Bring Your Own Device.

Bitglass' 2020 Personal Device Report

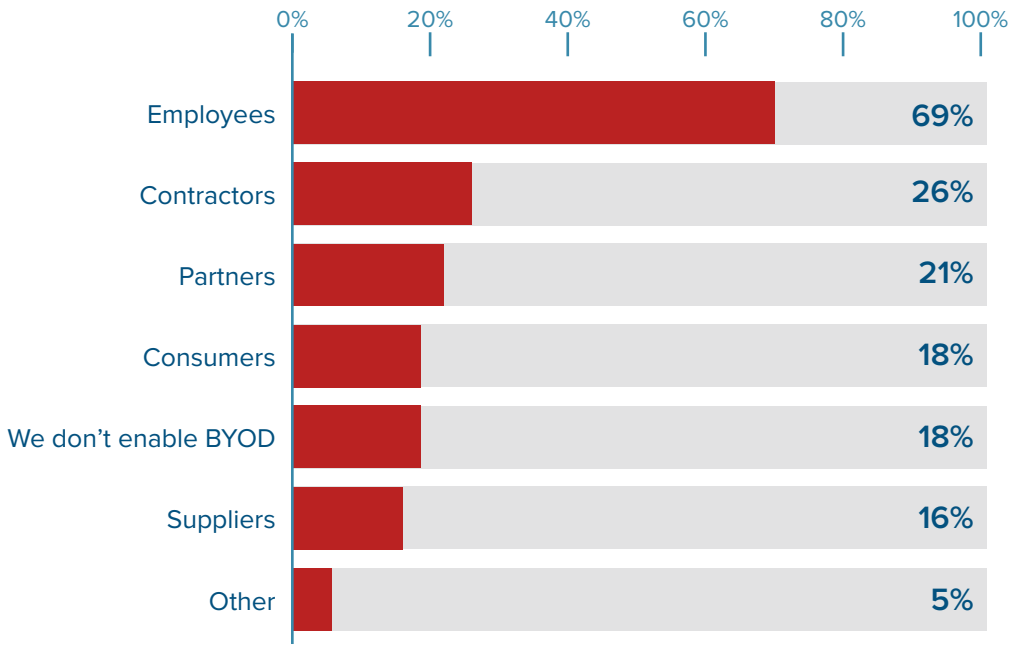
bitglass

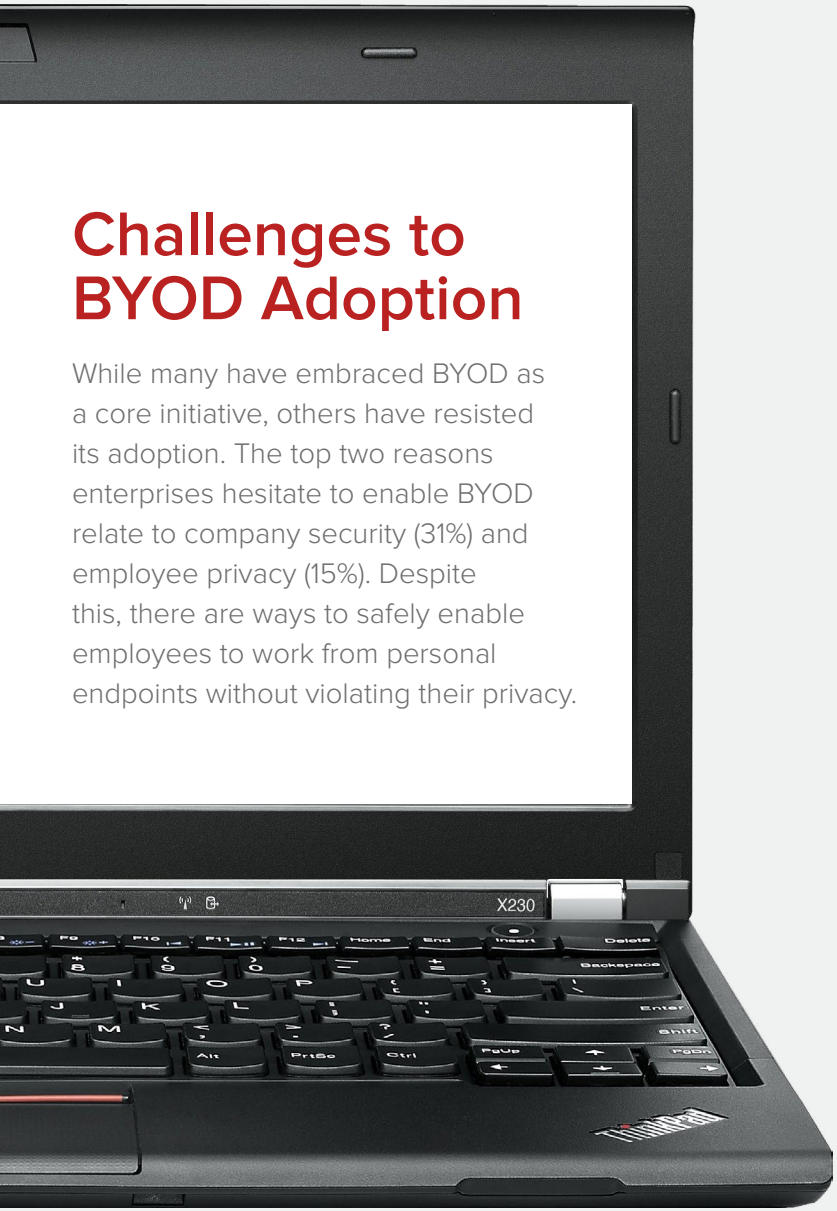
As bring your own device (BYOD) approaches surge, largely driven by requirements to work flexibly with personal and mobile devices, the complexity of the security requirements have surged. To make the challenge even more pronounced, the expansion of the “extended workforce”—contractors, partners, customers, and suppliers—lends itself to new use cases (e.g. new apps, new unmanaged devices) that can’t be managed via exception. As a result, most are faced with a fundamental question: how do organizations increase productivity without compromising the security of sensitive information?

BYOD in the Enterprise

This 2020 BYOD Report focuses on how companies have enabled the use of personal devices, their concerns around security, and the actions they have taken to protect data.
With breaches on the rise, and threat actors finding new ways to steal information, organizations must equip themselves with proper tools to protect data.

What user group(s) does your organization enable BYOD for?

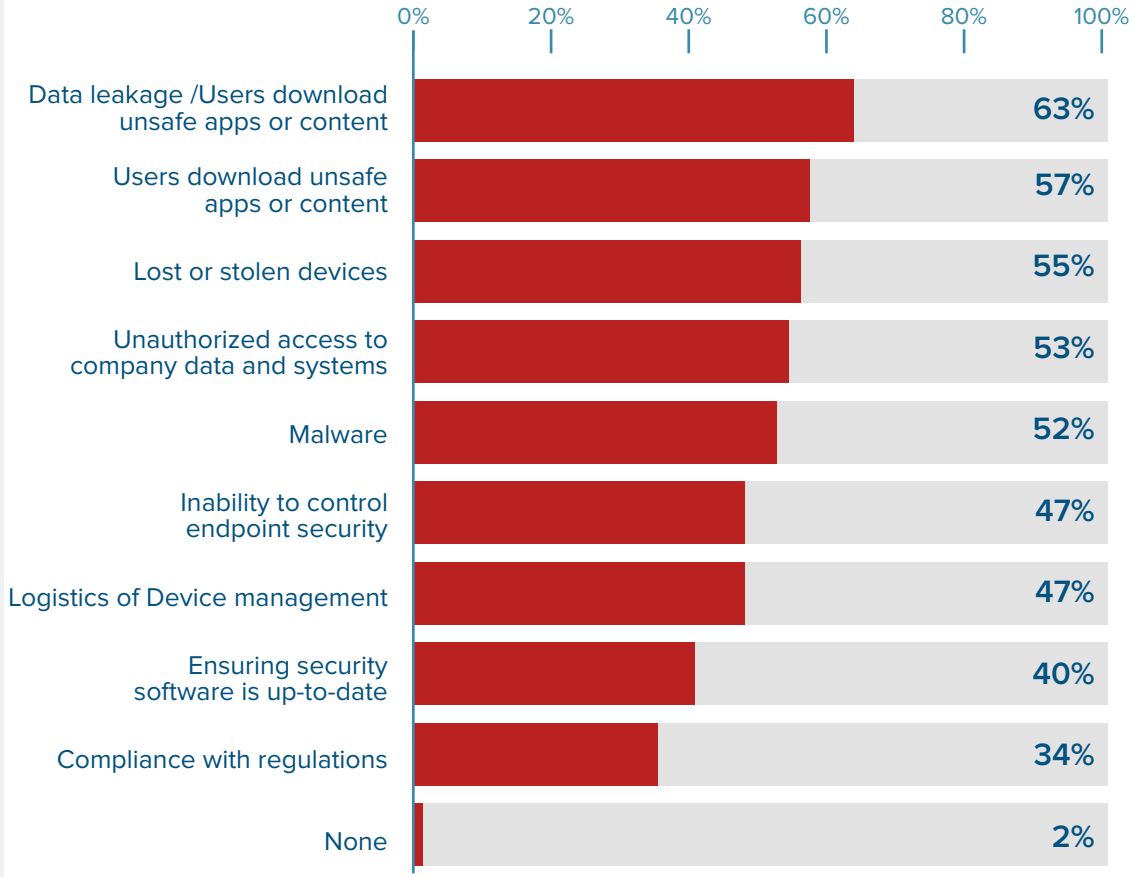


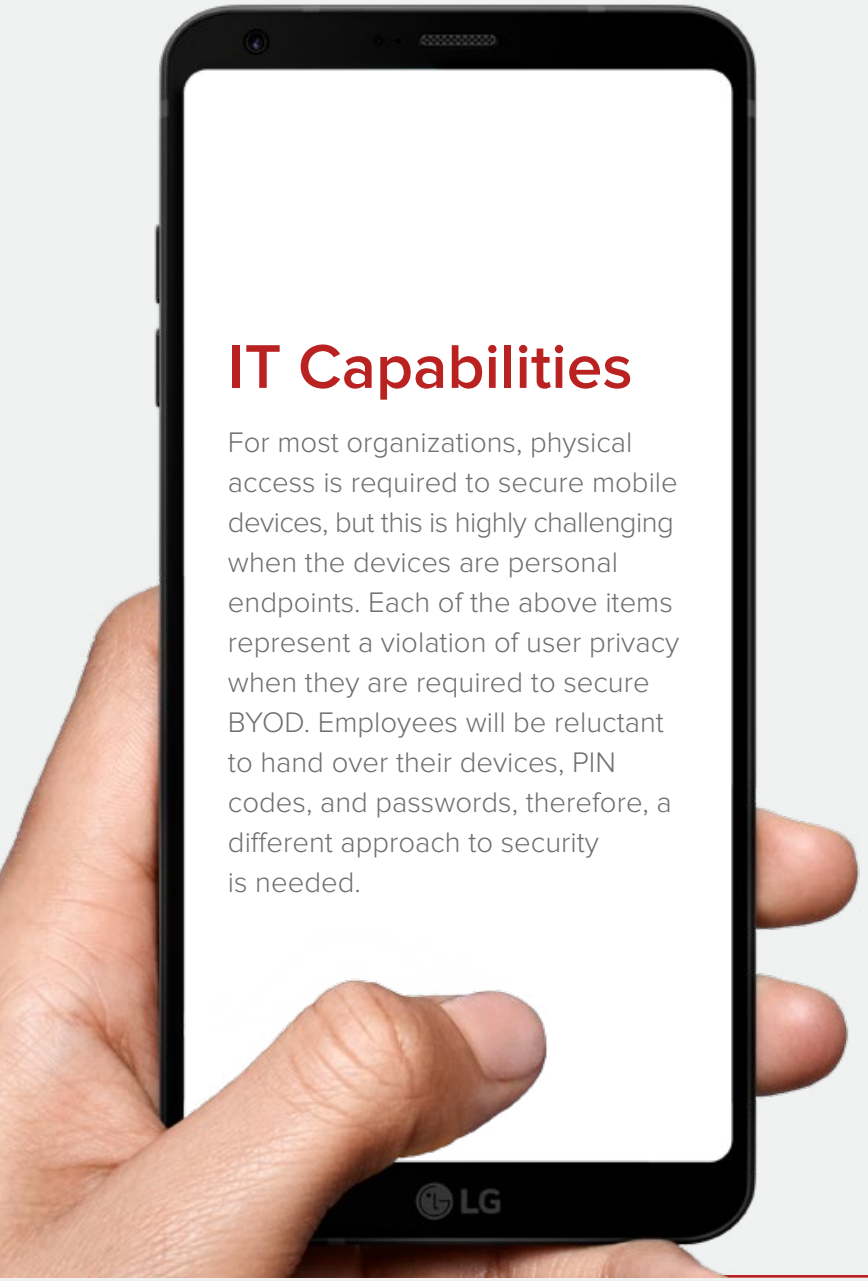


Challenges to BYOD Adoption

While many have embraced BYOD as a core initiative, others have resisted its adoption. The top two reasons enterprises hesitate to enable BYOD relate to company security (31%) and employee privacy (15%). Despite this, there are ways to safely enable employees to work from personal endpoints without violating their privacy.

What are your main security concerns related to BYOD?

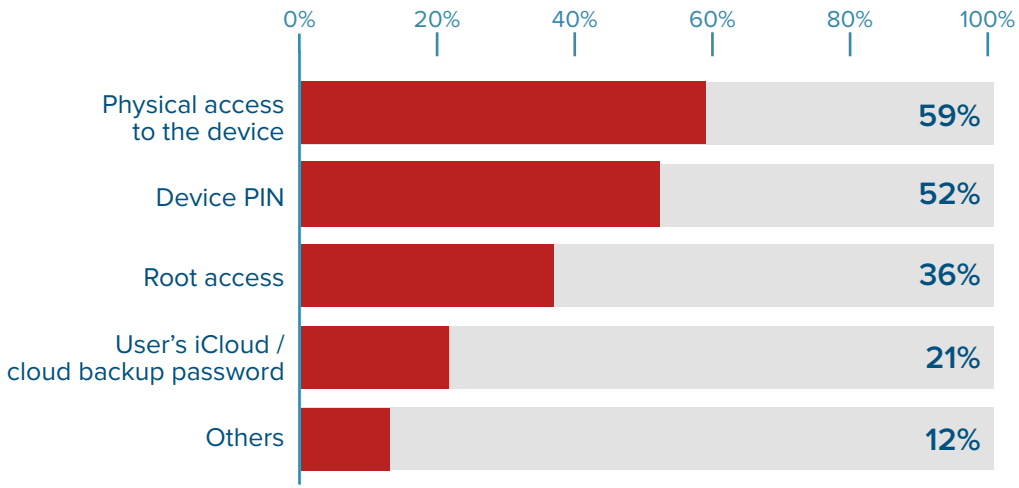


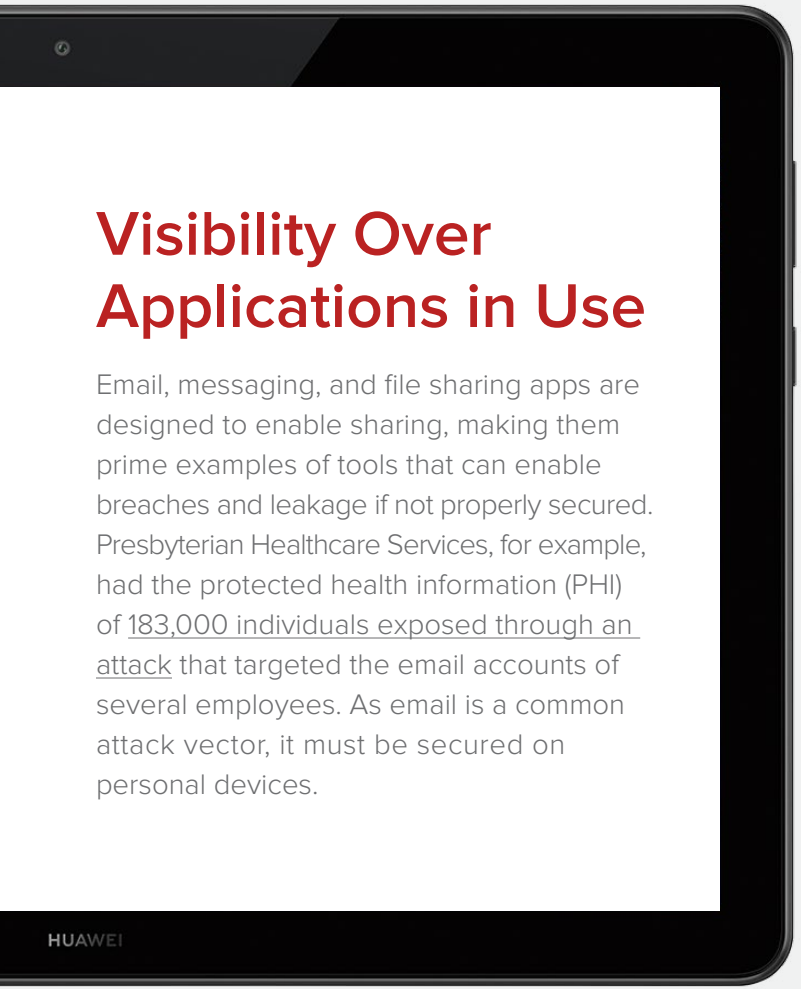


IT Capabilities

For most organizations, physical access is required to secure mobile devices, but this is highly challenging when the devices are personal endpoints. Each of the above items represent a violation of user privacy when they are required to secure BYOD. Employees will be reluctant to hand over their devices, PIN codes, and passwords, therefore, a different approach to security is needed.

Which of the following do you need when provisioning a mobile device?

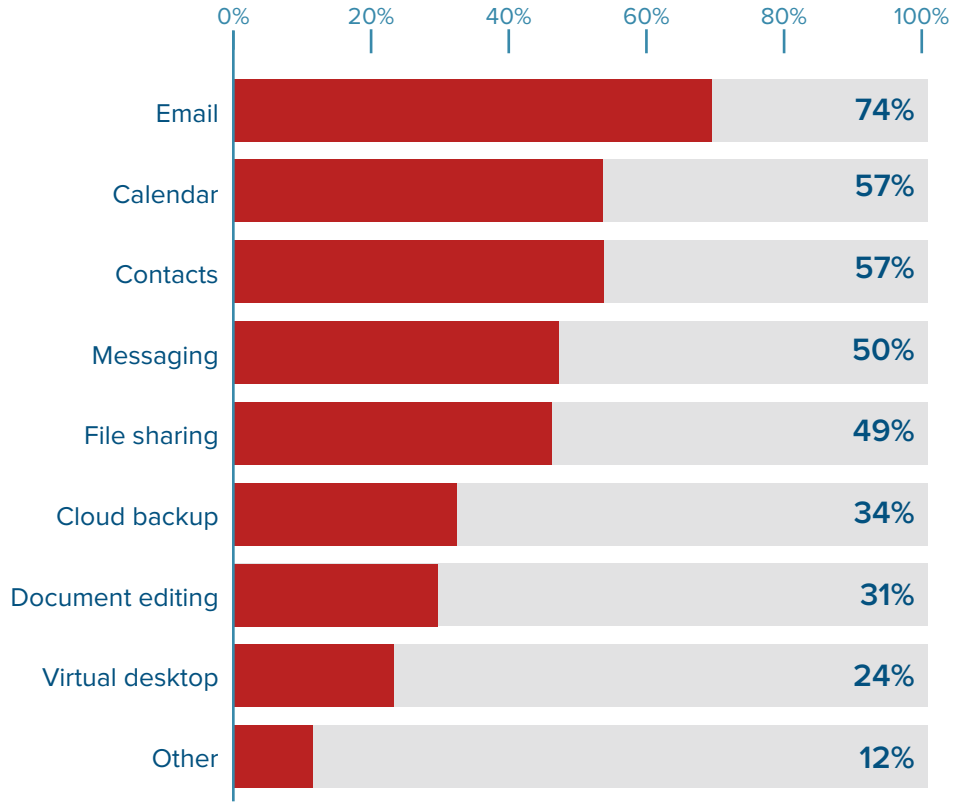


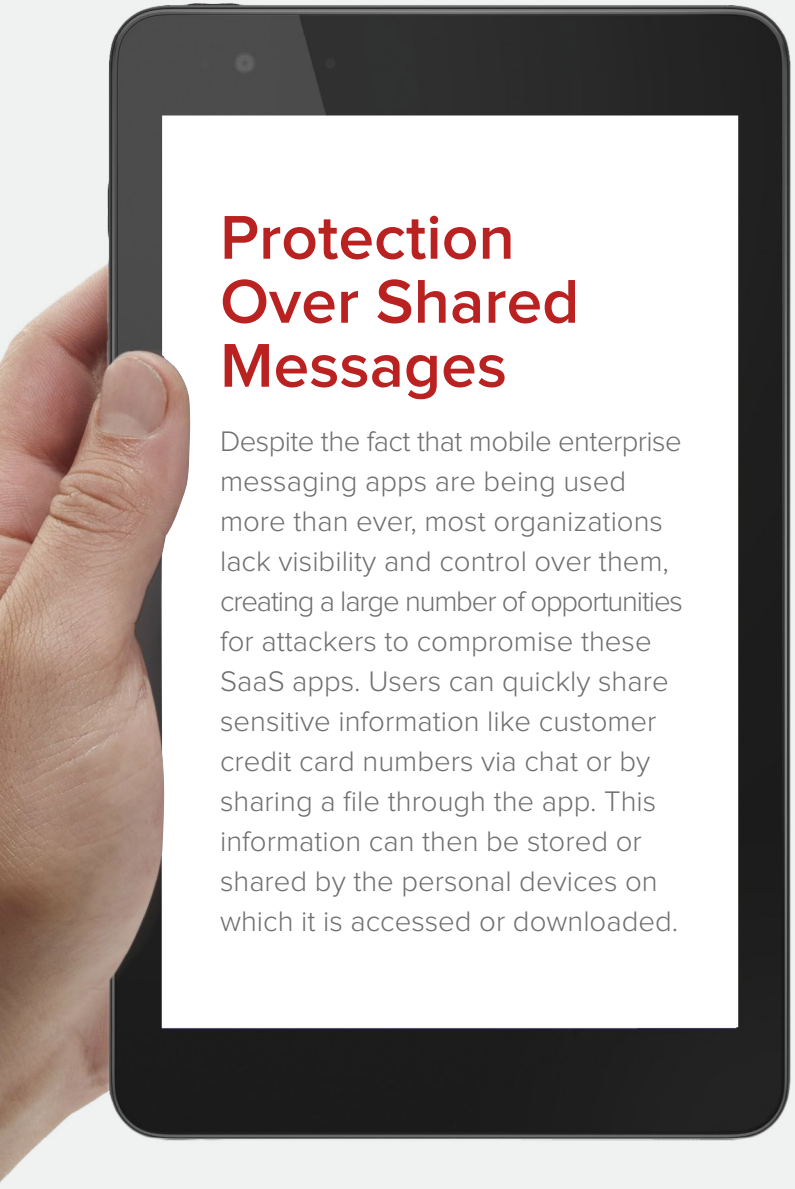


Visibility Over Applications in Use

Email, messaging, and file sharing apps are designed to enable sharing, making them prime examples of tools that can enable breaches and leakage if not properly secured. Presbyterian Healthcare Services, for example, had the protected health information (PHI) of 183,000 individuals exposed through an attack that targeted the email accounts of several employees. As email is a common attack vector, it must be secured on personal devices.

Do you have any visibility into the following applications on BYO devices?

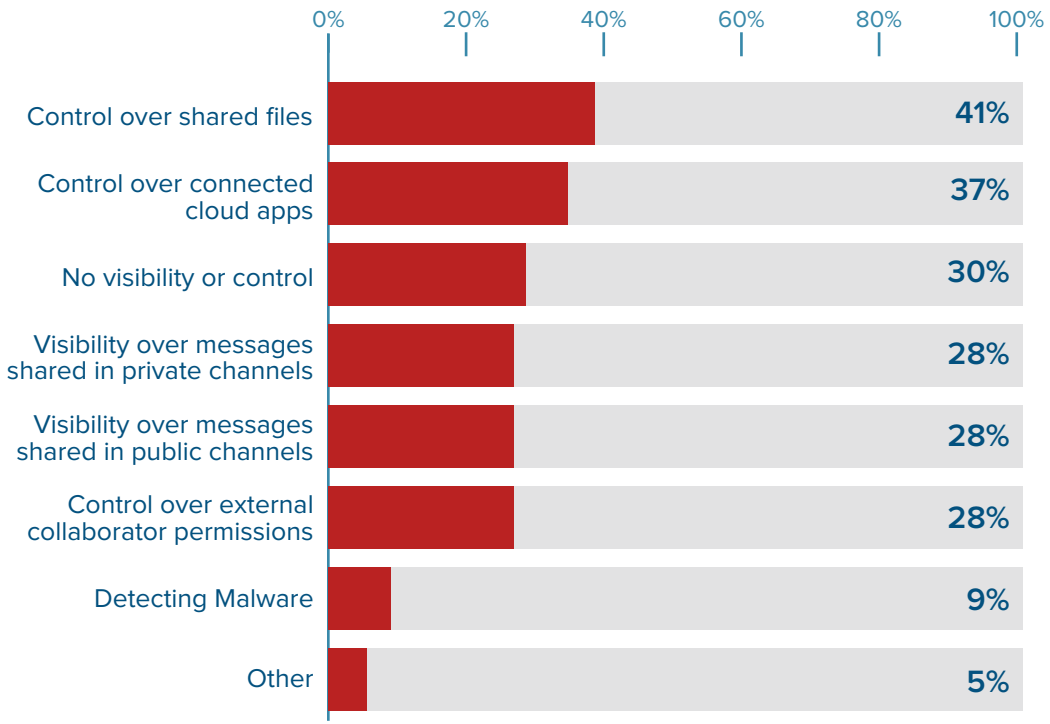




Protection Over Shared Messages

Despite the fact that mobile enterprise messaging apps are being used more than ever, most organizations lack visibility and control over them, creating a large number of opportunities for attackers to compromise these SaaS apps. Users can quickly share sensitive information like customer credit card numbers via chat or by sharing a file through the app. This information can then be stored or shared by the personal devices on which it is accessed or downloaded.

What security capabilities do you have in place for mobile enterprise messaging?

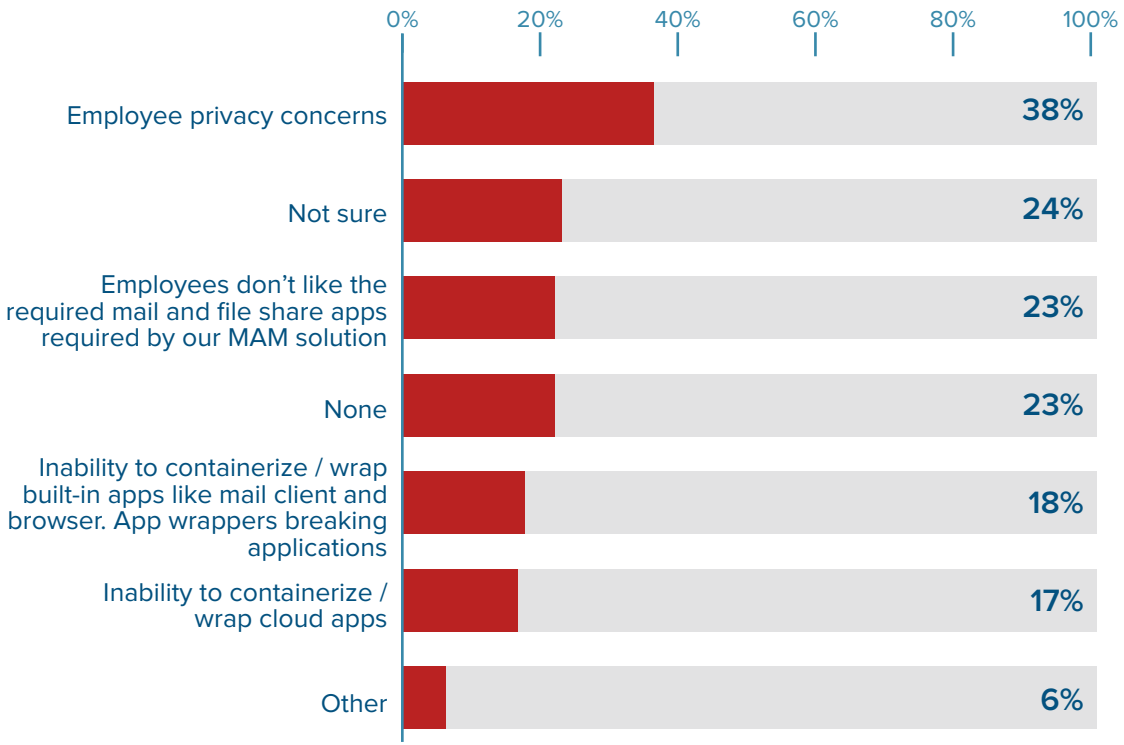


Mobile Device & Application Management

Even with the deployment and latency issues of mobile device management (MDM), it is the most common tool used to secure email on personal devices; however, many employees fear having their privacy invaded by MDM on their personal endpoints and resist installations. For the 24% of firms that don't secure email on BYO devices at all, data can easily be shared and downloaded by unauthorized parties.

MAM is challenging to use due to privacy and usability concerns, as well as the inability to wrap key apps. To secure BYOD, companies need security tools that respect privacy, provide a good user experience, and can secure data in any app. Flexibility and robust protections are both critical.

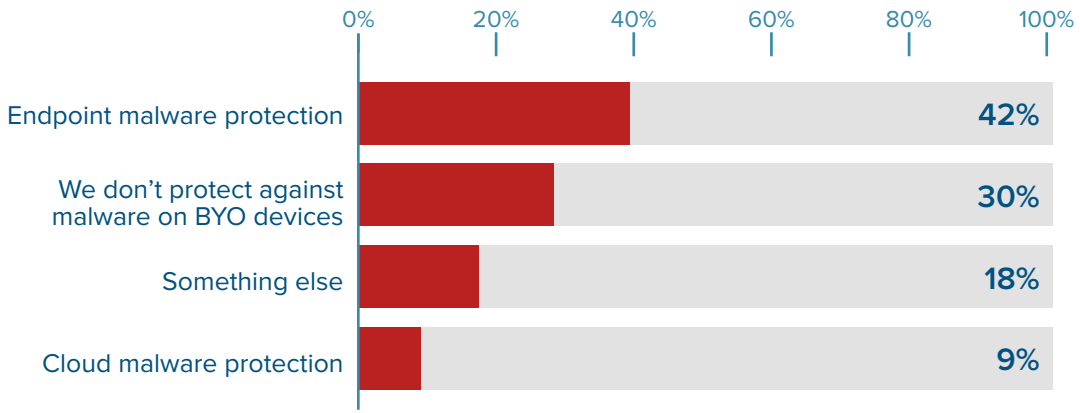
What challenges have you encountered with Mobile Application Management (MAM)?



Defense Strategy Against Malware

Due to the challenges of securing BYOD via endpoint software installations, the ideal solution is to leverage agentless or cloud-based tools that can keep threats from infiltrating companies via personal devices. Unfortunately, 72% of organizations either lack BYOD malware protection entirely or rely upon endpoint installations.

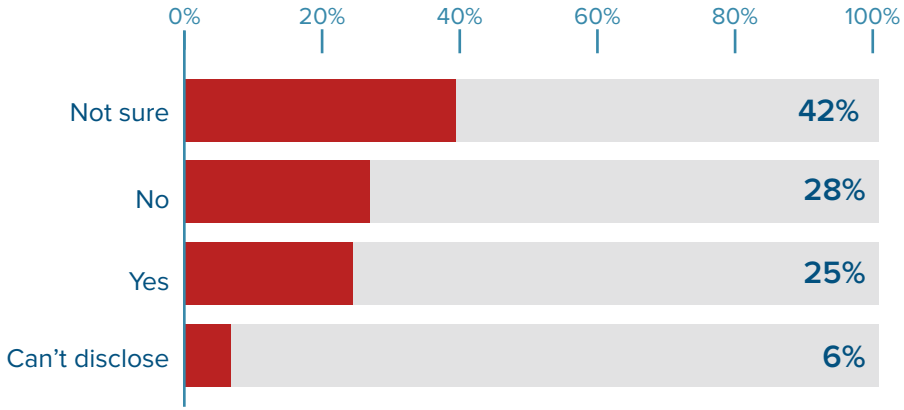
Which of the following do you use for malware protection on BYO devices?



Threats to BYOD Security

Only 28% of organizations were certain that their users hadn't downloaded malware over the last year. Malware, or ransomware like Petya and WannaCry, have brought organizations to their knees in recent years. Utilizing tools that provide advanced threat protection (ATP) is imperative for business success.

Have any of your BYO devices downloaded malware in the past 12 months?



Wrap-Up

The increases in mobility, productivity, and flexibility within an organization are some of the reasons why BYOD has been so widely adopted in today's cloud-first world. However, malicious actors are keen to take advantage of security loopholes, such as corporate data being accessed from unmanaged devices. In this report, the top BYOD security concerns for organizations were data leakage, lost and stolen devices, unsecured access, and malware. Fortunately, there are comprehensive security solutions capable of addressing these vulnerabilities.

- To prevent data leakage, organizations can enable data loss prevention (DLP) capabilities for data at rest, as well as data in transit—even when it is being accessed by personal endpoints.
- When it comes to protecting corporate data on lost and stolen personal devices, selective wipe can target and remove company information from users' devices without agents and without affecting personal data; full wipe can remove all content from a BYO device, but employees are typically wary about their privacy when full wipe is enabled.
- To ensure data is being accessed securely by authorized users only, IT personnel can utilize contextual access control, which governs access by factors like user group, location, and device type.
- For stopping malware infections, organizations should turn to agentless advanced threat protection (ATP) tools that leverage machine learning to identify and block zero-day threats at upload, at download, and at rest.

Phone: 408.337.0190
Email: info@bitglass.com

www.bitglass.com

About Bitglass

Bitglass, the Total Cloud Security 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.