55%
Not-up-to-Date Systems

36.4%
Mobile Devices

26.4%
Data at Rest in the Cloud

20.9%
On-Premises Security

1.6%
Other

FLANKING THE ENEMY

In this choose-all-that-apply question, over 60% of experts identified unmanaged devices as a critical security blind spot. The second largest blind spot was systems, applications, and programs that aren't up to date and leave vulnerabilities unpatched (55%). At 36.4%, mobile devices were seen as a security blind spot the third most often. Together, these vulnerabilities demonstrate the need for tools, like cloud access security brokers, that maintain comprehensive, real-time visibility and control over data.

WRAP UP

According to the experts surveyed by Bitglass, organizations' largest blind spots are currently unmanaged devices and not-up-to-date systems. Phishing is seen as the most effective way to steal data, and password-protected documents as the least effective security tools. The fact that White Hat and Black Hat hackers agree indicates the legitimacy of these security issues.

As the war of White Hat versus Black Hat continues, new vulnerabilities will inevitably emerge. As such, organizations must adopt real-time security solutions with comprehensive data protection across all devices and applications. Security must protect in the present but be built for the future.

bitglass

Phone: (408) 337-0190
Email: info@bitglass.com

www.bitglass.com

ABOUT BITGLASS

Bitglass, the total data protection company, is a global CASB and agentless mobile security company based in Silicon Valley. The company's solutions enable real-time end-to-end data protection, from the cloud to the device. Bitglass is backed by Tier 1 investors and was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution.