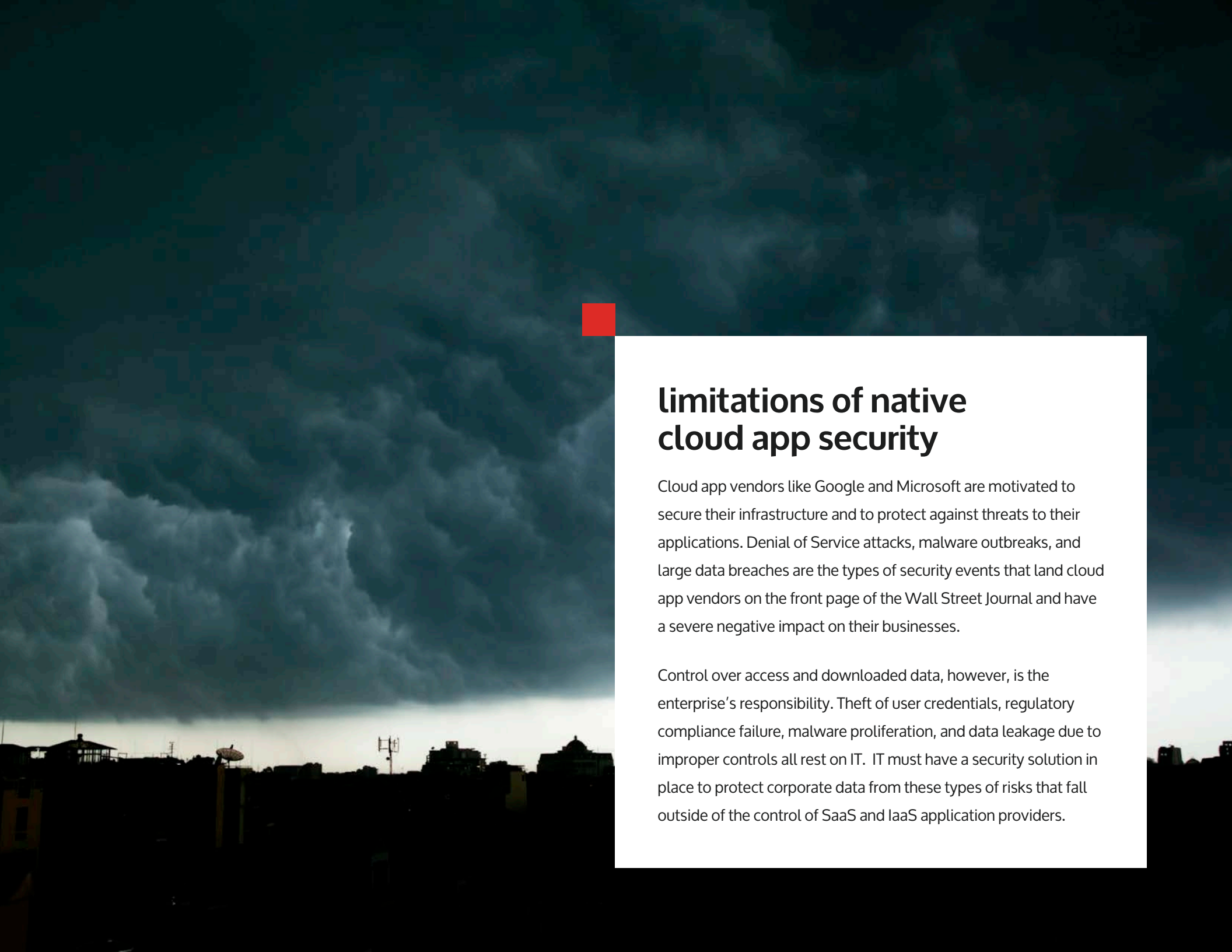
the definitive guide to cloud access security brokers

bitglass

Cloud apps like Office 365, Salesforce, and Amazon Web Services (AWS), have enjoyed unprecedented mainstream adoption in the enterprise, yet security concerns continue to plague public cloud adoption. Many organizations are eager to migrate to the cloud, but need visibility and control to keep sensitive corporate data safe. In order to secure cloud apps, organizations need a comprehensive security solution that offers visibility, data security, threat protection, and compliance.

Cloud access security brokers (CASBs) are a data-centric solution for securing both SaaS apps and IaaS platforms, end-to-end, from cloud to device. By intermediating or "proxying" traffic between cloud apps and end-user devices, CASBs offer IT administrators granular access control and deep visibility over corporate data—critical for organizations moving from internal, premises-based apps to the cloud.

> "The forces of cloud and mobility fundamentally change how "packets" (and the transactions and data they represent) move between users and applications. This causes a need to adjust the list and the priorities of investment in security controls for any organization that is consuming cloud services. [By 2020] 85% of large enterprises will use a cloud access security broker platform for their cloud services, which is up from less than 5% today."
>
> **—Craig Lawson, Neil MacDonald, Brian Lowans and Brian Reed, Gartner.**



limitations of native cloud app security

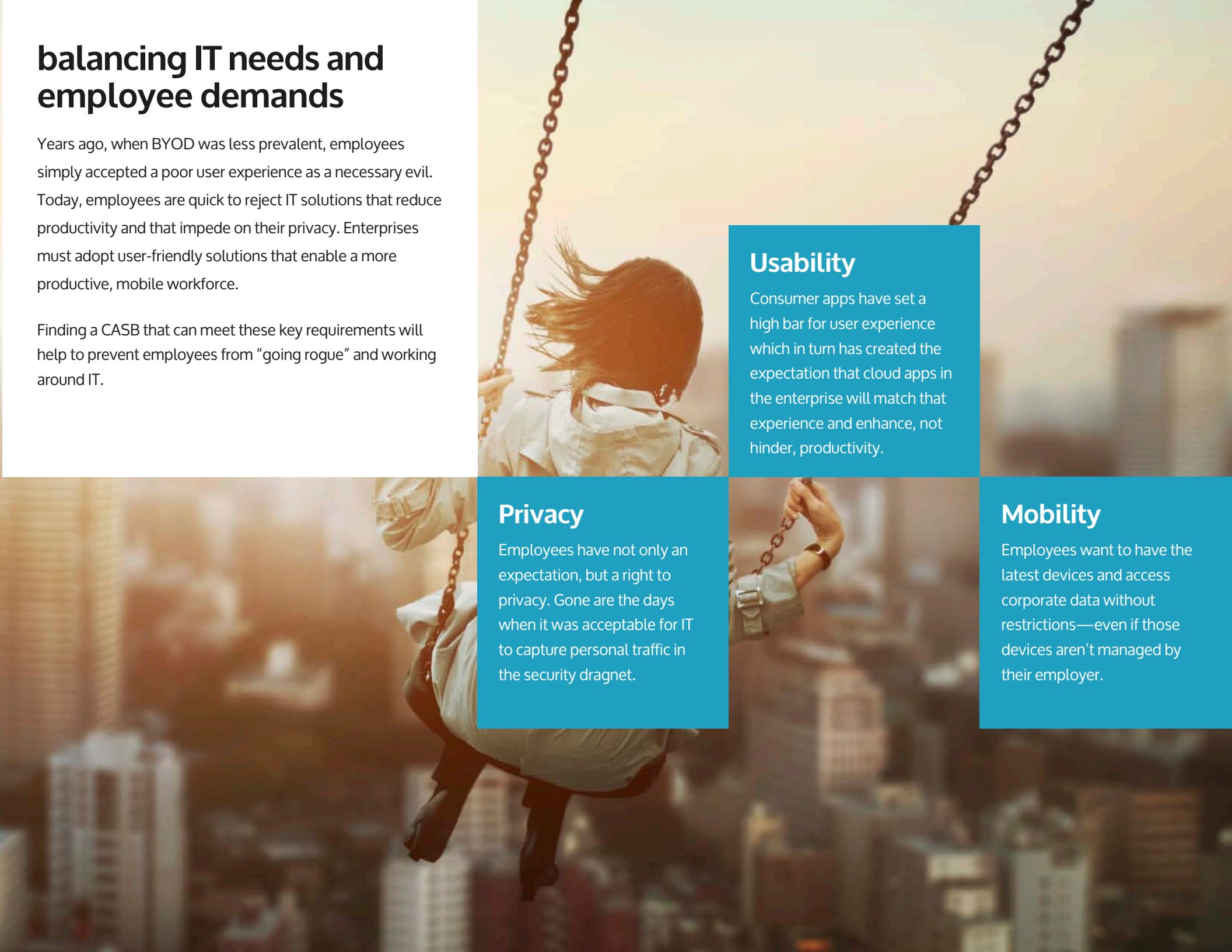
Cloud app vendors like Google and Microsoft are motivated to secure their infrastructure and to protect against threats to their applications. Denial of Service attacks, malware outbreaks, and large data breaches are the types of security events that land cloud app vendors on the front page of the Wall Street Journal and have a severe negative impact on their businesses.

Control over access and downloaded data, however, is the enterprise's responsibility. Theft of user credentials, regulatory compliance failure, malware proliferation, and data leakage due to improper controls all rest on IT. IT must have a security solution in place to protect corporate data from these types of risks that fall outside of the control of SaaS and IaaS application providers.

balancing IT needs and employee demands

Years ago, when BYOD was less prevalent, employees simply accepted a poor user experience as a necessary evil. Today, employees are quick to reject IT solutions that reduce productivity and that impede on their privacy. Enterprises must adopt user-friendly solutions that enable a more productive, mobile workforce.

Finding a CASB that can meet these key requirements will help to prevent employees from "going rogue" and working around IT.



Usability

Consumer apps have set a high bar for user experience which in turn has created the expectation that cloud apps in the enterprise will match that experience and enhance, not hinder, productivity.

Privacy

Employees have not only an expectation, but a right to privacy. Gone are the days when it was acceptable for IT to capture personal traffic in the security dragnet.

Mobility

Employees want to have the latest devices and access corporate data without restrictions—even if those devices aren't managed by their employer.

CASB data protection and visibility

While enabling mobility is often a boon to productivity, cloud apps also make data access much easier, which can pose a threat to security. A complete CASB must close the gap by protecting data-at-rest and data-in-motion end-to-end, from cloud to device. Leveraging both inline proxies and API integration into cloud apps, CASBs provide several data protection and visibility functions.

identity

discovery

mobile

cloud

cloud

Real-time, inline data protection.

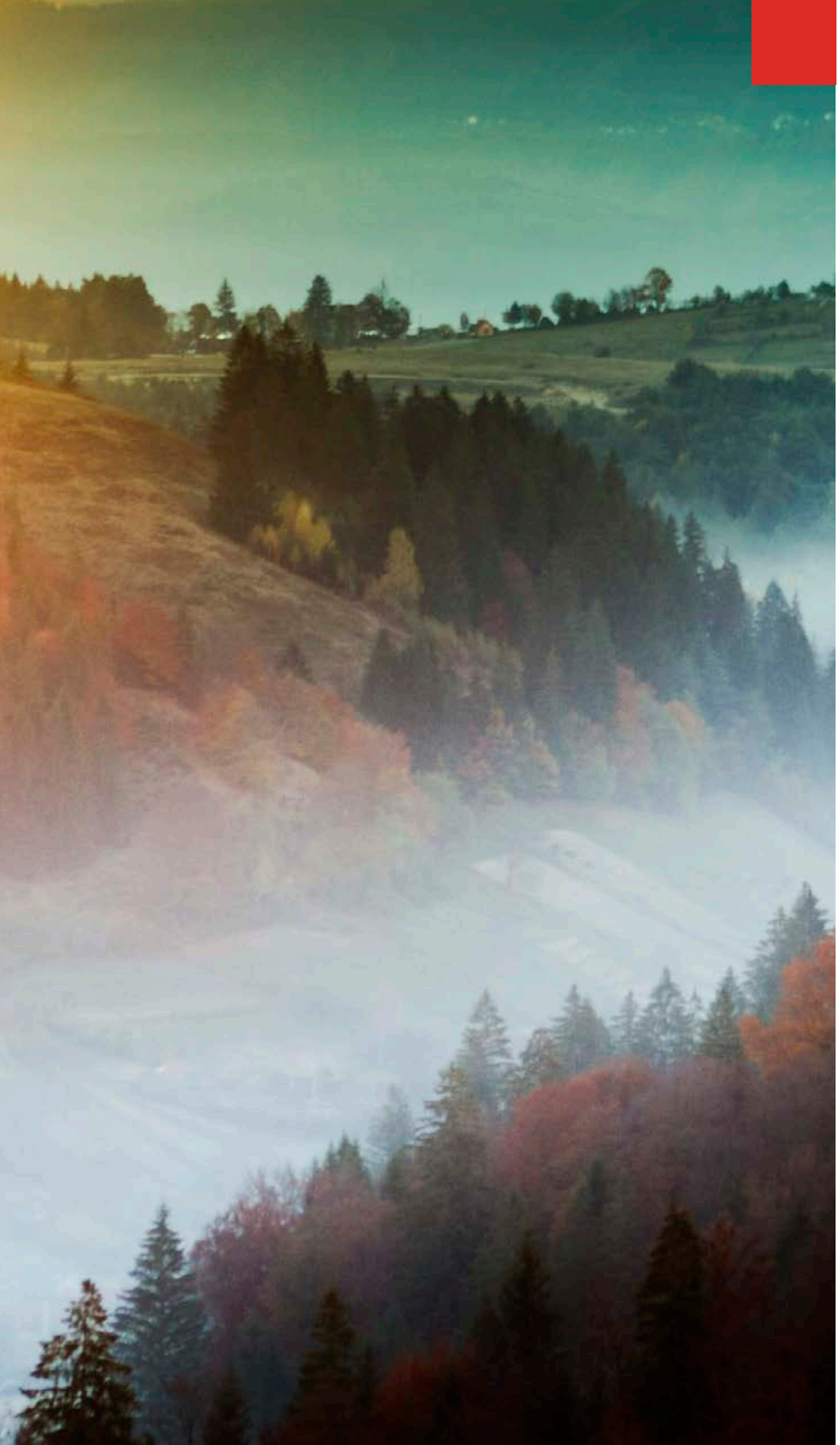
"Jim" logs into Salesforce from San Francisco and into Box from New York simultaneously. Alone, these two events may appear normal, but together they suggest the occurrence of a breach. The CASB might be configured to either notify administrators or force re-authentication on both devices with a SMS one-time password to identify and block the inappropriate use of Jim's credentials.

Visibility

Suppose "Jim" logs into Salesforce from San Francisco and into Box from New York simultaneously. Alone, these two events may appear normal, but together they suggest the occurrence of a credential compromise. The CASB might be configured to either notify administrators or force re-authentication on both devices with a SMS one-time password to identify and block the inappropriate use of Jim's credentials.

CASBs provide visibility that ranges from detailed, audit-level logging to suspicious activity detection and user behavior analytics. A deep understanding of how employees are using cloud apps is key to identifying risky or malicious activity. By tracking user activities, CASBs can generate a baseline behavioral profile, and alert on deviations so that IT can take immediate action. Visibility can also help IT build security policies that minimize risk of data loss without impeding on employee workflows, such as re-authenticating with two factor authentication when possible credential compromise is detected.

CASBs also provide a wealth of detailed, audit-level logging, providing information on all cloud app transactions, including downloads, logins, usage, and application specific behaviors like downloading a contact database in Salesforce or sharing a file externally through Box. CASBs typically generate logs in human readable form with search and filter functionality, and integrate seamlessly with SIEMs and other security operations tools and workflows.



Contextual Access Control

Contextual Access Control in a CASB governs the context by which a user is accessing cloud app(s). Policies can be defined based on access method (browser or native app), device (managed vs unmanaged), location (by country or IP address range), group, and more.

Policy options typically allow your organization to block, allow, or provide intermediate levels of access to apps and sensitive data by pairing access control policies with DLP policies.

Data Leakage Prevention

Say employee "John" uploads a file containing sensitive customer data to Office 365 OneDrive. John then shares the file externally to someone outside of the company. A CASB will identify this suspicious external share and quarantine for review by IT or by the user's manager. Once the external share is approved as legitimate, the file is released from quarantine and the share is enabled.

CASBs protect corporate data both in the cloud and on any device in real-time. API integration into cloud apps is used to scan and protect data-at-rest, and proxies are used for inline, real-time protection for data being accessed via both managed and unmanaged devices.

Using built-in APIs, CASBs are able to scan and identify sensitive content stored in apps like Office 365 and Google Apps, and apply granular access controls to data. With traditional solutions, access control capabilities are limited and IT is forced to simply allow or block access. With a CASB IT administrators have more flexibility in extending access with context- and content-aware Data Leakage Prevention policies.

Policy actions range from lightweight visibility to outright blocking. A lightweight CASB action might be to allow data to be downloaded, but with encryption, rights management, or tracking watermarks applied to the file. More aggressive actions include redacting sensitive content or blocking a file from download altogether. Aggressive actions are particularly useful when identified as risky, such as an attempt to download thousands of credit card numbers to a BYOD laptop. Every organization must make judgments and create policies around what protections and limits to apply based on their needs.

Say employee "John" uploads a file containing sensitive customer data to Office 365 OneDrive. John then shares the file externally to someone outside of the company. A CASB will identify this suspicious external share and quarantine for review by IT or by the user's manager. Once the external share is approved as legitimate, the file is released from quarantine and the share is enabled.

Cloud Encryption

By encrypting cloud data, your organization can enjoy the productivity benefits of the public cloud, while maintaining private cloud security. CASBs offer support for both field-level encryption, for structured data applications like Salesforce and file-level encryption, for any cloud application, including file sharing applications. In both cases, data is encrypted before upload to the cloud, and decrypted for consumption only when authorized by policy. CASBs typically offer their own "native" key management solution, but a more common deployment method is to integrate with your existing premises or cloud key management systems, typically via the KMIP protocol.

The biggest challenge with providing cloud encryption is encrypting at full strength, while simultaneously preserving key application functionality, such as search and sort. Ensure that your CASB is leveraging industry standard encryption, such as 256-bit AES with 256-bit initialization vectors. Proprietary and/or weakened encryption schemes provide very little in the way of security.

Threat and Malware Scanning

As cloud apps increase in popularity, their attractiveness to bad actors increases, making them a more popular delivery vehicle for malware. Many CASBs are now incorporating malware detection into their platforms, enabling scanning of data upon upload/download via proxy, as well as data-at-rest scanning via API. As with endpoint protection suites, not all anti-malware is the same. Integrations range from traditional signature or hash-based malware detection to next generation artificial intelligence based scanning for both known and unknown threats.

mobile

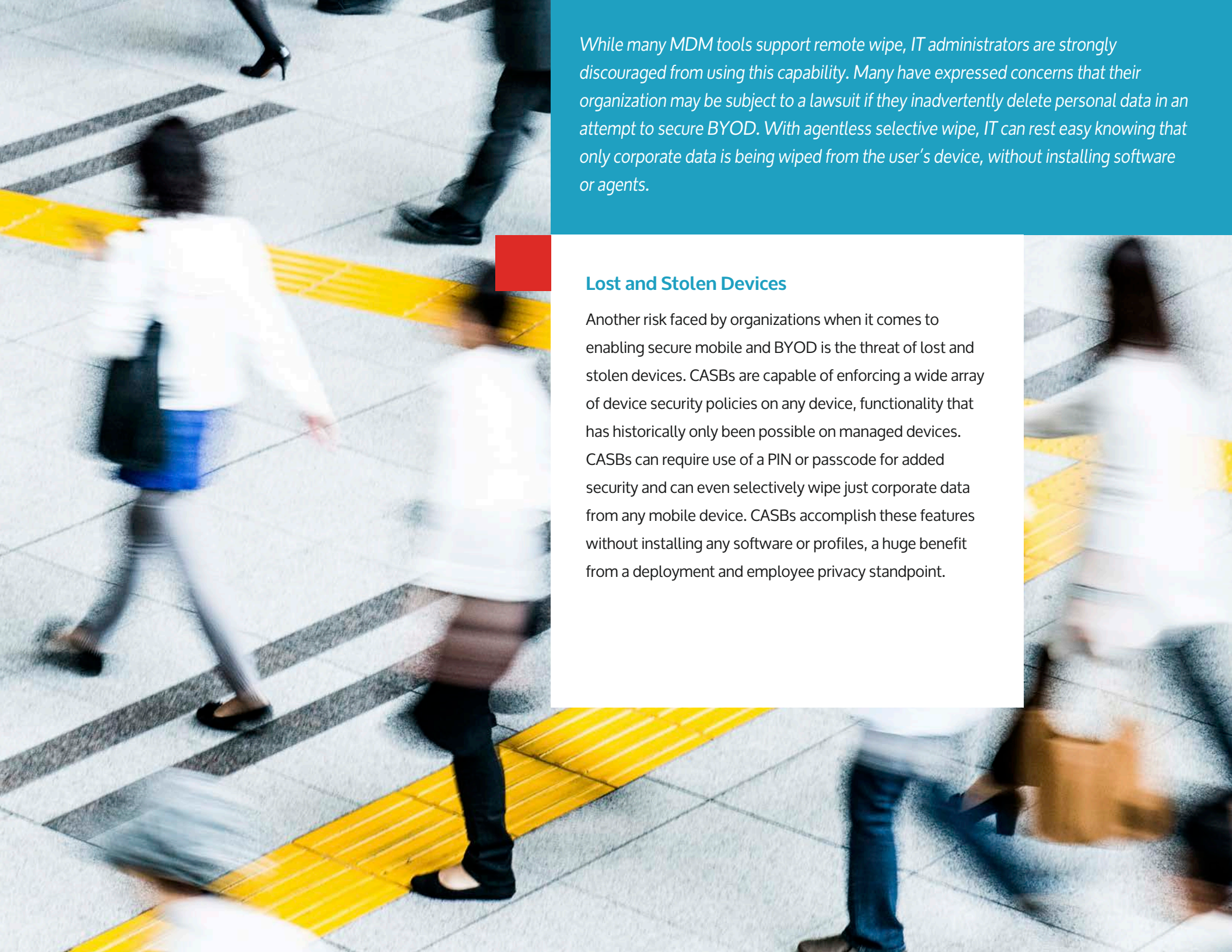
Secure BYOD with data-centric controls.

"Jane" downloads sensitive data to a BYOD device and access to that data is required as part of her job. A CASB can apply rights management to the file upon download, which provides access to the data in a secure fashion by requiring authentication to view the encrypted file. Jane can "check out" the file for offline access, but even if she leaves the company or forwards the file to someone outside the company, IT can continue to control access.

Data Leakage

When organizations focus entirely on securing devices instead of securing data, there is a real threat of data leakage. An employee can, for example, download a file with sensitive customer information to a managed device, move that file over to an unmanaged device, and perhaps upload that file to an unsanctioned cloud application. If the device were secured without other data-centric protections, IT would lose visibility and control over that file.

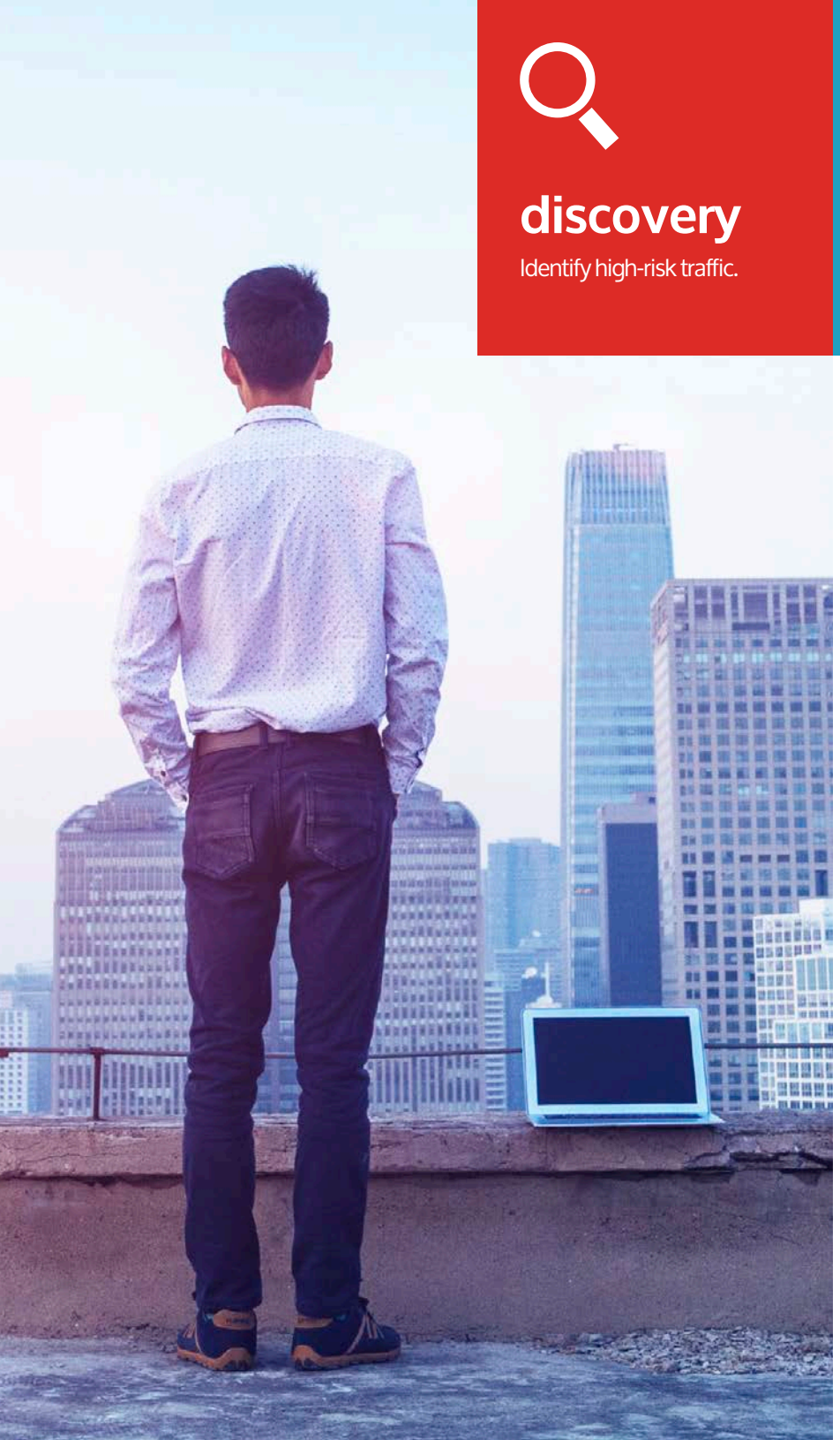
With a CASB, a content-aware DLP engine can encrypt, DRM, and watermark data in real time, ensuring that sensitive information stays protected across both managed and unmanaged devices.



While many MDM tools support remote wipe, IT administrators are strongly discouraged from using this capability. Many have expressed concerns that their organization may be subject to a lawsuit if they inadvertently delete personal data in an attempt to secure BYOD. With agentless selective wipe, IT can rest easy knowing that only corporate data is being wiped from the user's device, without installing software or agents.

Lost and Stolen Devices

Another risk faced by organizations when it comes to enabling secure mobile and BYOD is the threat of lost and stolen devices. CASBs are capable of enforcing a wide array of device security policies on any device, functionality that has historically only been possible on managed devices. CASBs can require use of a PIN or passcode for added security and can even selectively wipe just corporate data from any mobile device. CASBs accomplish these features without installing any software or profiles, a huge benefit from a deployment and employee privacy standpoint.



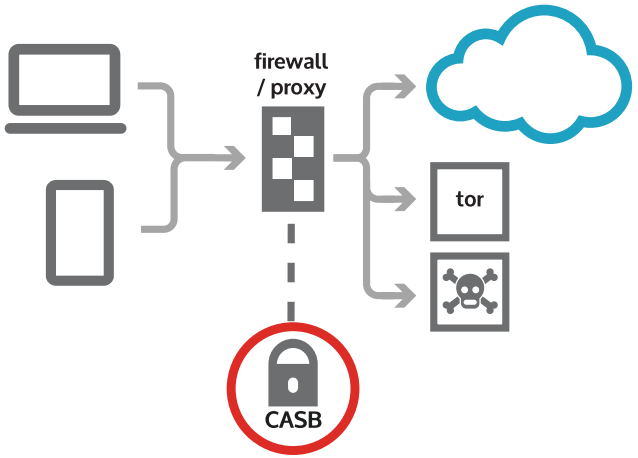
discovery

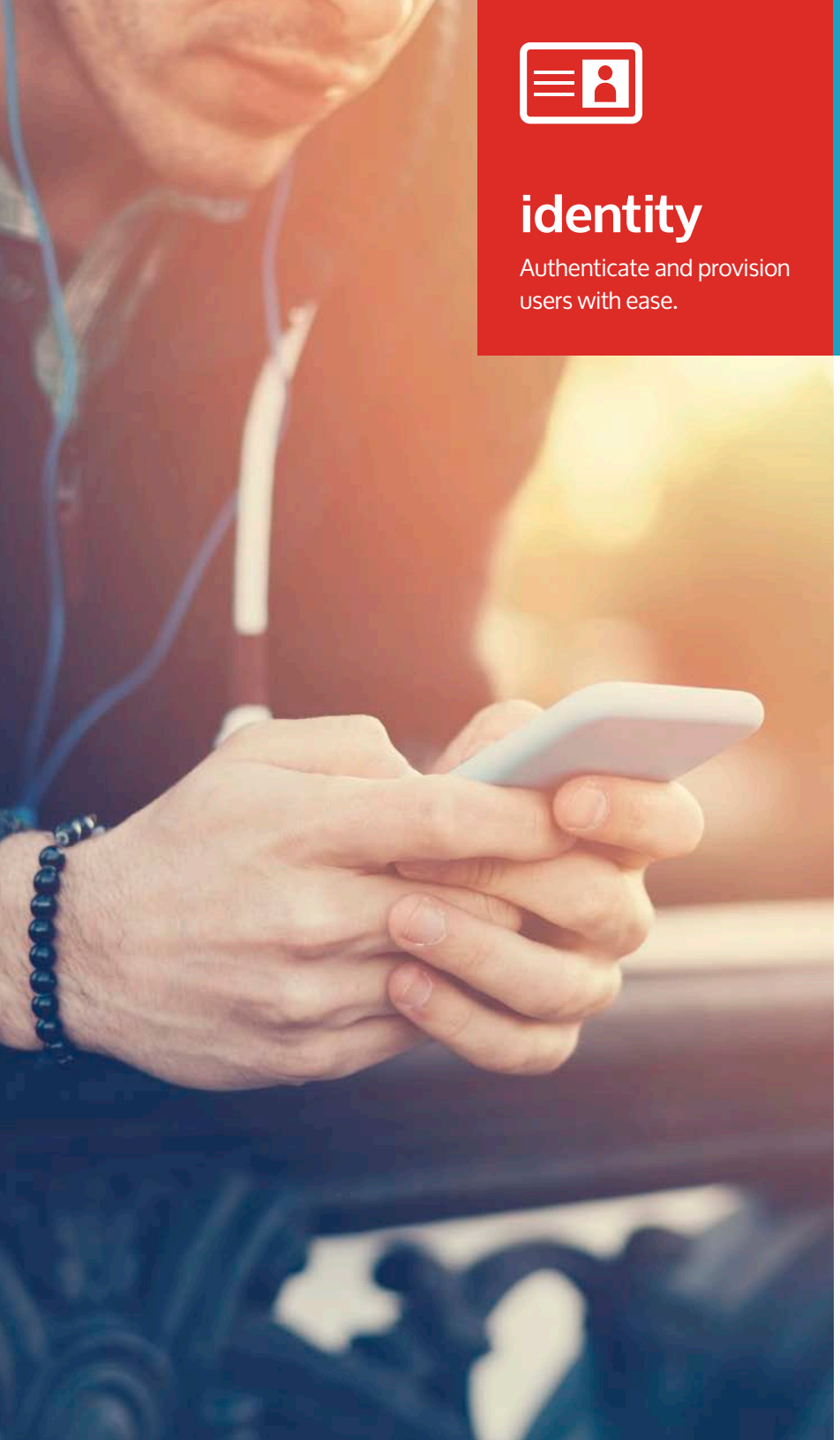
Identify high-risk traffic.

Imagine employee "Olivia" uploads a file to an unsanctioned cloud app, the typical Shadow IT problem. That one action isn't necessarily malicious and likely isn't indicative of a breach. However, if that same transaction occurred immediately after the device contacted a known malware command & control server, it may be an indicator of a data breach. CASBs can correlate across multiple events to quickly identify potential breaches and malicious activity based on the relative risks posed by different cloud apps.

Data leaving the corporate network and heading to high-risk destinations is a major concern for enterprises. High-risk destinations take many forms - malware command and control sites, anonymizers like Tor, unsanctioned "shadow IT" cloud applications, and more. Each of these destinations represents a threat of sensitive data exfiltration and must be identified in a timely fashion.

CASBs offer discovery services that analyze proxy or firewall data to identify vulnerable traffic between the network and high-risk destinations. Destinations associated with known malicious activity can be identified in order to remediate high risk endpoints and users. Unsanctioned shadow IT cloud applications are classified according to risk, allowing you to decide what to allow, what to block, and what to safely enable through a CASB proxy service. While blocking an unsanctioned cloud app may sound like an attractive solution, employees can often find an unrestricted network that allows use of that app, hence the importance of a data-centric approach to threat protection.





identity

Authenticate and provision users with ease.

Employee "Bob" typically logs in from his managed corporate laptop inside of the corporate network and uses a password. Over the weekend, Bob gets a new smartphone and decides to log in to one or more cloud apps from that device. The CASB will recognize the device and take Bob through additional authentication steps in order to validate that the new device actually belongs to Bob.

In many organizations, individual accounts are created within each cloud app, without a centralized identity system—a practice that can make provisioning new accounts and securely authenticating users more difficult.

A complete CASB features an integrated identity management solution or works with an existing identity management infrastructure to enable secure authentication across all cloud apps. An integrated CASB solution provides reduced operational overhead and reduced cost vs integrating separate standalone components.

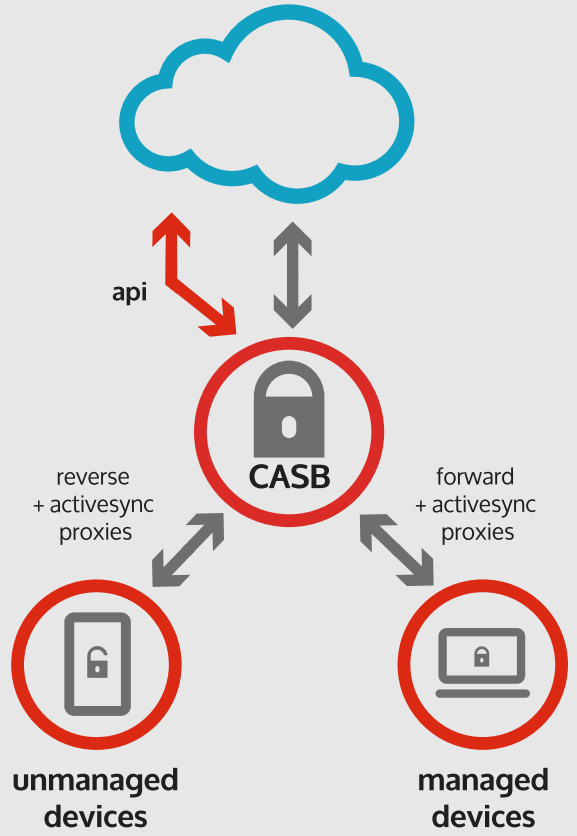
Secure authentication, often necessary to achieve regulatory compliance, can drastically reduce the attack surface that hackers can use to access corporate data. Organizations can also opt to employ more secure means of authentication for suspicious logins. Multi-factor auth, for example, requires both a user's password and access to the user's physical token.

The benefits of improved identity management are manifold - by deploying single sign-on, employees have just one password to remember and IT can provision new users with ease.

CASB technology

CASB architectures vary from one vendor to the next. Most vendors have a primary proxy mechanism upon which their architecture is built - either a forward proxy or a reverse proxy, supported by API integration into cloud applications for scanning data at rest. Proxies enable real-time, inline control. APIs, while not real-time, enable control over backend functions like external sharing and data-at-rest scanning. It is important to consider how each architecture is deployed and managed, as it can have a large impact on the supported applications and devices, and on the amount of operational overhead associated with managing the system.

Also keep in mind that web traffic is only one piece of the puzzle. Cloud-based productivity suites like Office 365 can be accessed via the web, but also via Microsoft Outlook, various OneDrive apps, and on any device that supports ActiveSync. A complete CASB must be capable of securing both web and mobile access.



reverse proxy

CASBs use reverse proxies to enable data security on unmanaged devices. The reverse proxy capability is also incredibly simple to deploy and use. No configuration is required on end-user devices—employees can simply log into the cloud app as they normally would and are automatically routed through the proxy.

While not applicable to client-server apps with hard-coded hostnames, the reverse proxy can be used to secure access to any cloud app from any device or network. Notably, only corporate traffic is sent via proxy, a benefit from an employee privacy perspective.

activesync proxy

CASBs that leverage ActiveSync proxies allow users to securely access corporate data in native apps. In fact, the most frequently used apps for work on mobile are mail, contacts, and calendar, all accessible via ActiveSync, critical for organizations deploying Office 365 or G Suite. End users need simply to log into their native mail or calendar app as they normally would. From an IT perspective, this provides a great user experience, enabling BYOD adoption, while maintaining the same visibility and control over data made possible by reverse and forward proxies.

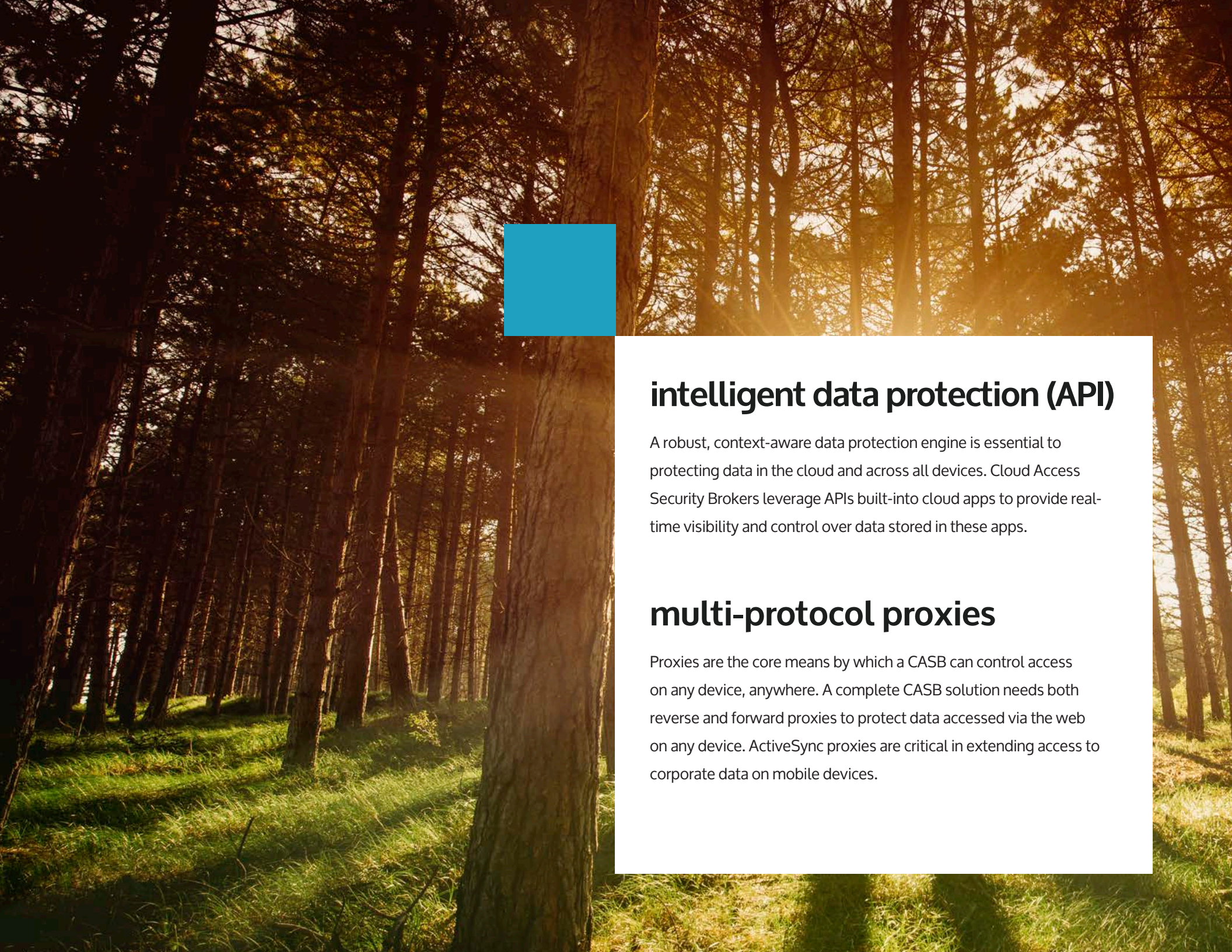
ActiveSync is also capable of device security capabilities generally associated with mobile device management tools, but without any agents, profiles, or certificates on the end-user's unmanaged device.

forward proxy

A forward proxy, while capable of securing traffic from all application types, including client-server apps with hard-coded hostnames, can be difficult to deploy and impedes on user privacy.

When deploying a forward proxy for cloud applications, the IT administrator must ensure that every firewall or browser through which the application may be accessed is configured to proxy the traffic for the cloud applications. This requires modifying proxy settings on user devices and firewalls across the company.

Since the proxy terminates and inspects SSL traffic for application domains owned by third parties, the proxy must also carry self-signed digital certificates that masquerade as the original domain. For example, a forward proxy that handles salesforce.com must masquerade as salesforce.com via a self-signed digital certificate for salesforce.com. Any browser used to access the application must also install and accept such a self-signed digital certificate.

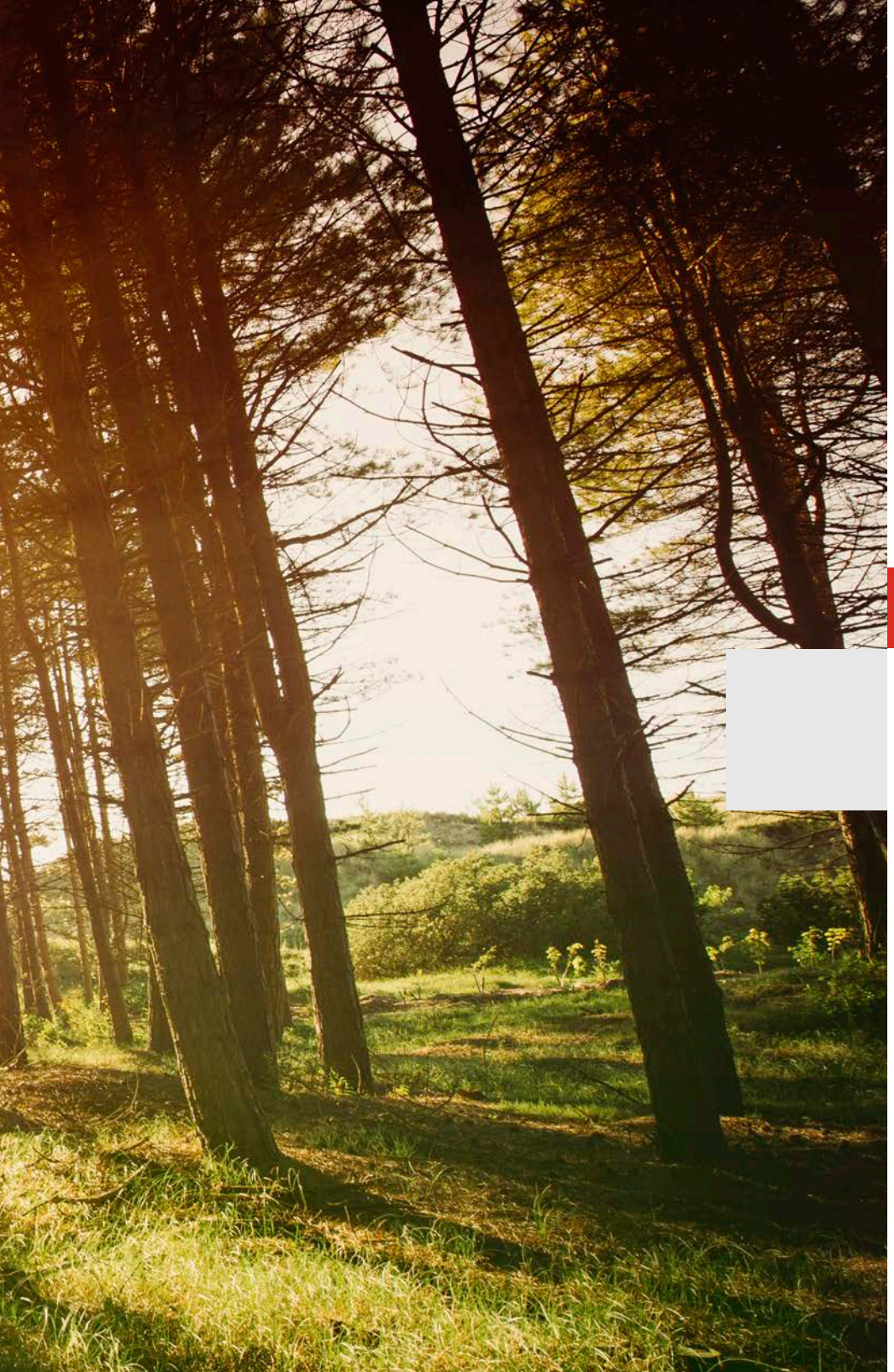


intelligent data protection (API)

A robust, context-aware data protection engine is essential to protecting data in the cloud and across all devices. Cloud Access Security Brokers leverage APIs built-into cloud apps to provide real-time visibility and control over data stored in these apps.

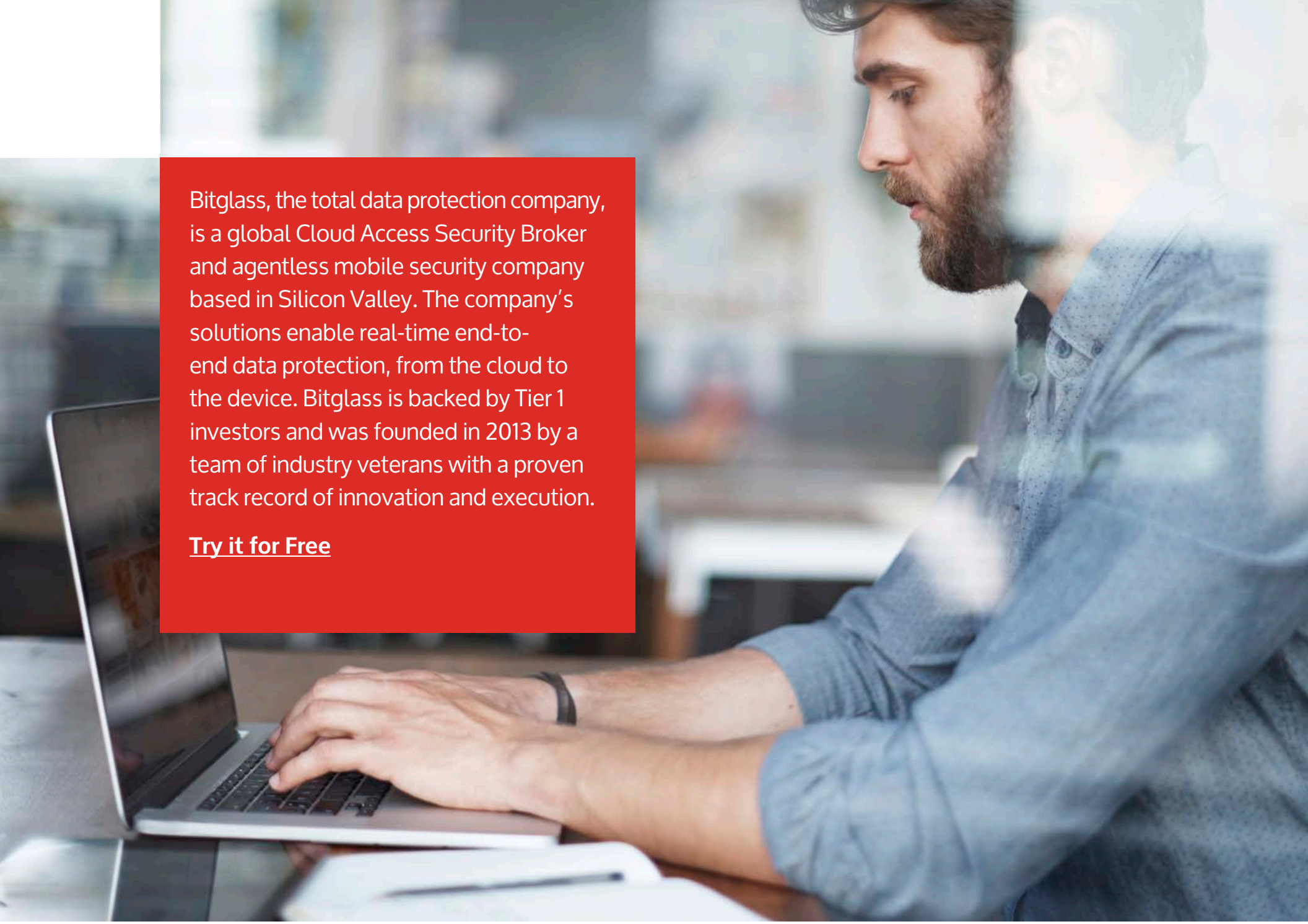
multi-protocol proxies

Proxies are the core means by which a CASB can control access on any device, anywhere. A complete CASB solution needs both reverse and forward proxies to protect data accessed via the web on any device. ActiveSync proxies are critical in extending access to corporate data on mobile devices.



wrap up

Cloud Access Security Brokers are quickly emerging as a must-have security solution for organizations looking to adopt public cloud applications. CASBs bridge the gaps that cloud app vendors have left to the enterprise to solve—data security, visibility, compliance, and threat protection. Organizations need a solution that can secure cloud data on any device, anywhere.



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.

Try it for Free

For more information, visit www.bitglass.com

elasticito

E: information@elasticito.com
T: +44 1183 271 171

bitglass