BYOD AND IDENTITY

What you see isn't always what you get.

bitglass

Growing demand for flexibility and mobility in the workplace has prompted enterprises to adopt bring your own device (BYOD) policies. However, security concerns have driven many IT departments to reevaluate their unmanaged device security postures.

Bitglass' research team surveyed 200 IT and security professionals at a national Gartner conference to learn more about the evolution of BYOD security in a mobile-first world.

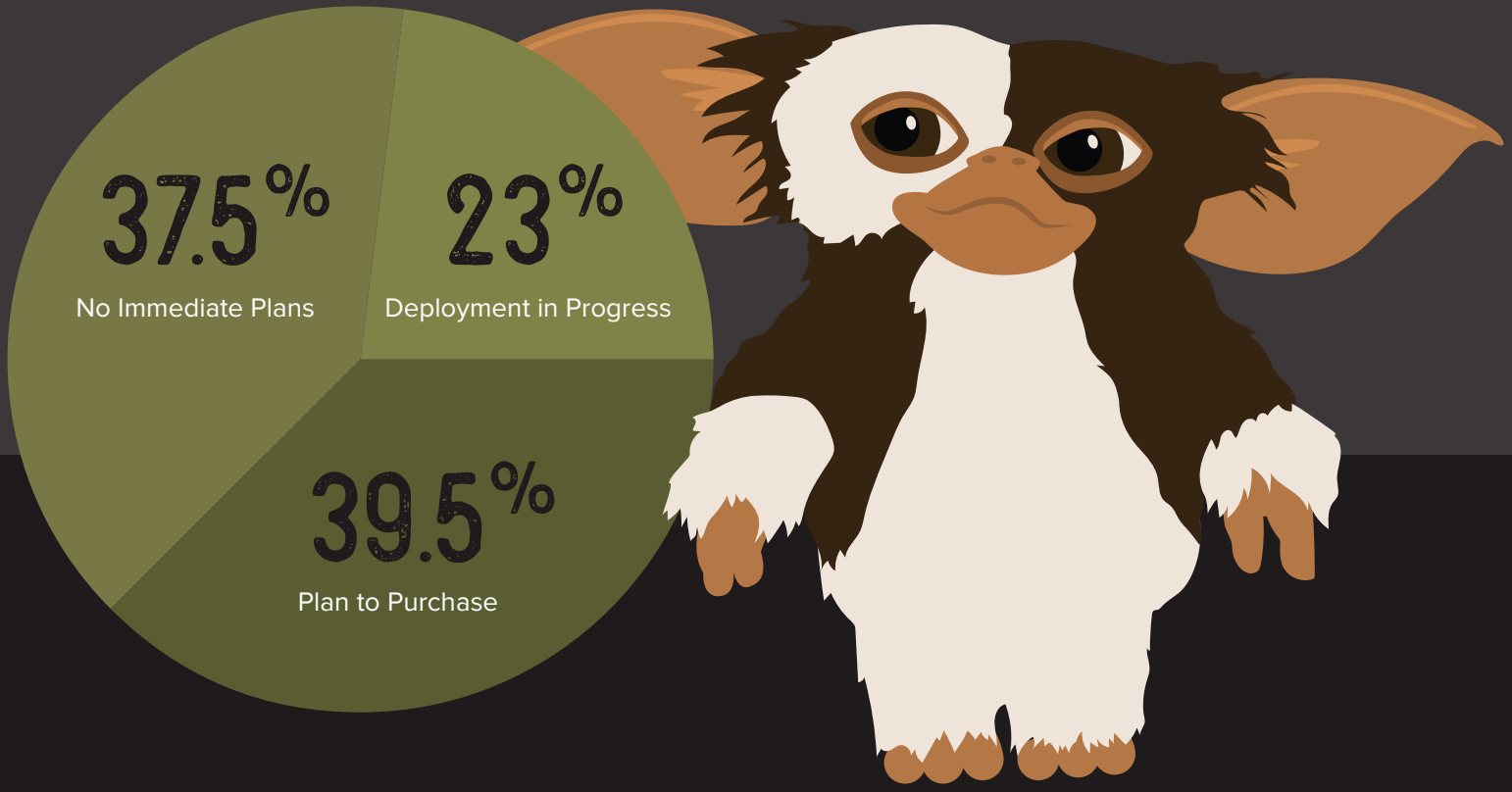
Planning for Your Mogwai

Nearly two in three enterprises have deployed or plan to deploy a CASB for BYOD security.

Traditional answers to the BYOD security challenge—mobile device management (MDM) among them—have proven invasive, cumbersome to deploy, and are often rejected by employees. IT departments have since turned to next-generation BYOD security solutions like cloud access security brokers (CASBs).

CASBs allow organizations to have visibility and control over BYO devices and cloud applications.

CASB Deployment Plans



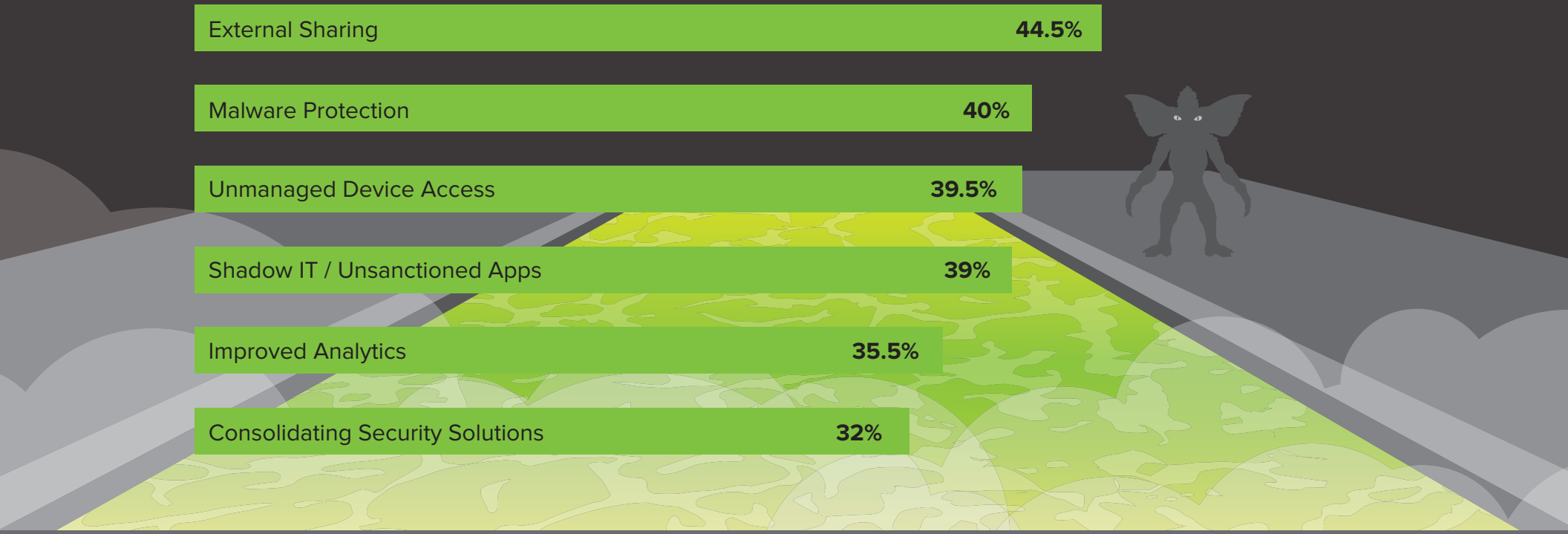
Avoiding an Outbreak

BYOD security and access remain among the top concerns for IT departments. When asked for their priorities in protecting corporate data on these devices, respondents highlighted several threats that they are actively looking to mitigate.

External sharing, malware protection, and unmanaged device access are the leading concerns for security professionals, indicating that organizations are doubling down on protecting data beyond the corporate network.

Shadow IT and unsanctioned apps (39%), improved analytics (35.5%), and consolidating security solutions (32%) were also selected as security concerns.

Top Security Priorities for 2018

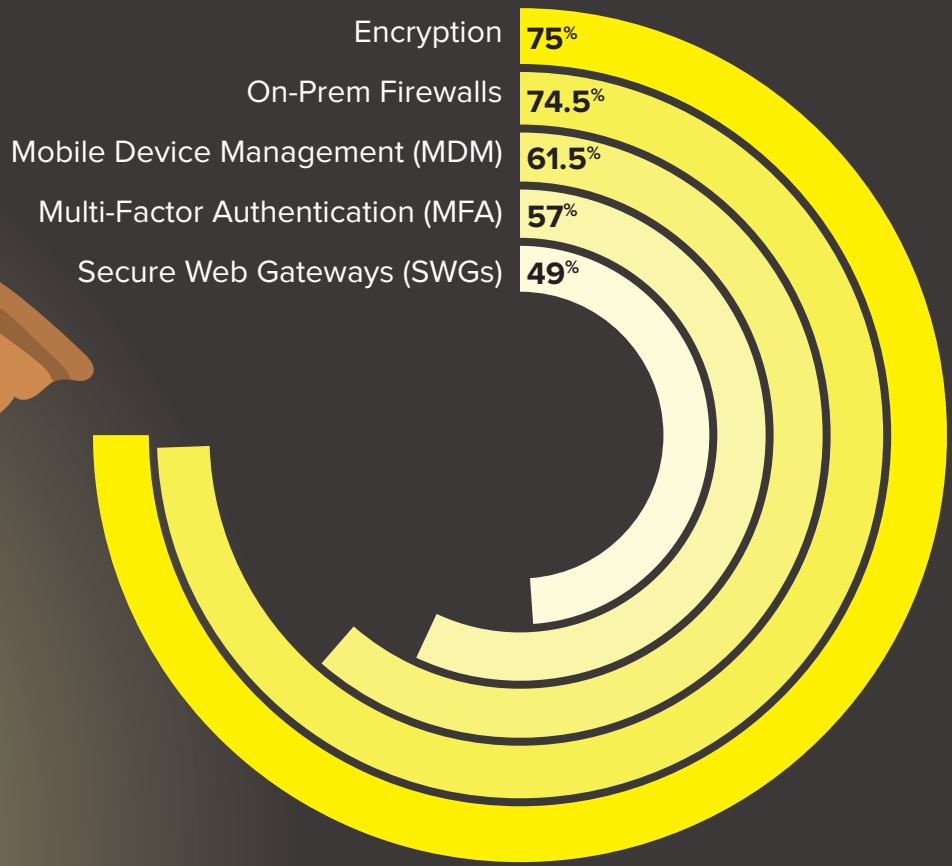


Keep Your Data out of the Light

75% of organizations still use an on-premises firewall, but many are transitioning to alternative solutions for BYOD security.

Traditional security solutions, while still widely used, have become inadequate for the modern era. Advances in work environments have required IT to shift toward new means of protecting cloud and mobile traffic. Next-generation solutions like CASBs and Secure Web Gateways (SWGs) have been deployed in a growing number of enterprises today.

How Enterprises Secure Corporate Data



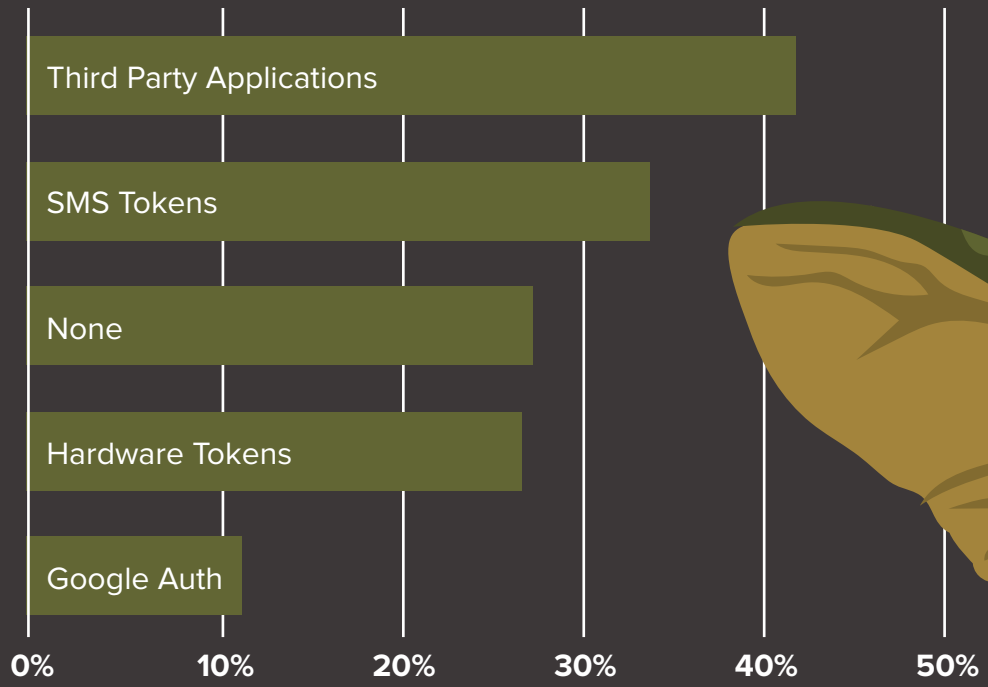
Are Your Users Gremlins or Mogwais?

1 in 4 organizations rely solely upon user-generated passwords.

Having a secure method for BYOD authentication is table stakes for enterprises that want to enable employee mobility. Some recent security breaches—the 2017 Deloitte breach, for example—were in part due to weak, single-factor methods of authentication. With just an administrator's email and password, hackers are able to access mass amounts of corporate data.

Fortunately, 72.5% of security professionals use some combination of SMS tokens, hardware tokens, or applications like Google Authenticator. 41.5% reported that they rely on third-party identity providers (IdPs) like Okta or ADFS to enable MFA.

Required MFA Methods for BYOD



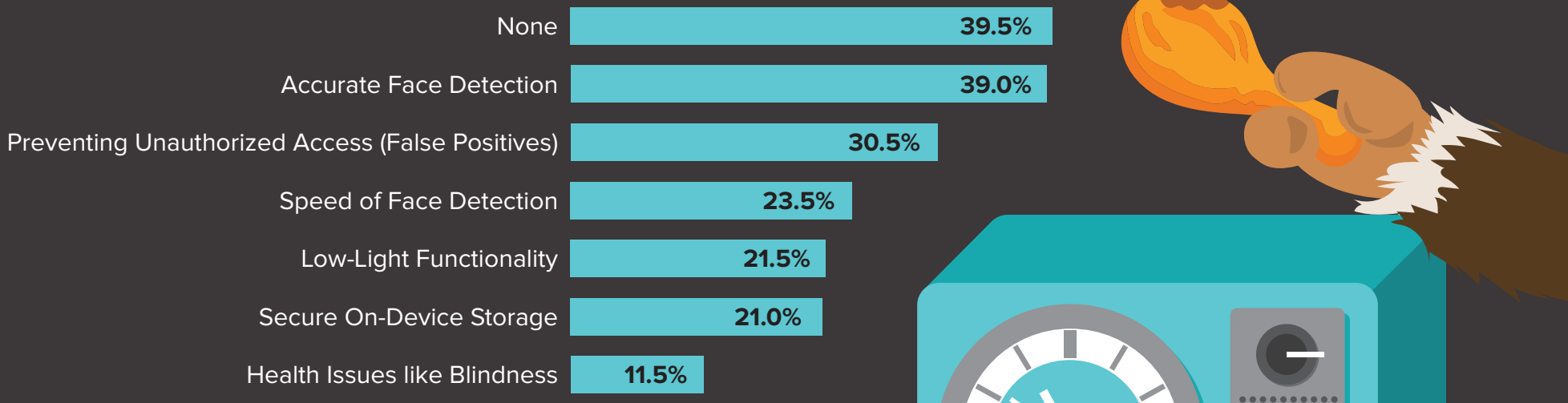
The Next Generation of Gizmos

40% have no reservations surrounding Apple Face ID.

Technology is moving beyond passwords and into the realm of biometric authentication mechanisms like fingerprint and face recognition. These methods of securing devices are regarded as more secure because they are unique to each user.

When asked about Apple's Face ID as a method of mobile authentication, responses were split on the tool's reliability. Concerns included accuracy of face detection (39.5%), prevention of unauthorized access (30.5%), and speed of face detection (23.5%).

Apple Face ID Reservations



Wrap-Up

BYOD requires that enterprises adopt modern methods of security. Looking ahead, IT departments will be forced to change the way that they think about data protection—particularly as new technologies like Apple's Face ID enter the market. Forward-thinking enterprises are focused on total data protection, secure authentication, and the tools that best balance security and employee productivity.

bitglass

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

www.bitglass.com

About Bitglass

Bitglass is a global CASB and agentless mobile security company based in Silicon Valley. The total data protection solution enables real-time, end-to-end security, from the cloud to any 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.