



THREATS BELOW THE SURFACE



A NEWFOUND URGENCY
IN CLOUD SECURITY

 bitglass



Since 2014, cybersecurity has come to the forefront of news, culture, technology, and business. Cloud security, given widespread adoption in the last several years, is critical for every organization and requires a new, more comprehensive approach to data protection.

Threats to corporate data are evolving more quickly than most enterprises can adapt and large scale breaches are becoming more frequent.

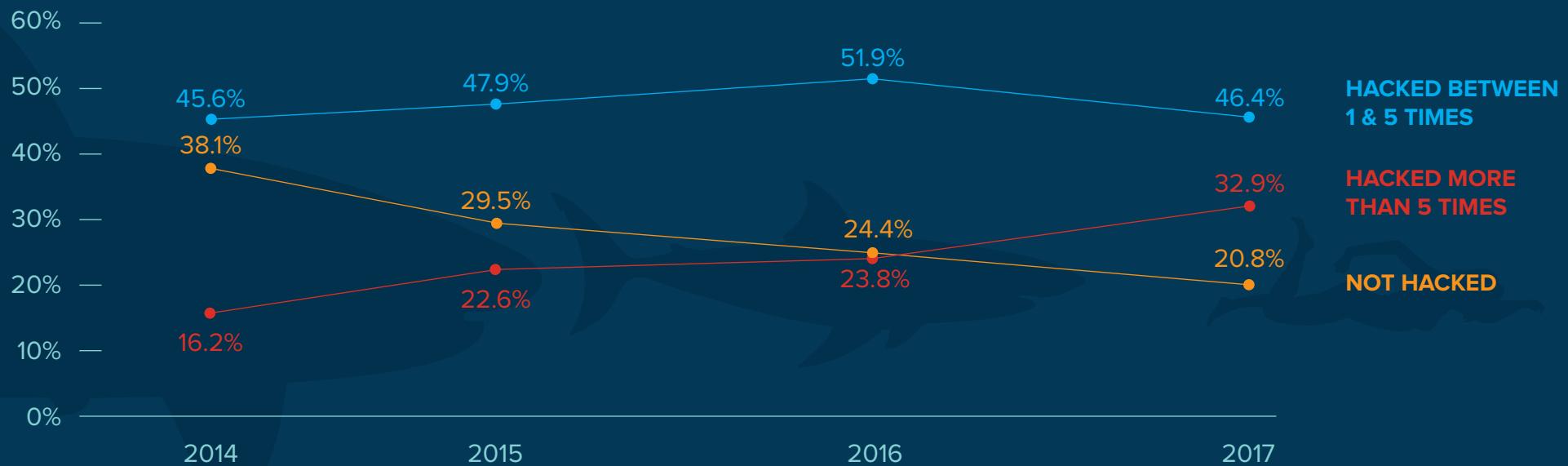
In the last year alone, **87%** of organizations were victims of a cyber attack, and **1/3** were hacked more than 5 times.

In partnership with the CyberEdge Group and Information Security Community, we surveyed over 3,000 IT professionals on risks, priorities, and capabilities that are top of mind for enterprises to understand the state of cloud security.

UNDERESTIMATING THREATS

In our [year-ago survey](#), a majority of organizations claimed to not have suffered a breach in the past 12 months. Lulled into a false sense of security, many enterprises have been complacent in their move to the cloud.

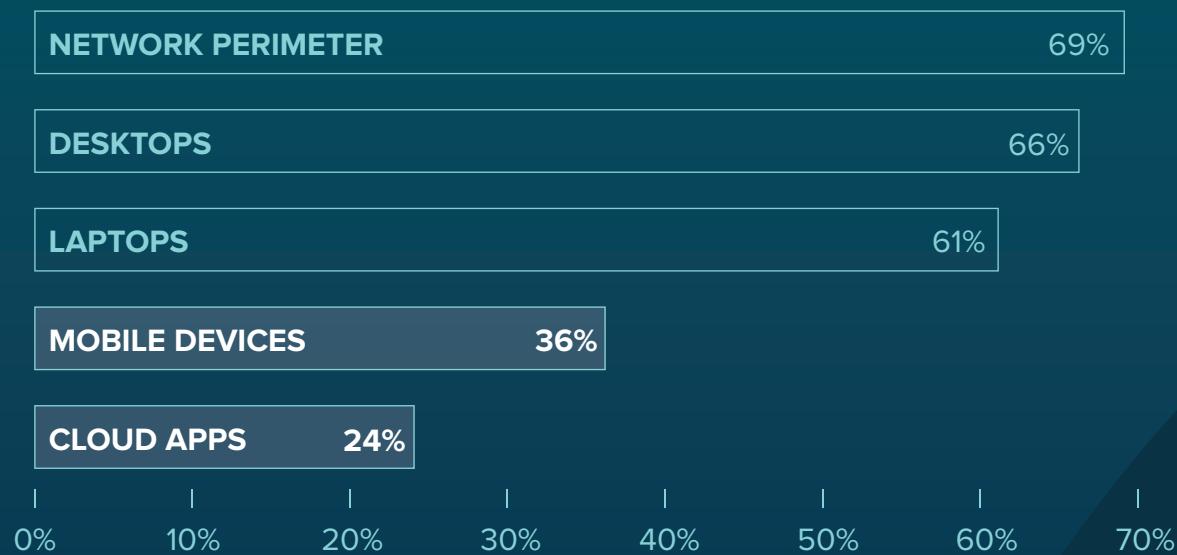
1 in 3 organizations were hacked more than 5 times in past 12 months. Double the rate from 2014.



This year, 87% of organizations suffered some cyber attack in the past 12 months and 86% believe another cyber attack in the next 12 months is likely. In fact, organizations have averaged 8 cyber attacks in the past 12 months.

DANGER: NO VISIBILITY

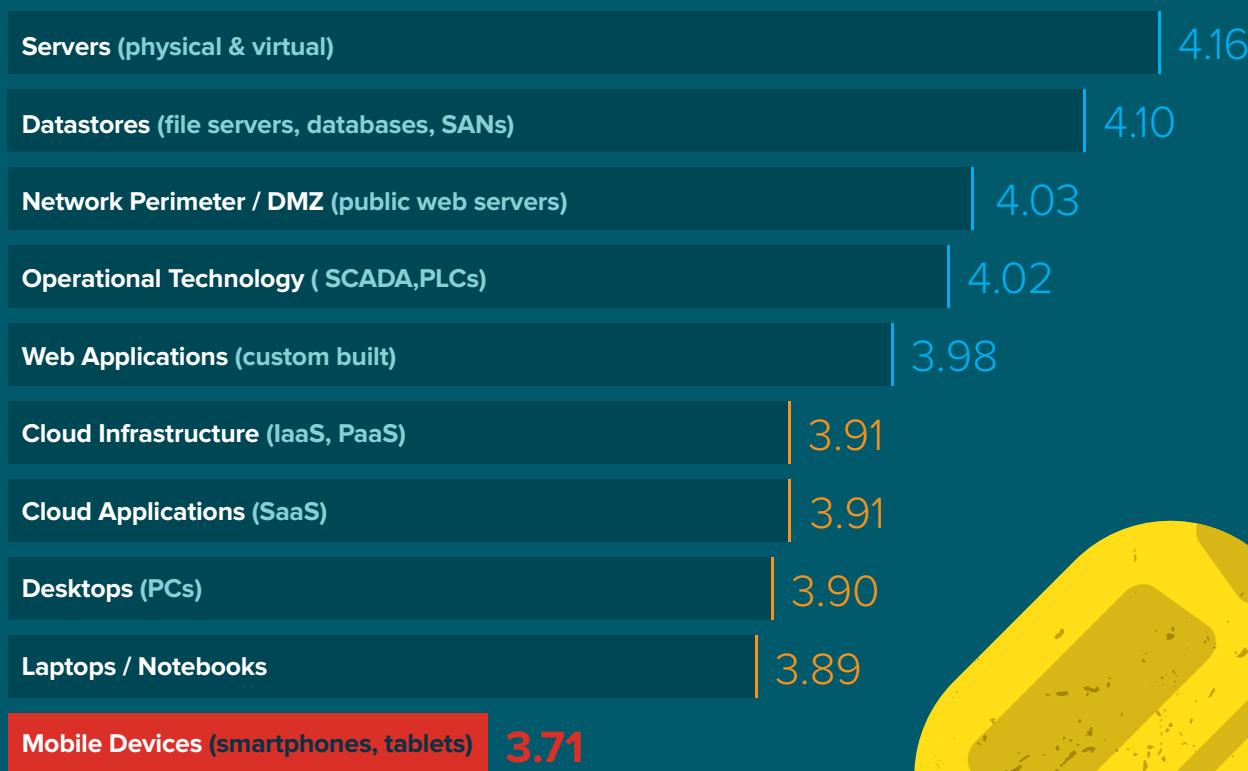
Despite public cloud apps becoming the foundation for organizational productivity, only **24% routinely monitor SaaS and IaaS apps for security risks**, compared to over 60% for desktops, laptops, and the network perimeter. Only 36% monitor mobile devices.



THE WEAK LINK

Despite the efforts made to secure mobile with MDM and MAM, most IT pros believe these existing solutions are inadequate.

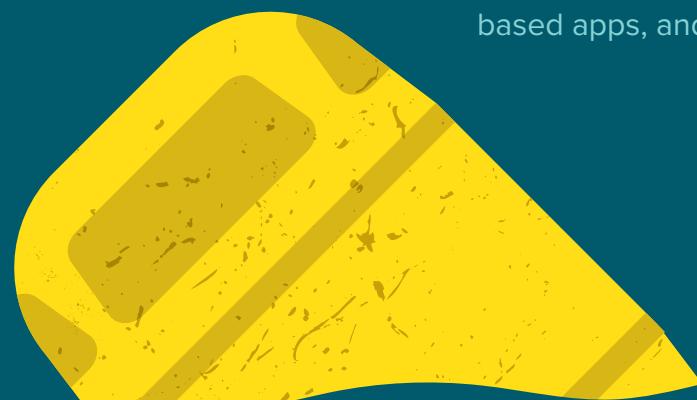
On a scale of 1 to 5, with 5 being the highest rate your organization's overall security posture (ability to defend against cyberthreats) in each of the following IT components: (n=1,088)



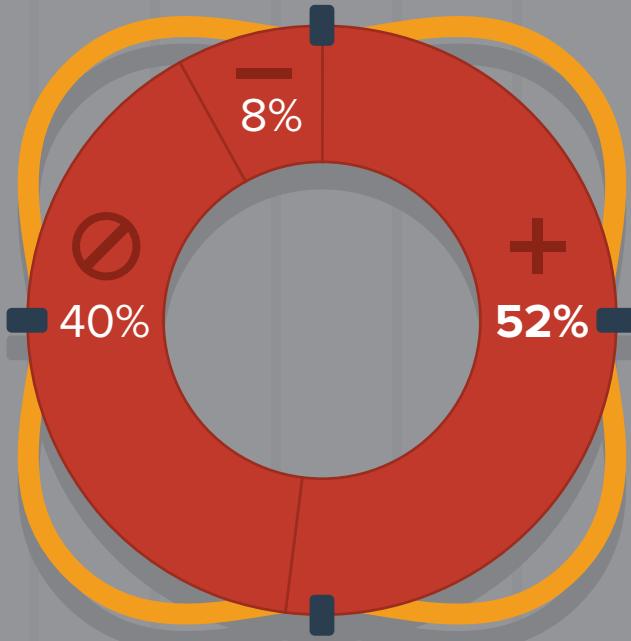
Asked to rate their organization's security posture, more identified mobile as somewhat vulnerable or highly vulnerable than any other system.

While some still believe cloud to be more vulnerable than premises-based apps and custom web applications, the vast majority agree that both are secure relative to mobile.

Across the board, these numbers are up from a year ago, where IT leaders were less convinced of their organization's ability to secure SaaS, IaaS, premises-based apps, and endpoints.



SPEND MORE, SAVE DATA

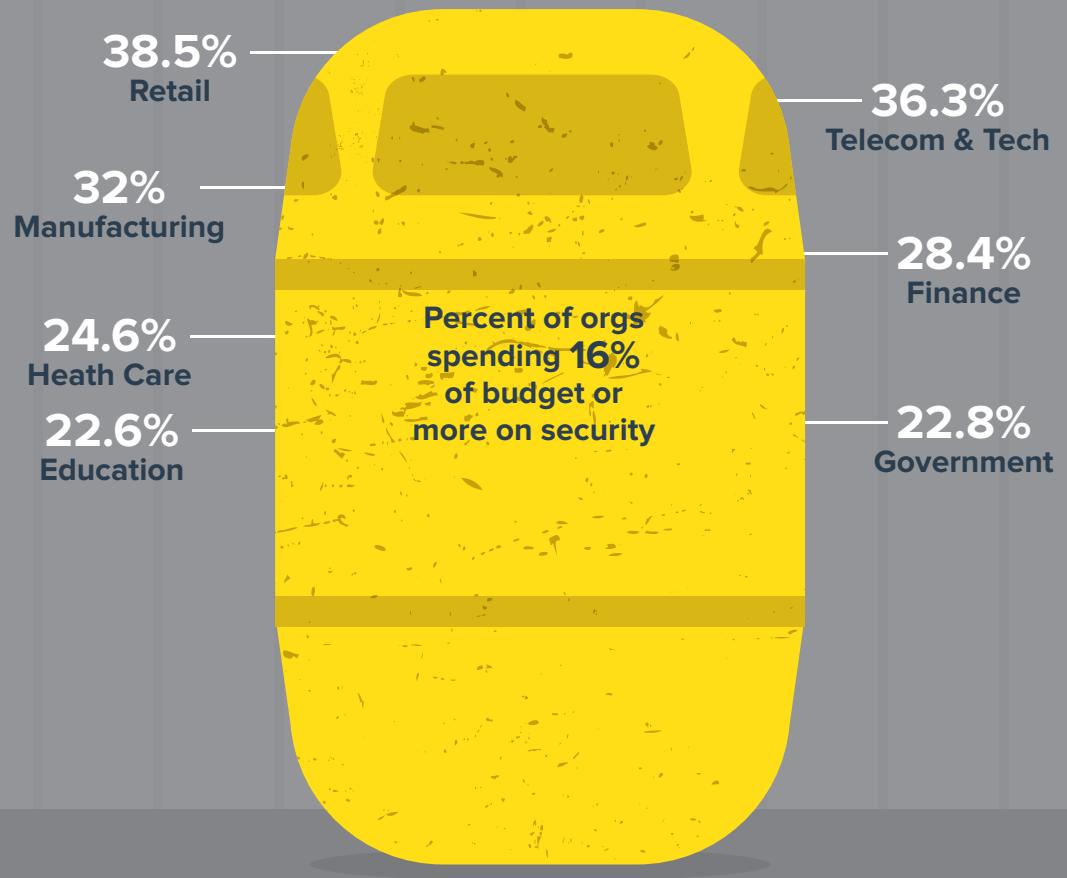


52% plan to increase their security budget

40% foresee no changes

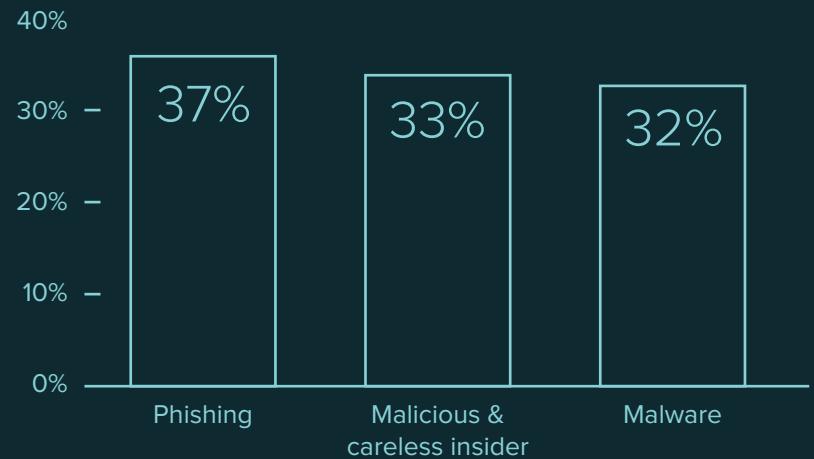
8% expect spend to decline

For 33% of organizations, IaaS security is the top priority followed closely by SaaS app security at 31%.

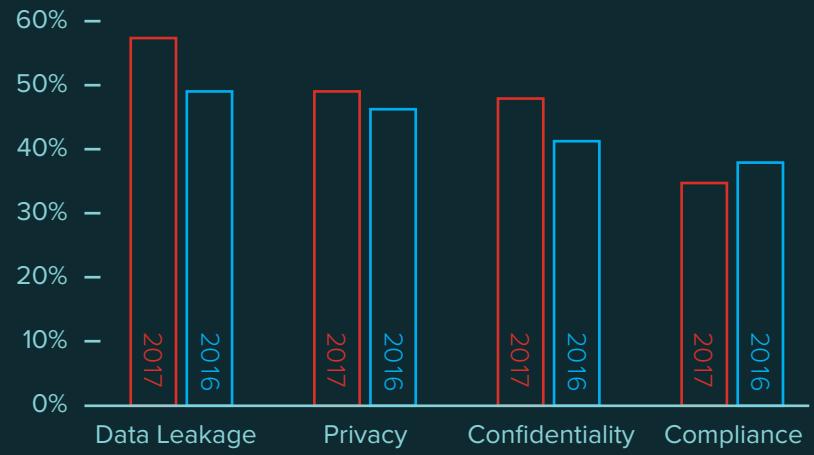


More organizations in the retail and tech sectors are spending a large proportion of budgets on security than in other verticals. Security conscious industries including finance and healthcare aren't far behind, where security budgets continue to grow rapidly.

PHISHING, MALWARE, AND MORE CONCERNS ARISE



For 37% of respondents, phishing is the top concern followed by insider threats (33%) and malware (32%)

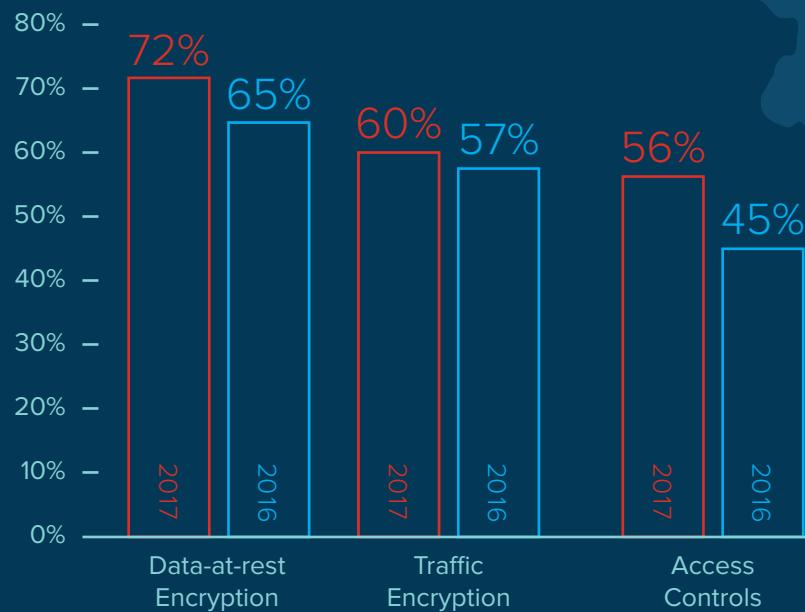


As for cloud-specific concerns, data leakage (57%), data privacy (49%), confidentiality (47%), and compliance (36%) are the issues enterprises are struggling with most, many up year-over-year.

SWIMMING TO SAFETY

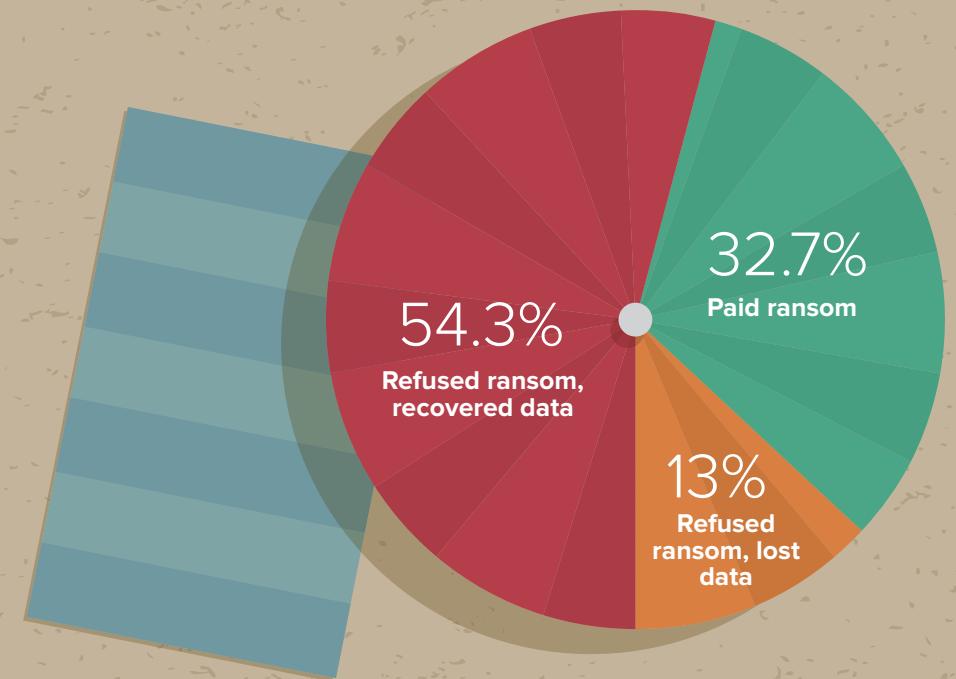
62% say improved threat detection is the most critical threat management capability

Enterprises that have moved to the cloud are well aware of the security gaps and limitations of these apps. In these organizations, data encryption (72%), traffic encryption (60%), and access controls (56%) are the capabilities most in demand.

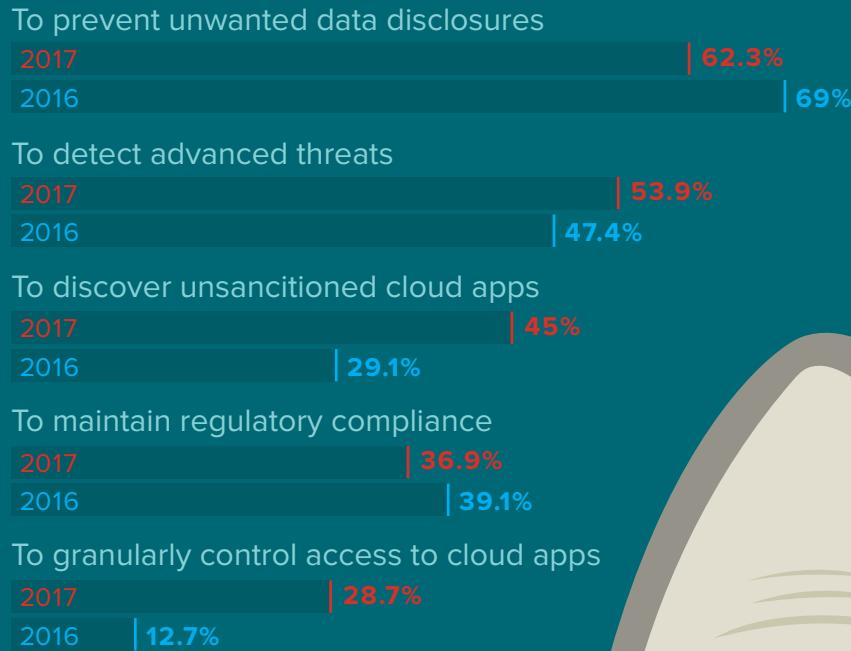


HANDLING RANSOMWARE

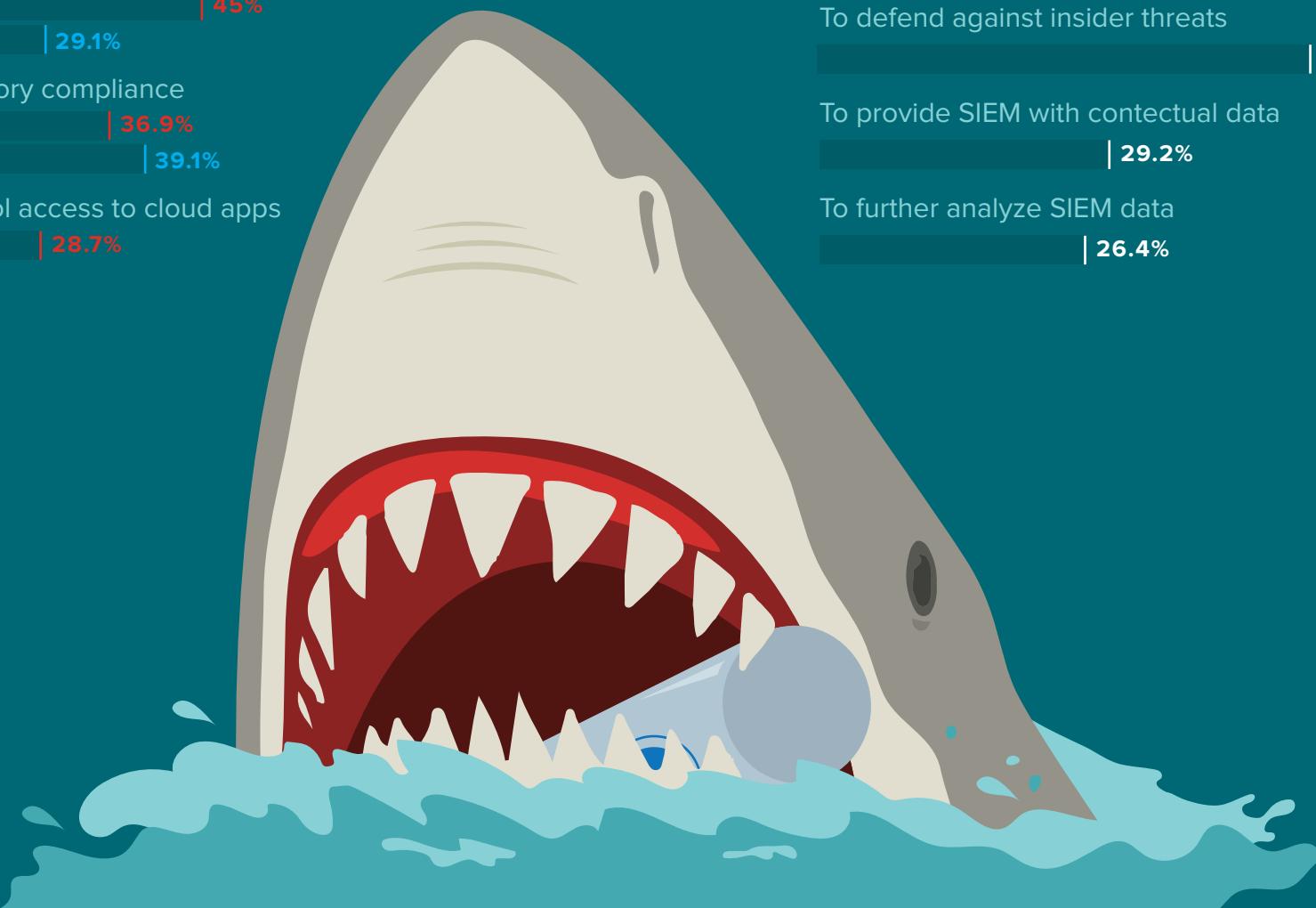
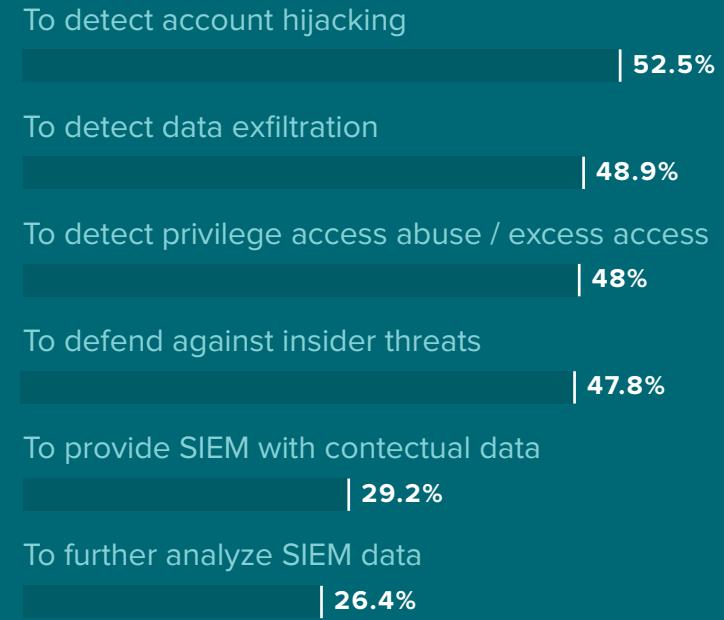
Ransomware is a major concern, but **54.3%** of enterprises managed to recover data without paying up.



WHY ARE ENTERPRISES USING CASBS?



WHY ARE ENTERPRISES USING UEBA?



WRAP UP

The cloud security landscape has changed a great deal in the past year, from the threats facing organizations to the security solutions many are using to protect themselves. One thing is clear: gaps still remain. While many have some means of alerting on potential leaks or unauthorized accesses, few have the ability to identify and remediate threats in real time and few can secure unmanaged mobile devices.

In the coming year, as more organizations put their security budgets to work, expect to see much needed capabilities—access controls, cloud DLP, encryption—become widespread. Only comprehensive cloud security that works across apps can truly be effective in defending against the threats that lurk just beneath the surface.



Phone: (408) 337-0190

Email: info@bitglass.com

www.bitglass.com

ABOUT BITGLASS

Bitglass, the total data protection company, is a global Cloud Access Security Broker 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.