5 Must-Haves for Your Access Solution

Akamai

Business no longer happens between the four walls of an office building.

This will likely continue to propagate as knowledge workers are more productive, motivated, and loyal to their company when given the option to work remotely.[1]

94% of companies offer flexible work arrangements[2]

140% increase to the work-at-home population (non-self-employed) since 2005[3]

The composition of today's workforce is varied.

Enterprises increasingly rely on contractors, partners, suppliers, developers, distribution channels, and other third-party entities to support their initiatives. This trend, too, is expected to grow more prominent in the coming decade.[4]

This globally distributed and diverse workforce needs flexible yet straightforward access to the corporate network, regardless of user location, device type, employee affiliation, and application location (on-premises, SaaS, IaaS).

SALARIED EMPLOYEES ARE THE MAJORITY AT ONLY **42%** of organizations[5]

77 MILLION (2014 – 2019) freelancers globally, a 36% increase in just 5 years[6]

Expedience and fluidity can't come at the cost of security, especially given the realities of modern cybercrime.

WORLDWIDE CYBERCRIME COSTS **$600 BILLION** — up $100 billion USD since 2014[7] (2014 – 2019)

40%+ of security breaches are linked to authorized users[8]

Access requirements have evolved – so too must access solutions.

Providing application access via aging and cobbled-together software and hardware including traditional VPNs, proxies, and remote desktop technologies is no longer a viable option.

Here are five demands you should make of an updated, comprehensive application access solution:

01 Application- versus network-level access

Traditional access solutions were designed to punch a hole in the network firewall, typically providing unrestricted network-level access. In the event of a breach – whether the result of misused credentials, misplaced devices, or a malicious hack – this access allows lateral movement, permitting navigation across the network and unrestricted access to applications and data.

MUST-HAVES

Look for a modernized application access solution that supports a Zero Trust security framework; every request should be verified and qualified, replacing network-level permissions with case-by-case, custom, application-level access.

02 Enhanced security capabilities

Legacy access technologies lack intelligence; they cannot accurately and adaptively confirm or validate identity, therefore exposing the enterprise to risk. Nor do traditional VPNs integrate with other security mechanisms such as data path protection, application security and acceleration, and single sign-on (SSO).

MUST-HAVES

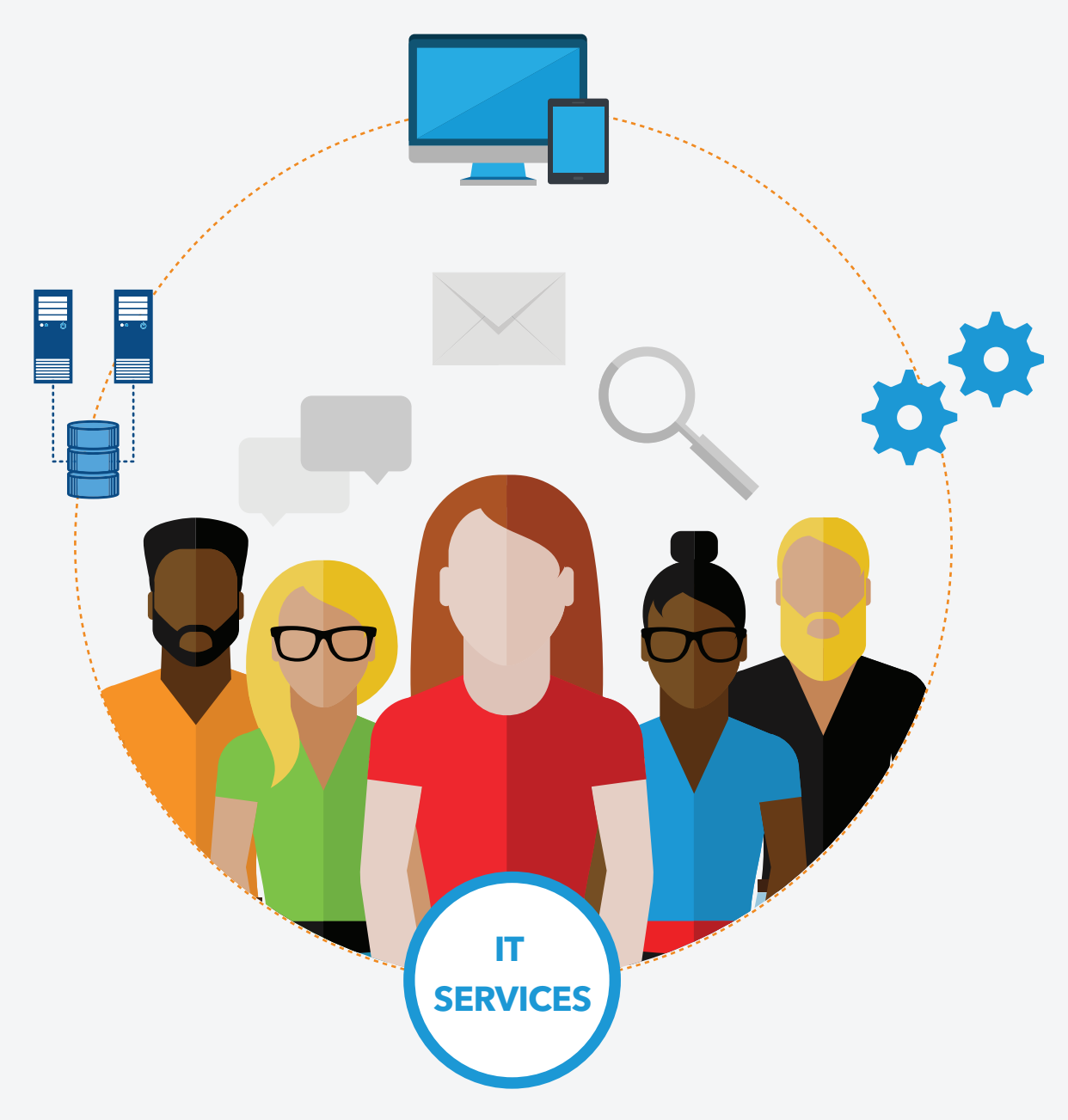
Look for an updated application access model that enables security teams to ensure stronger and identity-aware access. It should work with existing multi-factor authentication (MFA) technology — or offer an integrated MFA solution — as well as a plethora of other advanced security technologies. Access should be agile, locale- and device-independent, and transient.

03 Easy IT management

Onboarding and decommissioning via traditional access models can mean configuring or dismantling more than 10 network and application components per user.[9] IT is also bombarded by help desk requests as a result of fragmented sign-on experiences and erroneous access denials. As a result, access provisioning, basic maintenance, system updates, and user support are complicated and time-consuming processes that monopolize senior IT resources.

MUST-HAVES

Look for a new access solution that removes these complexities, empowering IT to easily and quickly provision and manage access, so they can focus on more strategic and forward-looking imperatives.

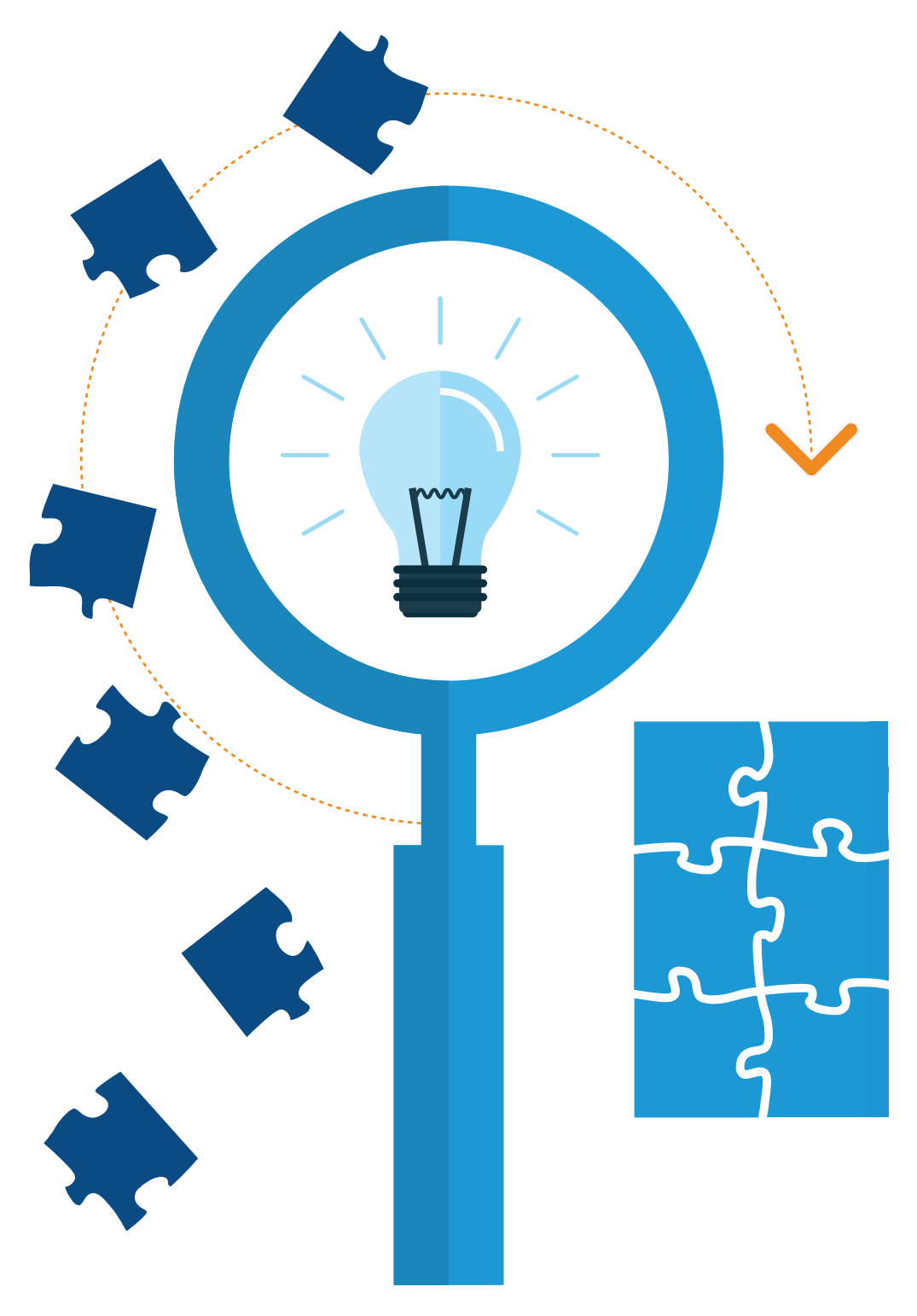


04 Fast and simple monitoring and reporting

Traditional application access solutions make auditing complex or nearly impossible, as they often fail to provide IT with visibility or aggregated reporting of network access and activity. But this reporting and monitoring can be integral for enterprise security as well as application performance purposes.

MUST-HAVES

Look for an advanced solution that offers a single portal through which to easily view and administer access control policies based on user identity, group membership, access method, geolocation, and more. Additionally, reporting should be securely archived and, if a company desires, simply integrate into an existing SIEM.

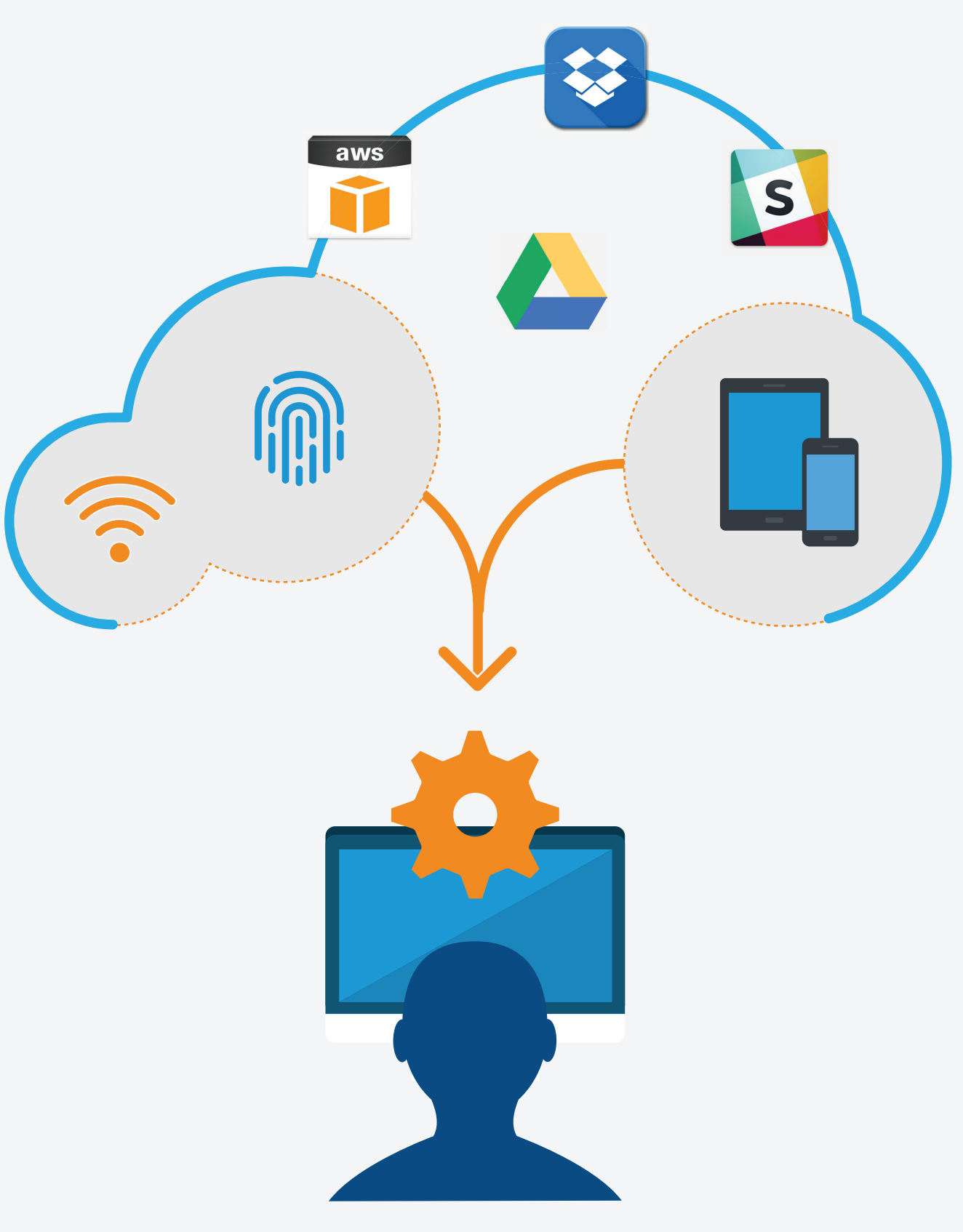


05 Seamless user experience

User expectations of application access and performance have changed. They want the same experience from their corporate applications as they receive from consumer applications: simple, fast, and intuitive access on the device of their choosing, from any location. Enterprises that can deliver this well will not only improve employee engagement and productivity, but will also free up IT resources that were previously hampered by locked accounts and forgotten passwords.

MUST-HAVES

Look for a contemporary access solution that offers users SSO across all application types — so they can authenticate once to access necessary applications with a click of a button — as well as one that can provide acceleration enhancements to applications.



Your business has transformed. Shouldn't your access solution follow suit?

To find out how Akamai can enable you to evolve your access solution while enhancing your enterprise's security,

visit akamai.com/eaa.

Sources:

1) https://www.ciphr.com/advice/10-essential-remote-working-statistics/
2) https://www.ifebp.org/bookstore/flexible-work-arrangements/Pages/flexible-work-arrangements-2017.aspx
3) http://globalworkplaceanalytics.com/telecommuting-statistics
4) https://www.upwork.com/press/2017/10/17/freelancing-in-america-2017
5) https://www2.deloitte.com/insights/us/en/focus/human-capital-trends/2018/contingent-workforce-management.html
6) Ibid.
7) https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHd&
8) https://www.akamai.com/us/en/multimedia/documents/report/remote-access-security-challenges-and-opportunities.pdf
9) Ibid.

Akamai