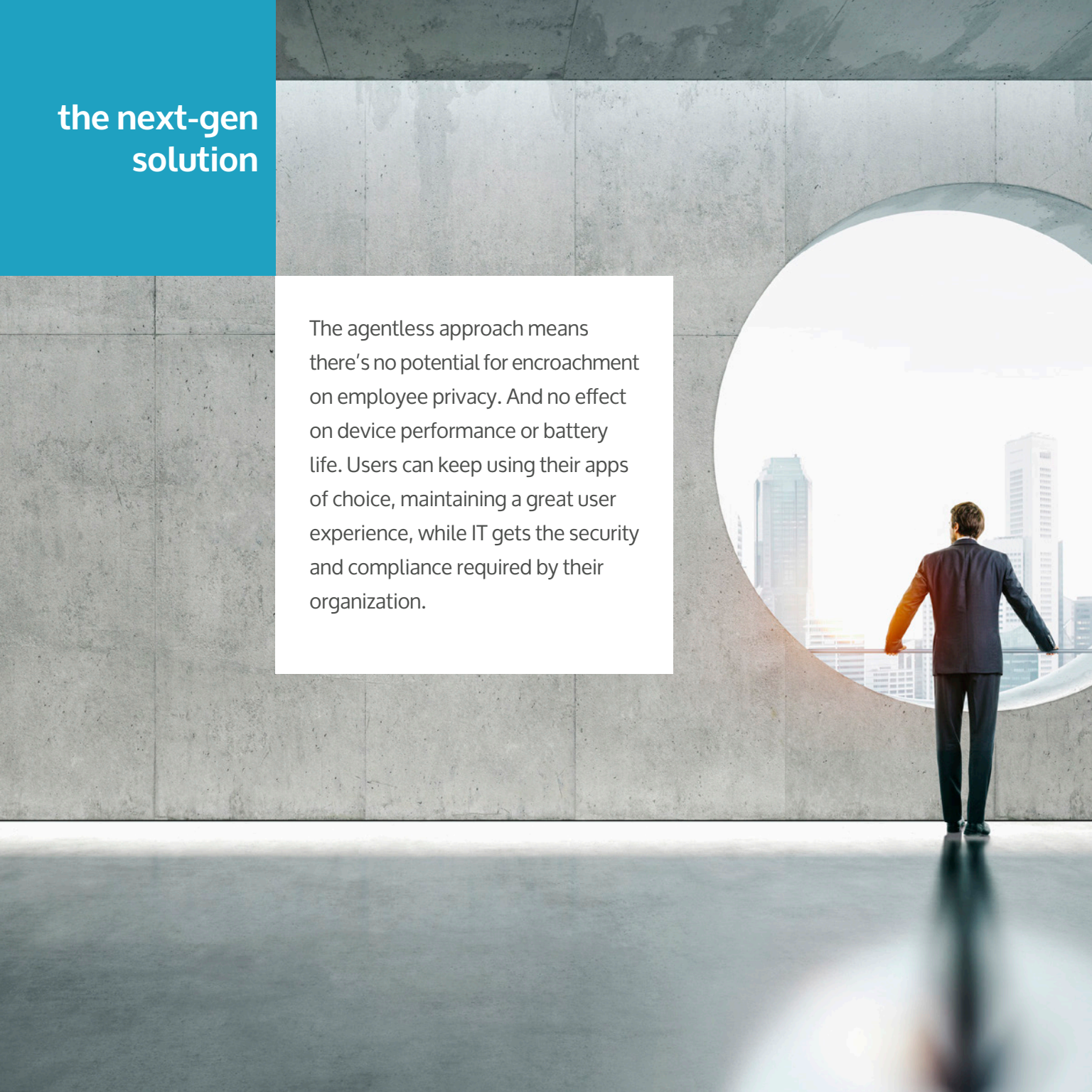
mobile
solution brief

bitglass

BYOD Security has been a constant challenge for many enterprises. Stories of failed MDM deployments are rampant, with firms struggling achieve meaningful adoption. According to the latest Bitglass BYOD security survey, one in three organizations have attempted to deploy an MDM solution, yet a massive 57 percent of employees refuse MDM for BYOD. The root cause of these failures is an attempt to manage and control devices that don't belong to the organization. The goal at the heart of any BYOD security program is to secure corporate data on devices, not the devices themselves. Bitglass takes a fundamentally different approach to mobile security, one that employs a proactive, data-centric security posture. Bitglass provides an agentless BYOD security solution that is a lightweight yet powerful alternative to MDM.

the next-gen solution

The agentless approach means there's no potential for encroachment on employee privacy. And no effect on device performance or battery life. Users can keep using their apps of choice, maintaining a great user experience, while IT gets the security and compliance required by their organization.

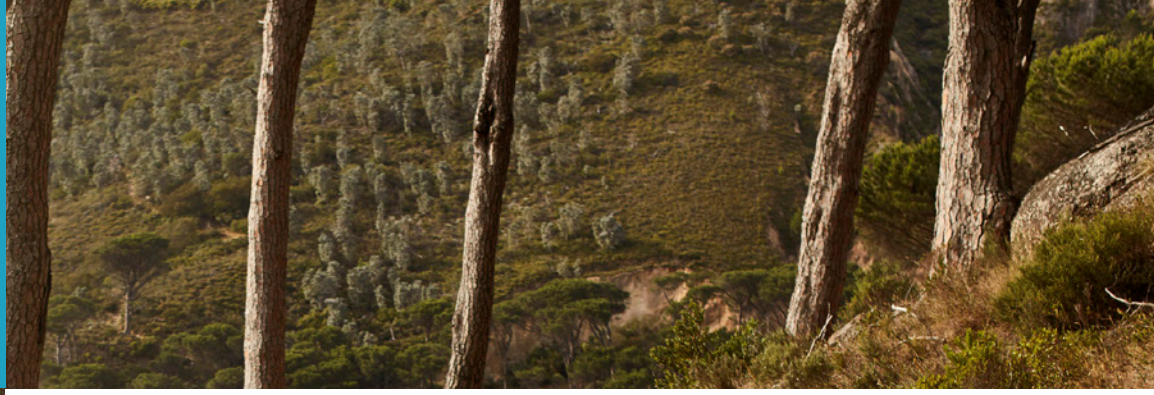


the future of secure mobility

Bitglass enables IT teams reduce the threat surface by controlling the flow of high-risk data to devices via DLP and access control, and protect data once it's on the device through data-centric controls such as rights management and encryption. Admins can use prebuilt or custom policies to prevent sensitive data from download or sync to BYOD. For example, customer PII or PHI in a spreadsheet can be redacted dynamically from an email downloaded on a mobile device. Or if per policy an email is deemed too sensitive to be viewed on a mobile device, it can be blocked with a warning message in its place.

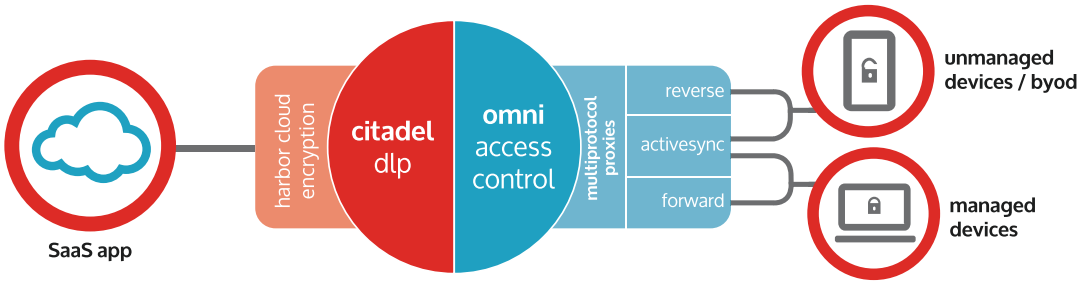
Essential security policies, including PIN codes and device encryption, are enforced across Android, iOS, and Windows mobile devices. For lost, stolen, or deprovisioned mobile devices, Bitglass enables the selective wiping of corporate data, without affecting users' personal data. This frees companies from potential liability concerns posed by a full device wipe, which is commonly employed by EMM vendors.

frictionless deployment

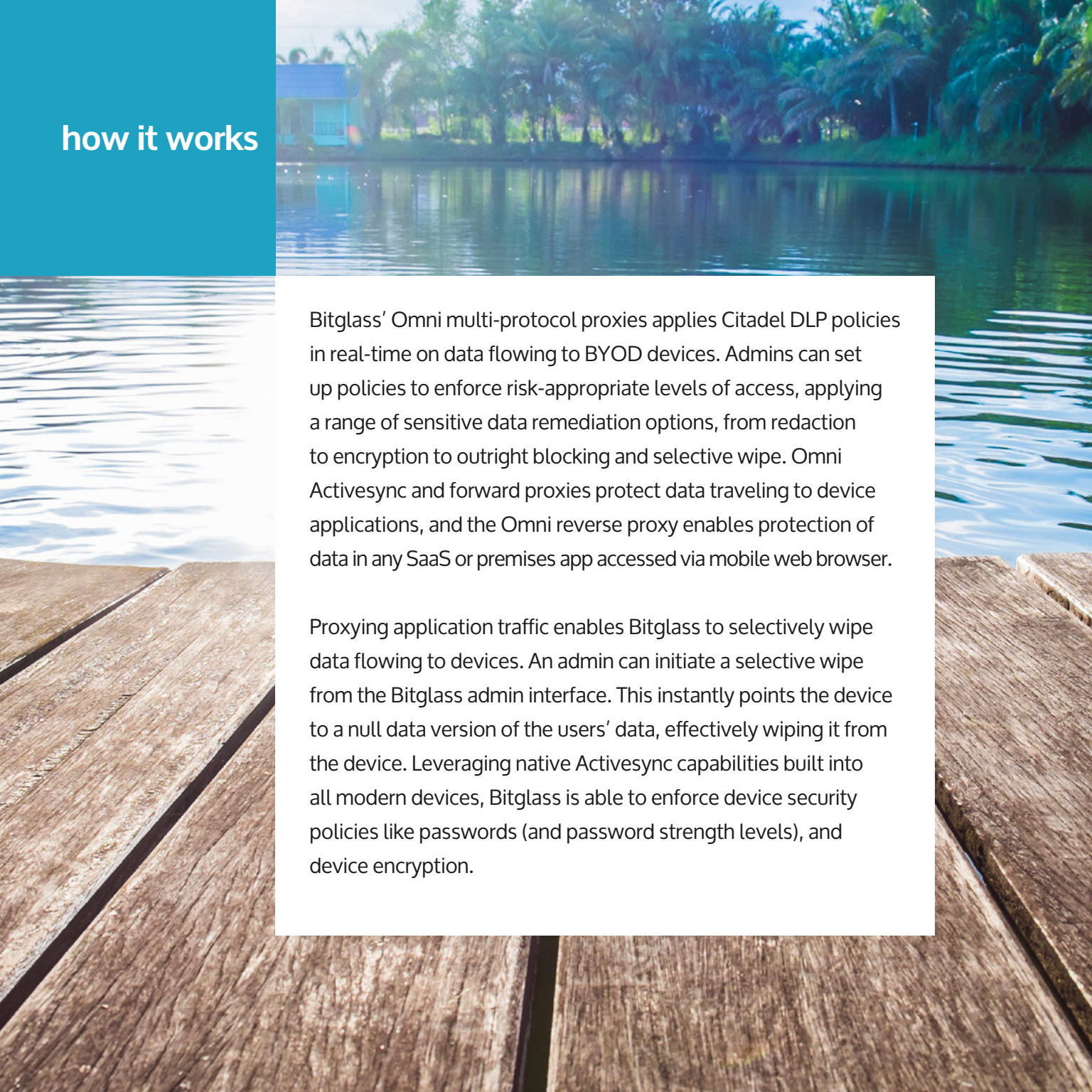


Bitglass eliminates the biggest barrier to any BYOD security program: deployment. For both admins and end users alike, setting up Bitglass takes just minutes—dramatically reducing the timeline for security program rollout.

Users don't need to install anything. They simply authenticate to their apps and the apps are automatically configured to communicate with the Bitglass service. Bitglass' service is completely cloud-based, with no software to install and minimal configuration overhead for admins.



how it works



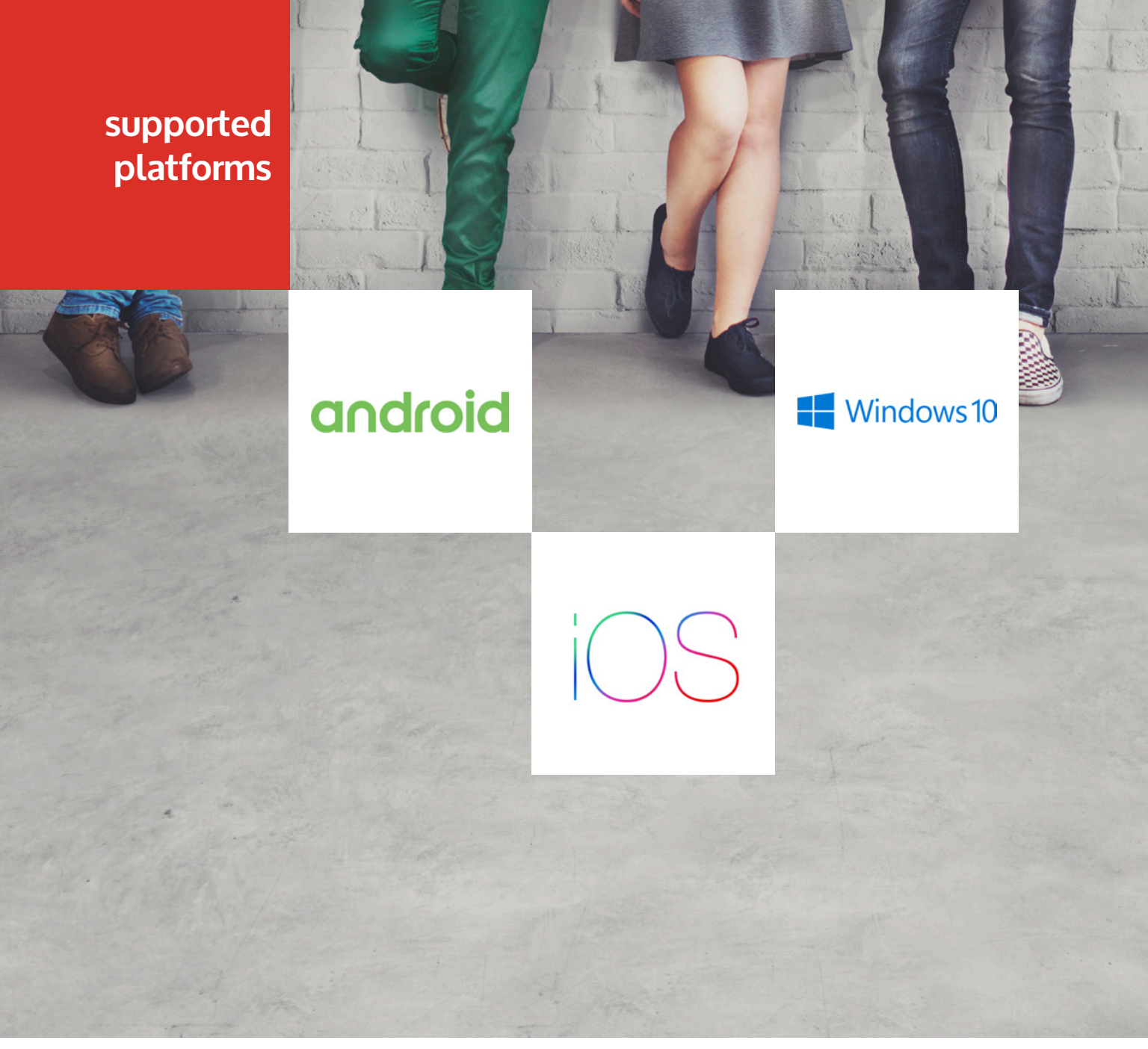
Bitglass' Omni multi-protocol proxies applies Citadel DLP policies in real-time on data flowing to BYOD devices. Admins can set up policies to enforce risk-appropriate levels of access, applying a range of sensitive data remediation options, from redaction to encryption to outright blocking and selective wipe. Omni Activesync and forward proxies protect data traveling to device applications, and the Omni reverse proxy enables protection of data in any SaaS or premises app accessed via mobile web browser.

Proxying application traffic enables Bitglass to selectively wipe data flowing to devices. An admin can initiate a selective wipe from the Bitglass admin interface. This instantly points the device to a null data version of the users' data, effectively wiping it from the device. Leveraging native Activesync capabilities built into all modern devices, Bitglass is able to enforce device security policies like passwords (and password strength levels), and device encryption.

bitglass vs. MDM

	bitglass	MDM
Device management policy	X	X
Selective wipe	X	X
Full wipe	X	X
Data security for internally developed apps	X	X
Data security for native mobile apps	X	X
Data security for native email/PIM on any device	X	
Data security for third party/SaaS vendor mobile apps	X	
Data leakage prevention	X	
Visibility for compliance and governance	X	
App store for in-house apps		X
Certificate management for email, WIFI, VPN		X

supported platforms



For more information, visit www.bitglass.com

bitglass