bitglass

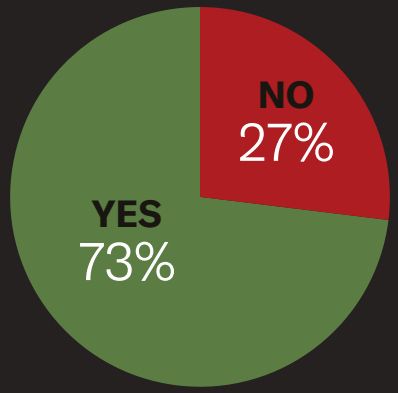
THREATBUSTERS

BITGLASS' 2019 INSIDER THREAT REPORT

Insider threats constitute a legitimate danger to enterprise security. While protecting data from malicious external actors is typically top of mind for most organizations, the fact remains that they must also defend against negligent and disgruntled insiders. To learn more about how well organizations are accomplishing this, Bitglass partnered with a leading cybersecurity community to survey IT professionals and gain unique insights about insider attacks.

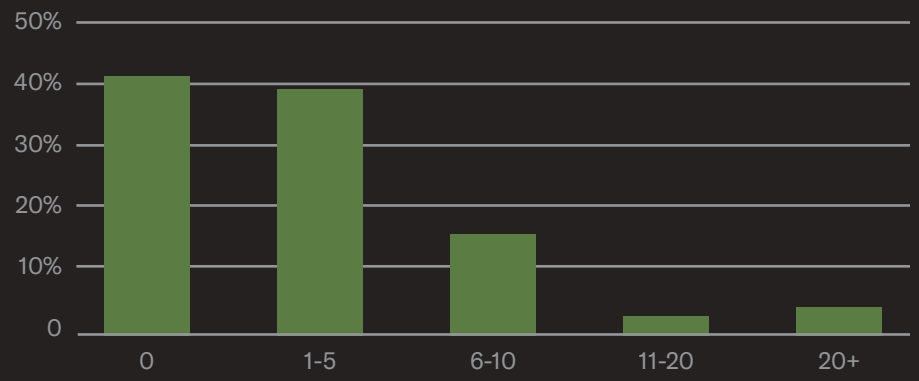
THE RISE OF INSIDER THREATS

Have insider attacks become more frequuent?

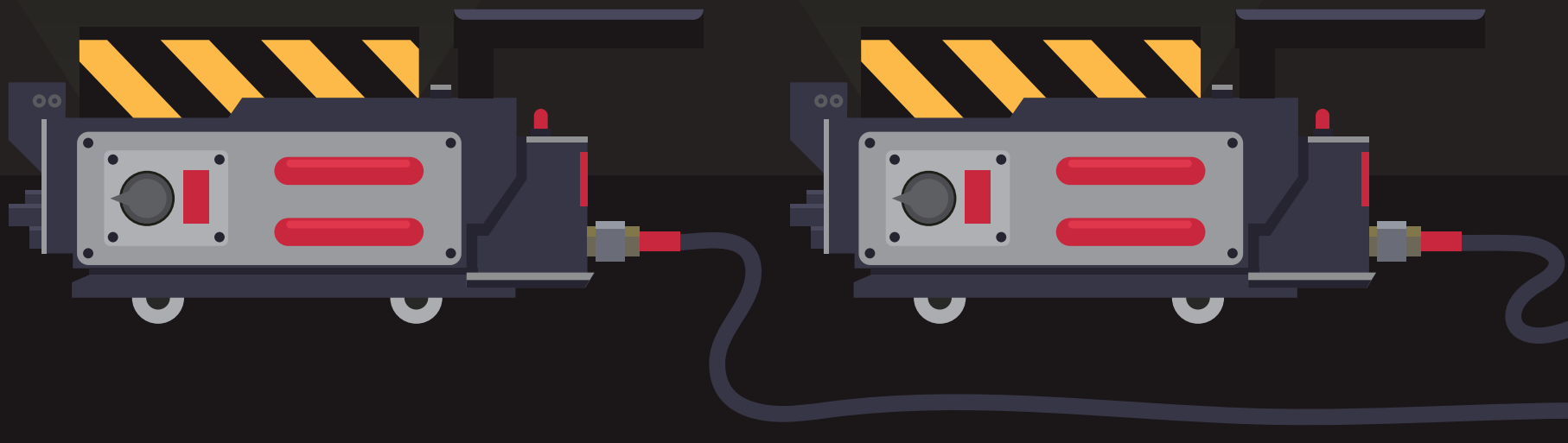


A massive 73% of respondents stated that insider attacks have become more frequent over the past year. When asked the same question in 2017, 56% responded in this fashion.

How many insider attacks did your organization experience in the last 12 months?

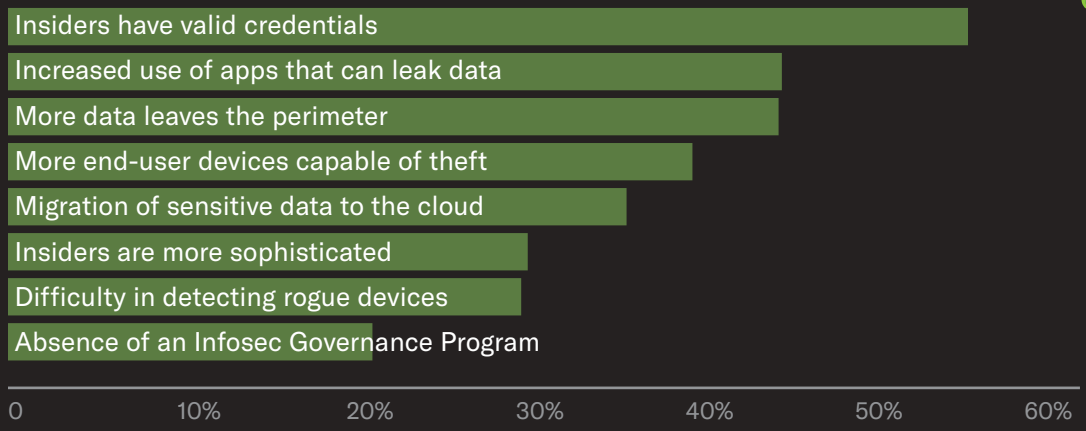


59% of organizations experienced an insider attack over the past year. This is an increase from the prior report in 2017 when only one in three firms reported an insider attack.



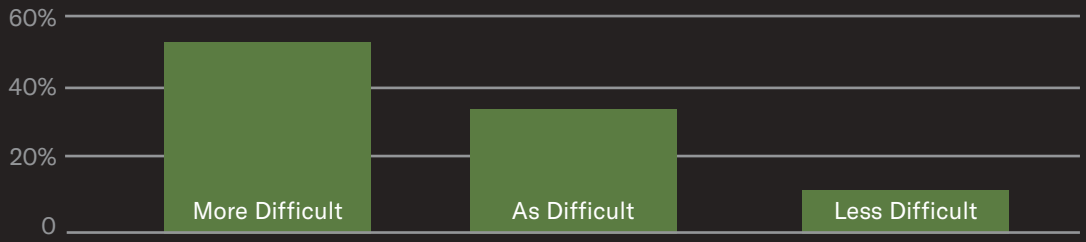
SEEING THE UNSEEN

What makes the detection of insider attacks more difficult than a year ago?



Four of the top five reasons for the growing difficulty in detecting insider attacks are related to data moving off premises and into a growing number of applications and devices.

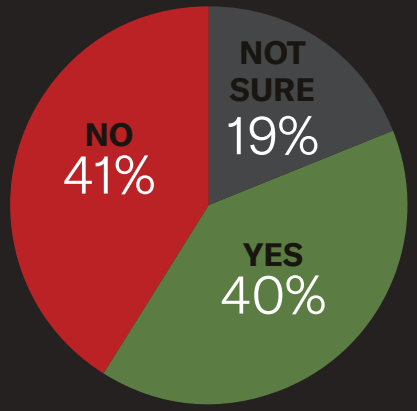
How difficult is it to detect insider attacks compared to external cyberattacks?



54% of respondents said that it is more challenging to detect insider attacks than it is to detect external cyberattacks.

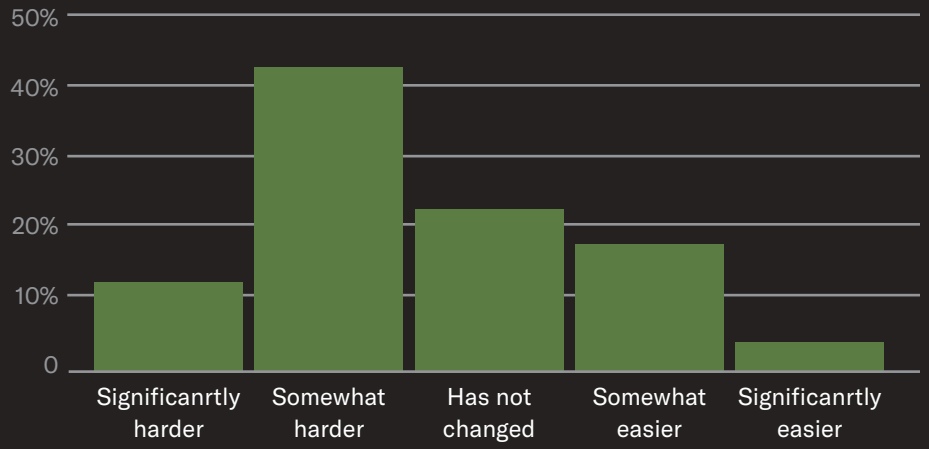
THREATS FROM BEYOND

Do you monitor abnormal user behavior accross your cloud footprint (SaaS, IaaS, PaaS)?

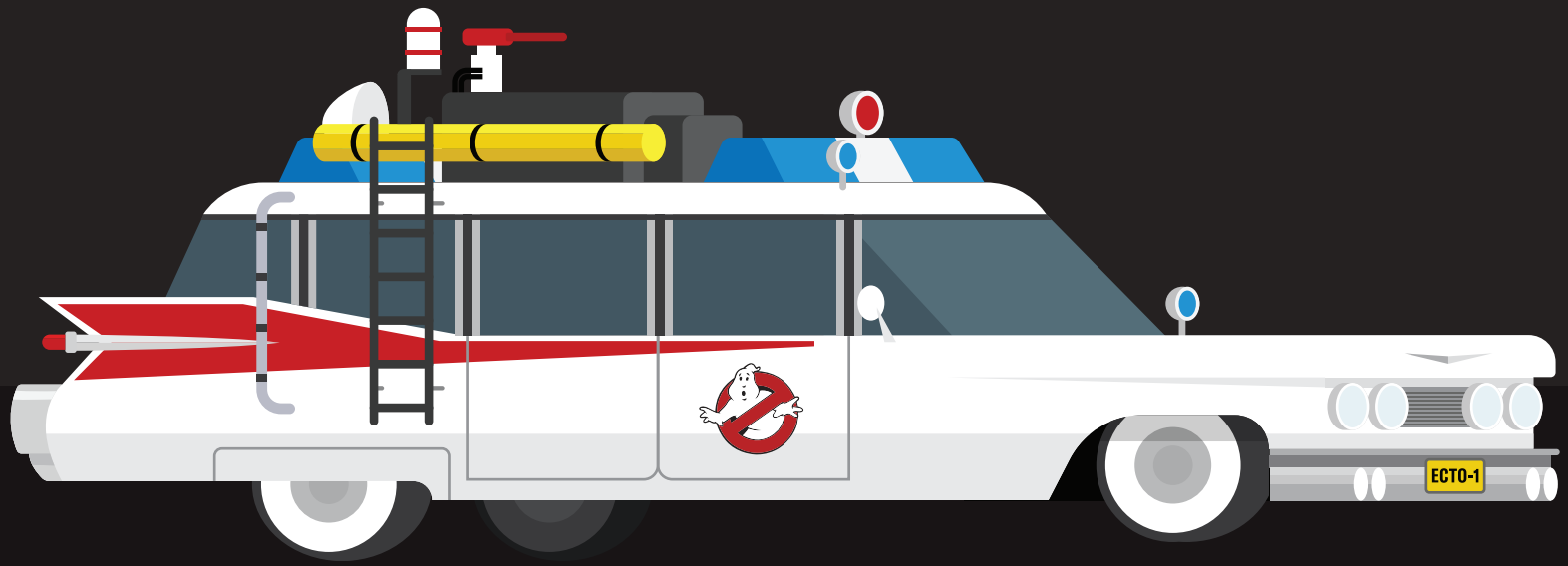


41% of respondents said that they do not monitor for abnormal user behavior across their cloud footprints, and 19% were unsure if they do so.

Since migrating to the cloud, detecting insider attacks is:

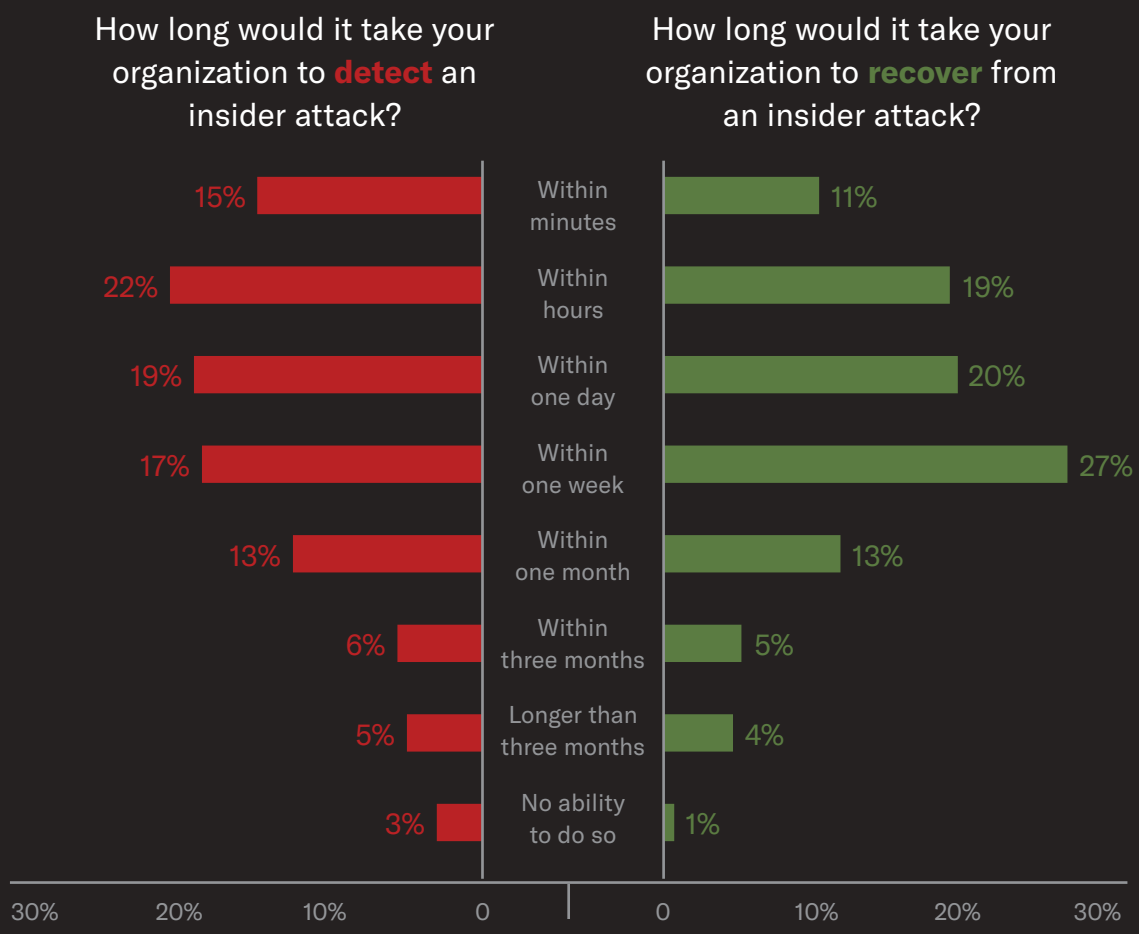


According to 56% of organizations, it is more challenging to detect insider threats after migrating to the cloud. It is likely that this is largely due to the aforementioned lack of monitoring.



FIGHTING OFF FRIGHTFUL FIENDS

Only about half of respondents (56%) claim that they can detect insider attacks within the day that they occur, and only 50% say they can recover within the same period. However, this still seems optimistic because insider attacks can span long periods of time and IT departments aren't necessarily aware of all of the attacks faced by their organizations.

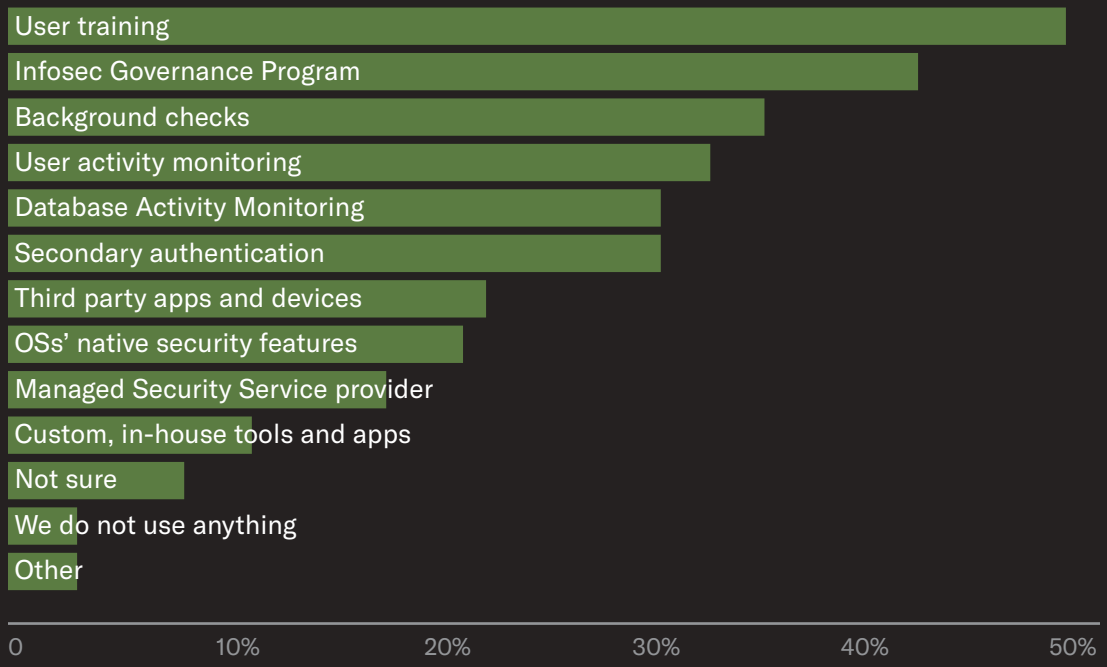


WHO YA GONNA CALL?

Four of the top five security tools identified by respondents were data loss prevention (52%), encryption (50%), identity and access management (50%), and user behavior anomaly detection (48%). All of these (as well as others further down the list) are available with advanced solutions like cloud access security brokers (CASBs).

HOW'S THE GRID HOLDING UP?

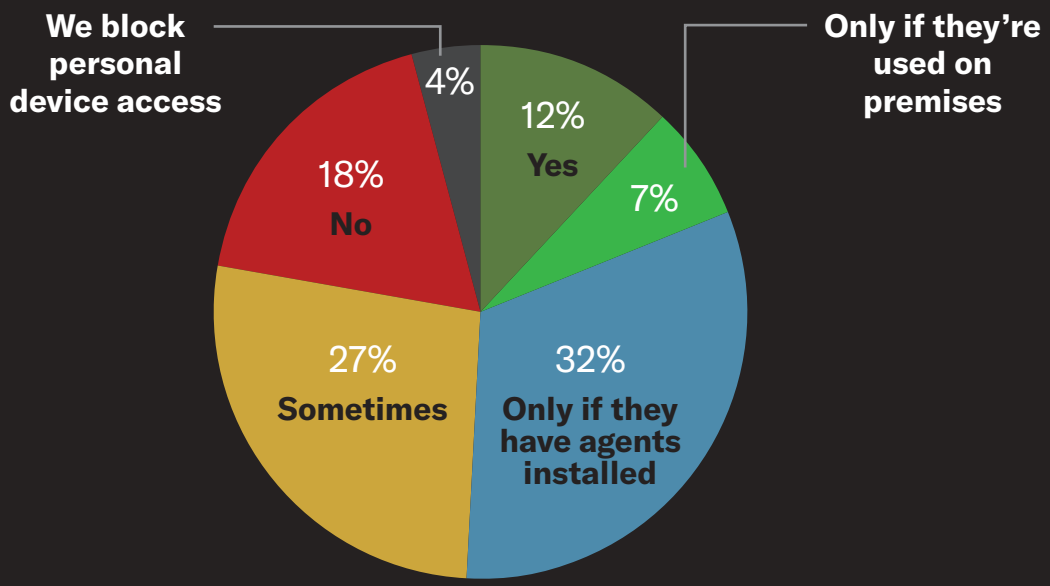
How does your organization combat insider threats today?



Merely 50% of firms provide user training to combat insider threats. Additionally, key functionality such as user activity monitoring and secondary authentication are only used by 33% and 31% of organizations, respectively. As such, it is not surprising that 68% of organizations feel moderately to extremely vulnerable to insider threats.

DO YOU BELIEVE IN BYOD?

Can you detect insider threats stemming from personal mobile devices?

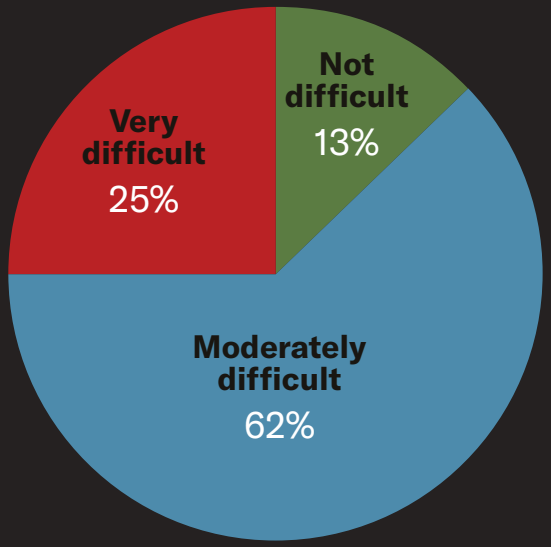


Only 12% of enterprises are able to detect any insider threat stemming from a personal mobile device—27% said that they can only do so sometimes. This is consistent with a separate question in which respondents identified endpoints in general (59%) and mobile devices in particular (46%) as the two assets most commonly used to launch insider attacks.

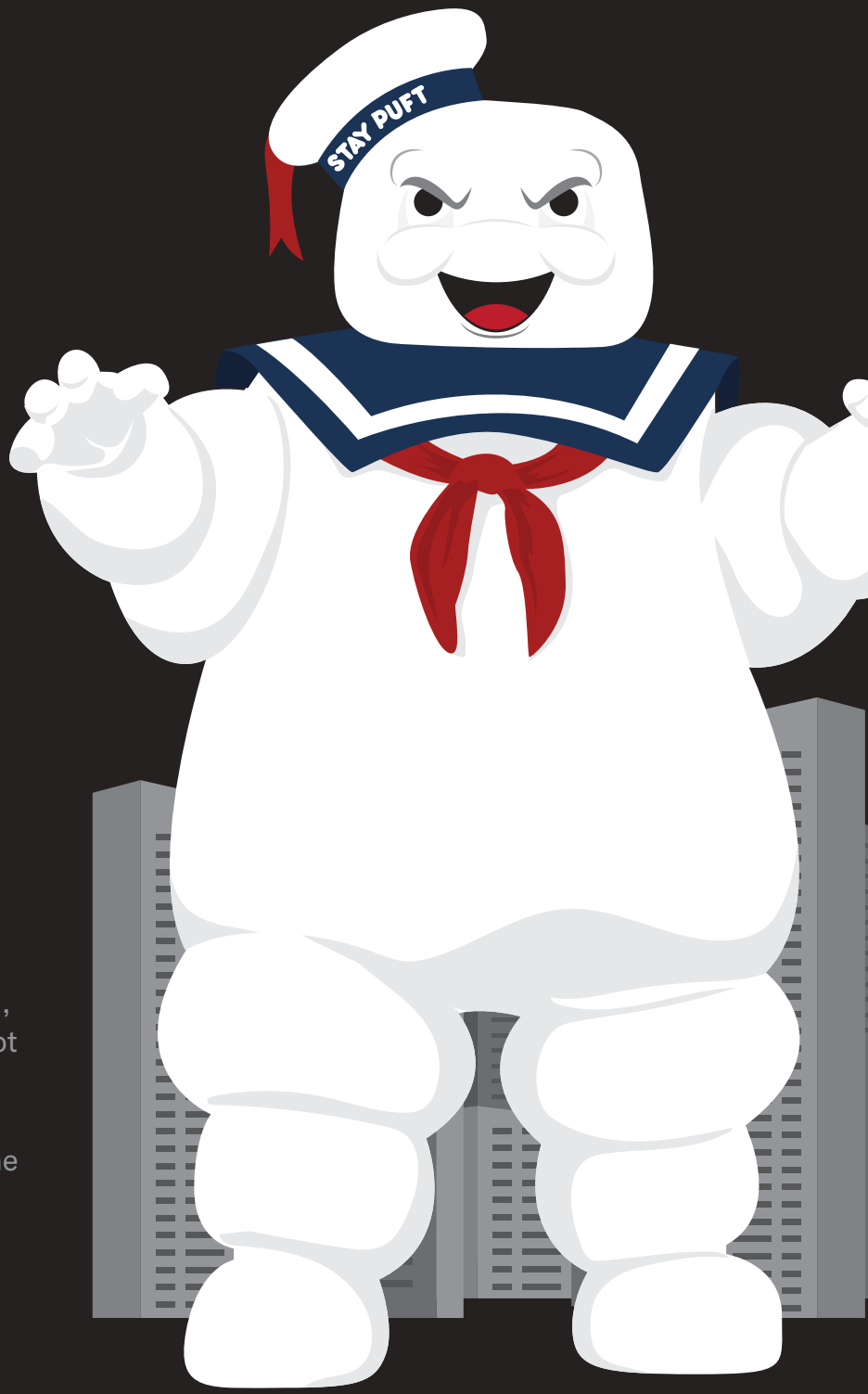
39% of respondents said that their organizations can detect insider threats on personal mobile devices if they have agents installed or are used on premises. However, this is not sufficient in a world where mobile devices access data off premises and employees reject agents on their personal phones.

DEFINITELY MORE THAN ELEVEN–FIVE A YEAR

How difficult is it to determine the actual damage of an insider attack in your organization?



87% of respondents found it moderately to very difficult to determine the actual damage caused by insider attacks. In light of the findings on the previous pages, this should not come as a surprise. For many enterprises, user behavior in the cloud is not being monitored, the appropriate data protection tools are not being used, and personal mobile devices are not being properly secured. Naturally, these all make it more challenging to detect, remediate, and assess the damage done by insider attacks.



WRAP-UP

For enterprises that want to be secure and successful in today's dynamic, competitive business environment, they must be able to prevent and respond to insider attacks. As detailed above, many organizations still need to take steps if they want to be capable of doing so. Fortunately, there are specialized security solutions that are up to the challenge.

bitglass

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

www.bitglass.com

ABOUT BITGLASS

Bitglass, the Next-Gen CASB company, is based in Silicon Valley with offices worldwide. The company's cloud security solutions deliver zero-day, agentless, data and threat protection for any app, any device, anywhere. 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.