Complete IT Systems

5 steps to secure home devices & improve productivity for remote work

Contents

The nature of remote work

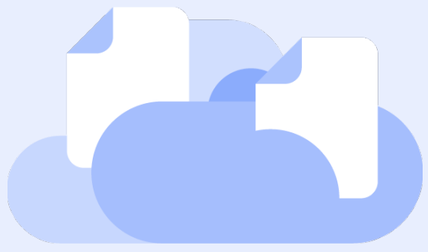
Modern security empowers employees and companies to thrive in remote work.

Due to sudden global changes, remote work became an essential part of a modern enterprise. For remote work and employees to thrive, it's essential to ensure fast and secure access to company data and resources. Innovative rather than outdated security practices are critical to support the new way of work, where security empowers employees and companies by enhancing productivity and collaboration.

Remote work benefits:
Flexible hours
Flexible location
Work-life balance
Productivity

Office work vs remote work

The shift from traditional office work to remote work brought on unique challenges accessing company resources.



Traditional office work

Access to data within a corporate network perimeter

Access to resources based on inside or outside network perimeter

Company data in mostly on-premises

Access granted based on user credentials that can be easily compromised

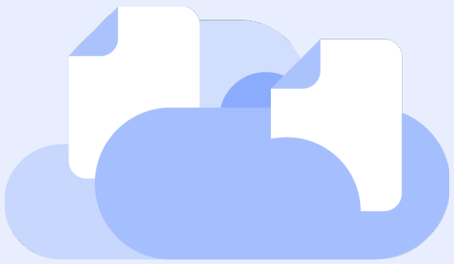
Requires a traditional VPN when accessing resources outside the corporate network and risks network exposure

Connecting to a corporate network to access resources via a VPN is slow and unreliable

When access fails, no remediation steps provided; needs help from IT and adds additional cost

Security measures in place, provided by the company

Remote work



Access to data from outside of the corporate network perimeter

Access to resources from anywhere

Company data in the cloud and on-premises

Access granted based on user identity and access policies to improve security

No need for a traditional VPN to access resources; mitigates network exposure risks

Fast and reliable access to company resources on a corporate network

When access fails, remediation steps are provided to fix access issues immediately at no extra cost

Lack of security measures due to BYOD, home networks, lack of security knowledge

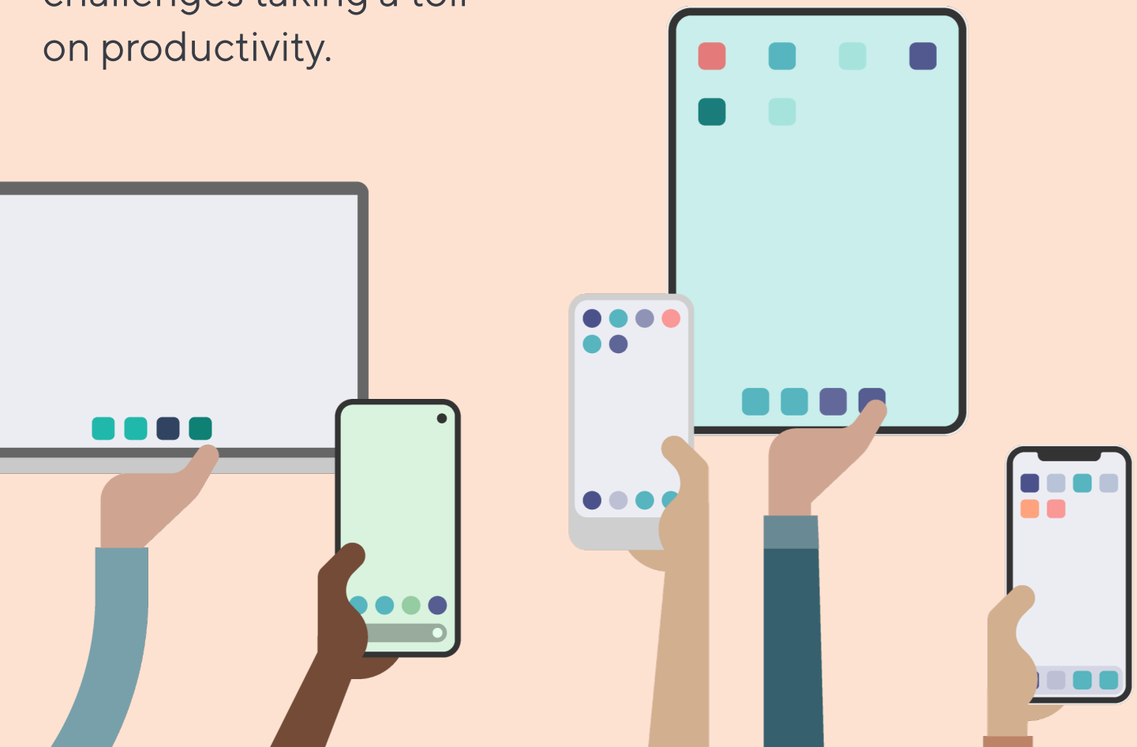
Five remote work security & usability challenges

Despite the benefits of remote work, it can also bring security challenges. Those challenges span from the used technologies, user security knowledge and awareness, and the ever-increasing cyber-attacks. In many cases, an attacker needs to compromise only one device, with a phishing attack or exploit a vulnerability in an unpatched system, to access key resources in the company network. Such events can lead to company network exposure and eventually to data breaches.

1. Connecting to an office network

Potential company network exposure (if connecting unknowingly with a compromised device).

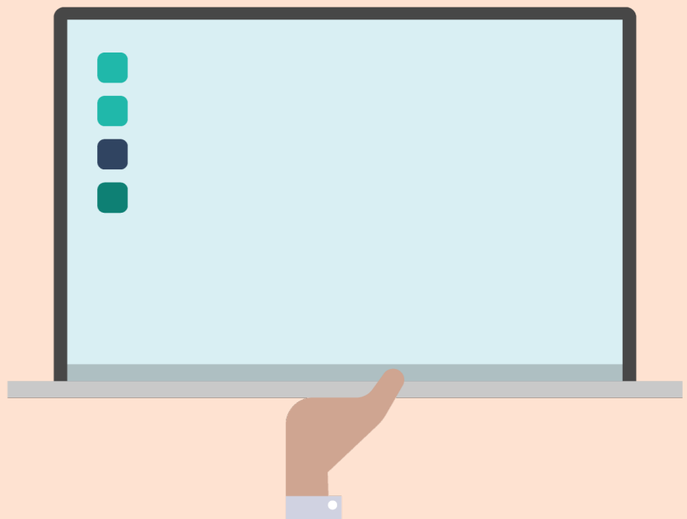
Connectivity and speed challenges taking a toll on productivity.



2. Device security challenges

Outdated device's operating system (OS) version is more prone to known and exploitable vulnerabilities.

Jailbroken or compromised devices.



3. Network security challenges

Lack of visibility into who's accessing what set of resources, using which devices from where and how long.

Compromised devices can "teleport" to the network.

Lack of remediation steps upon failed access.

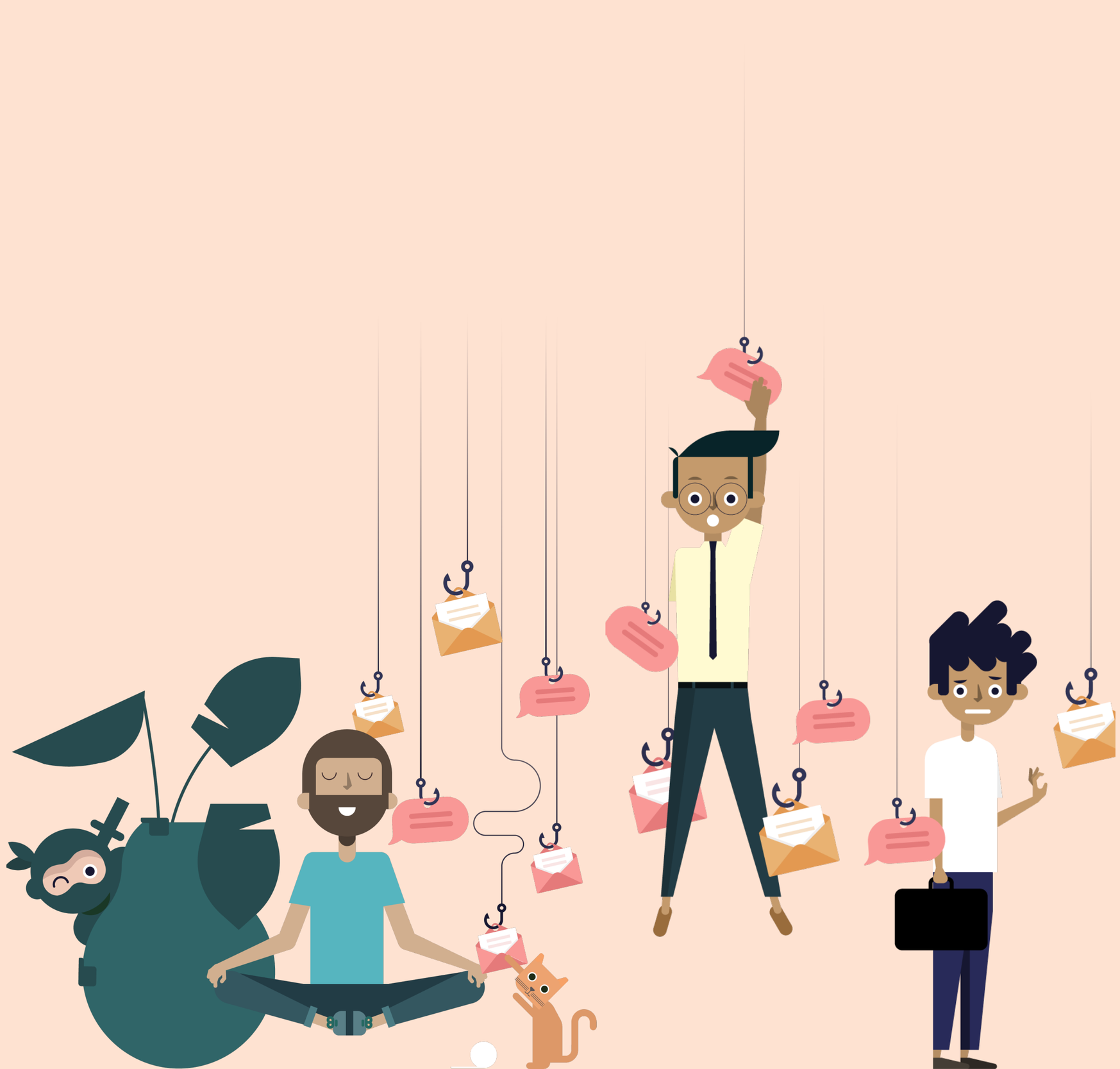
Challenges supporting multi-cloud connection to access resources.

4. Phishing and other cyber threats

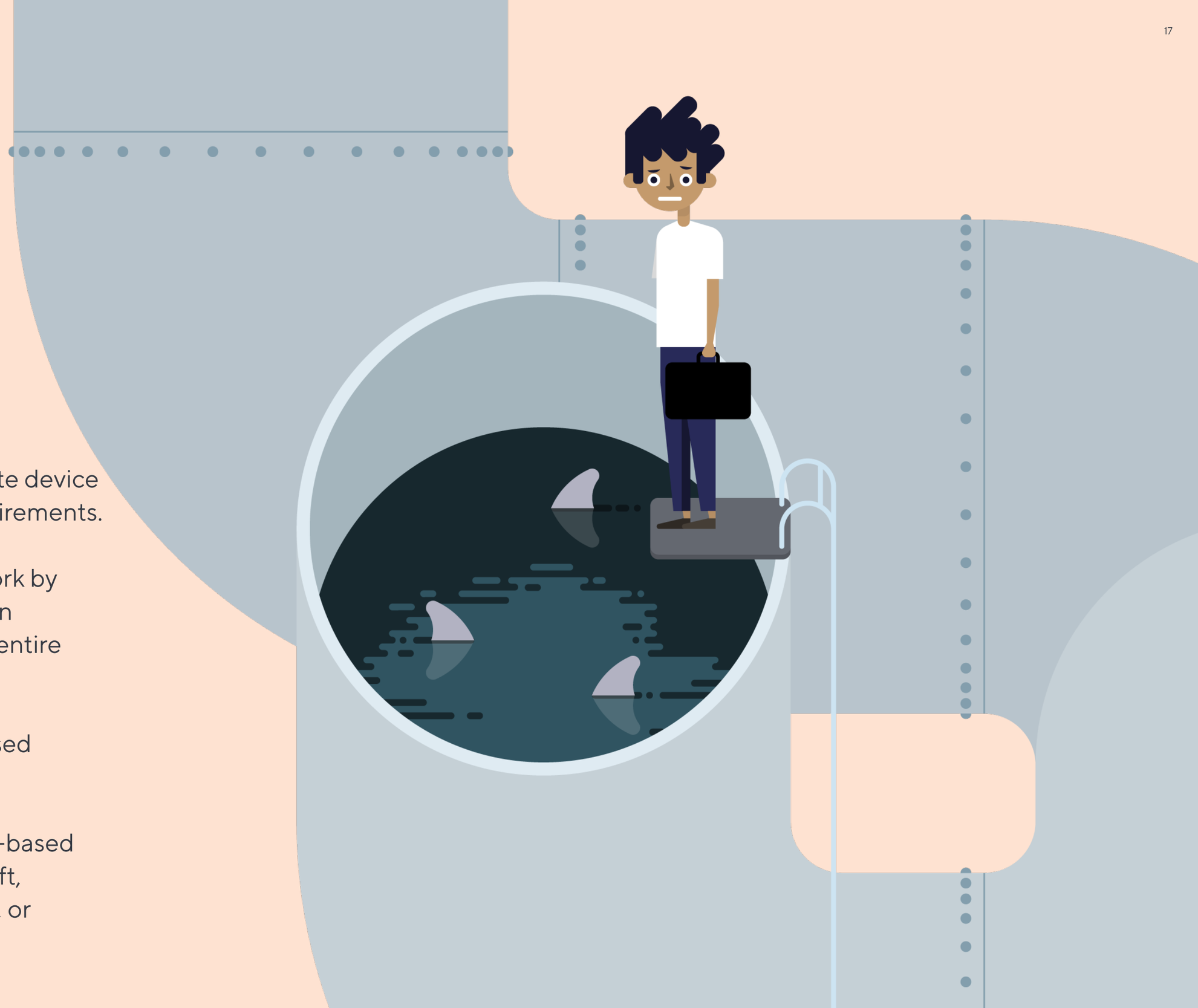
Aims to steal personal data, work or financial account credentials, or any other valuable data.

It appears to be sent from a reliable source and usually contains malicious links or attachments.

This leads to clicking on links that steal accounts credentials or installing fraudulent software.



5. VPN challenges



VPNs do not enforce corporate device security and compliance requirements.

VPNs expose company network by providing access not only to an intended resource but to the entire company network.

VPNs do not support role-based access.

VPNs don't protect from web-based attacks such as credential theft, phishing, drive-by downloads, or malvertising.

Five steps to secure devices and improve productivity

To enable secure and productive remote work, provision employee owned devices and shared home computers and securely connect these unmanaged devices to the corporate networks and applications.

Barracuda CloudGen Access helps to secure and simplify access to any on-premises, cloud, or hybrid app and workload and allows secure access to company data from any device or location.

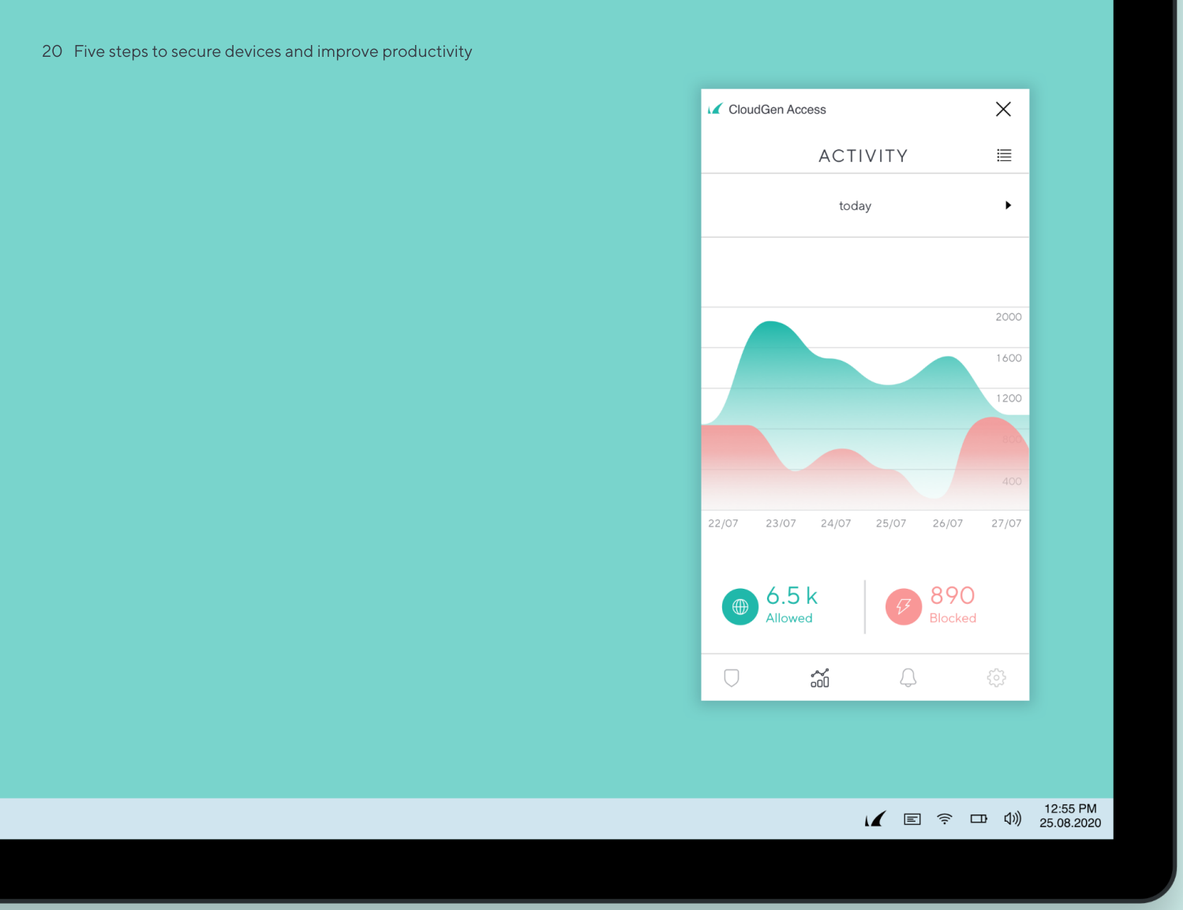
Compared to traditional VPNs, Barracuda CloudGen Access enables you to achieve:

70 %
Improvement on access flows

20 %
Reduced access latency

5 min
Deployment

Visibility to all remote access requests



1. Secure your devices

Ensure devices to upgrade to the latest operating system (OS) version to enhance device security.

Block web-based attacks such as phishing, malware, ransomware.

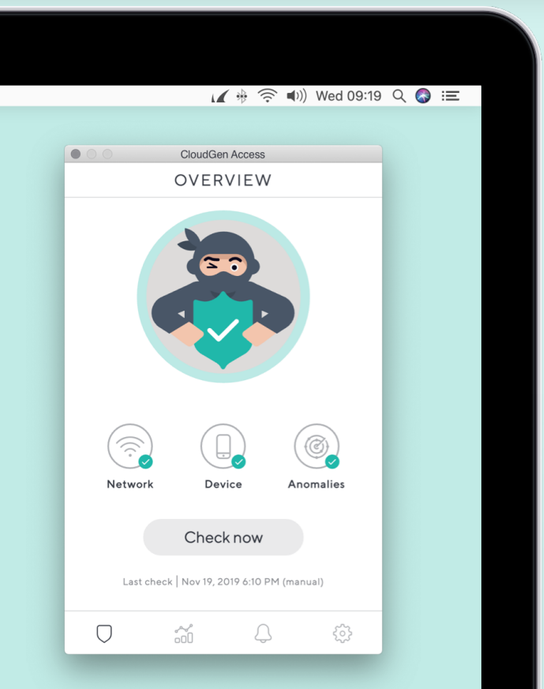
2. Secure your network

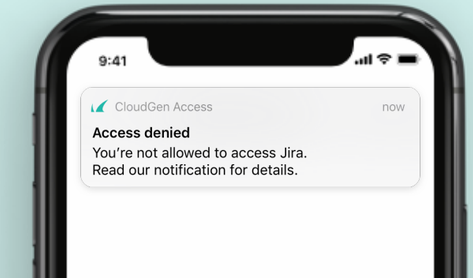
Get insights into who's accessing what resources, using which devices.

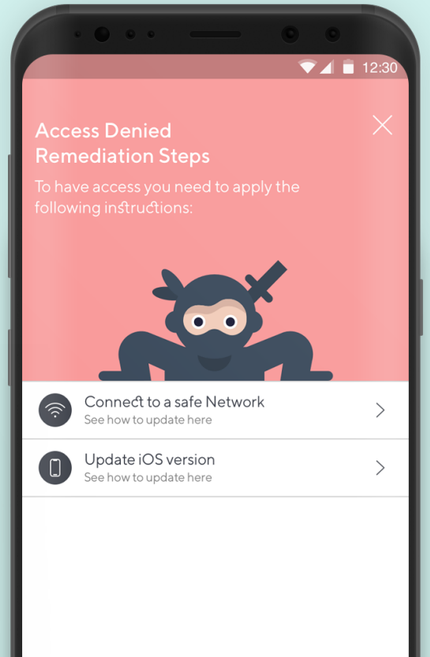
Protect company networks from compromised devices.

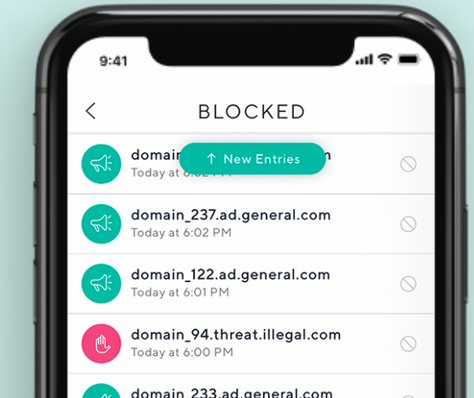
Provide easy remediation steps due to access or posture policy violations.

Easily support a multi-cloud infrastructure to access resources.









3. Secure access

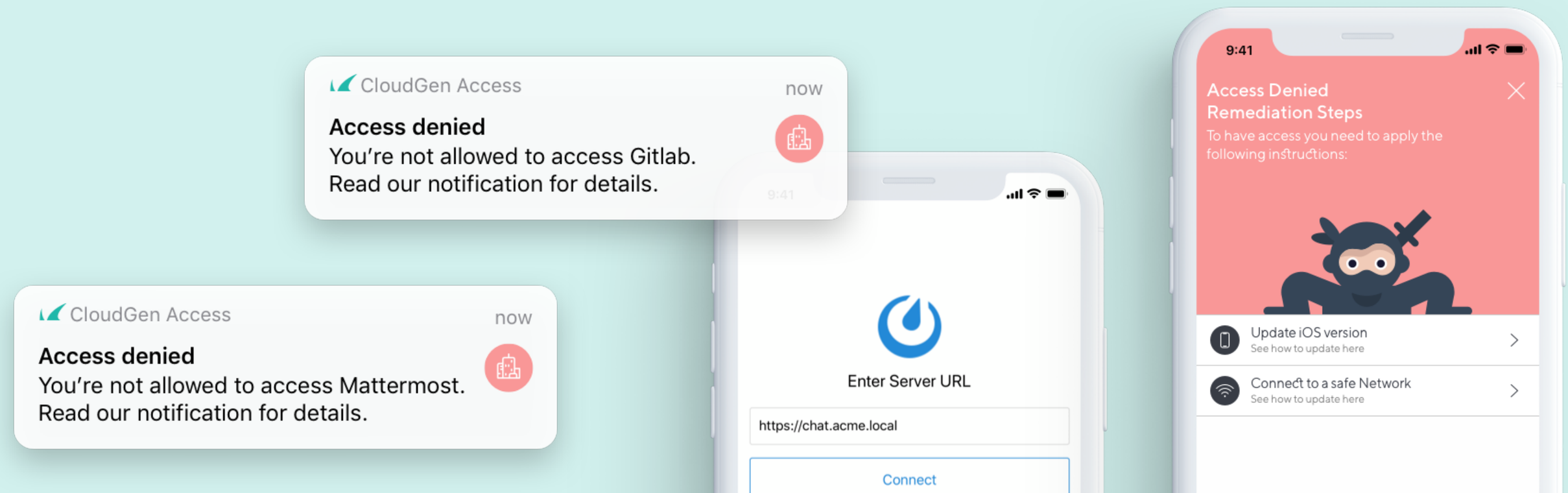
On-premises apps

Set role and attribute-based controls to grant contextual access to trusted users and devices.

Gain total visibility into access activities, and mitigate risks.

Ensure data privacy: your data-plane never leaves your infrastructure.

Secure access without any additional network latency.



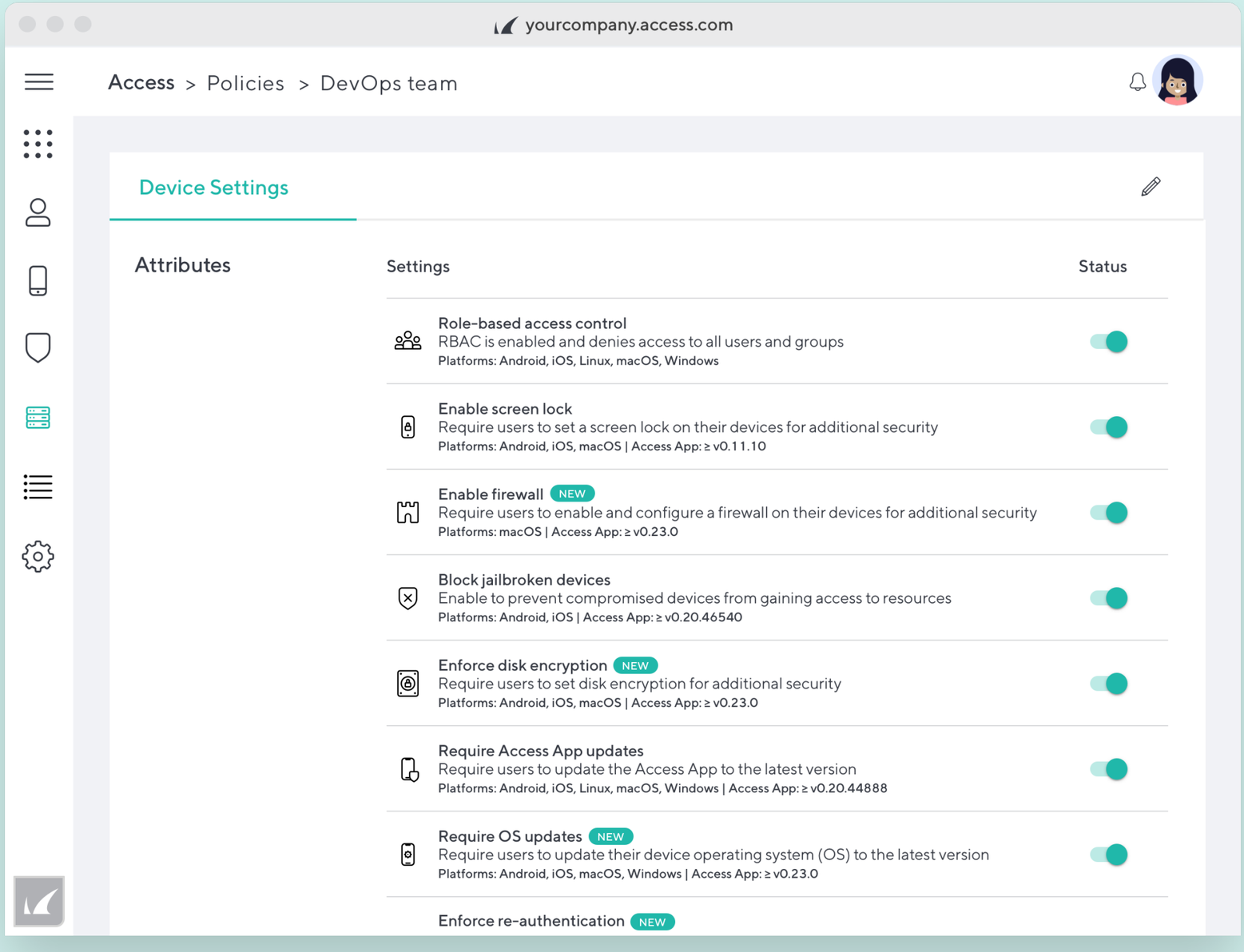
3. Secure access

Enforce policies and empower users

Maintain security with continuous assessment of user and device identity and security posture.

Manage global policies such as disk encryption and device screen lock and automatically block access for compromised devices.

Improve productivity and remove friction with simple, self-service remediation steps for blocked users.



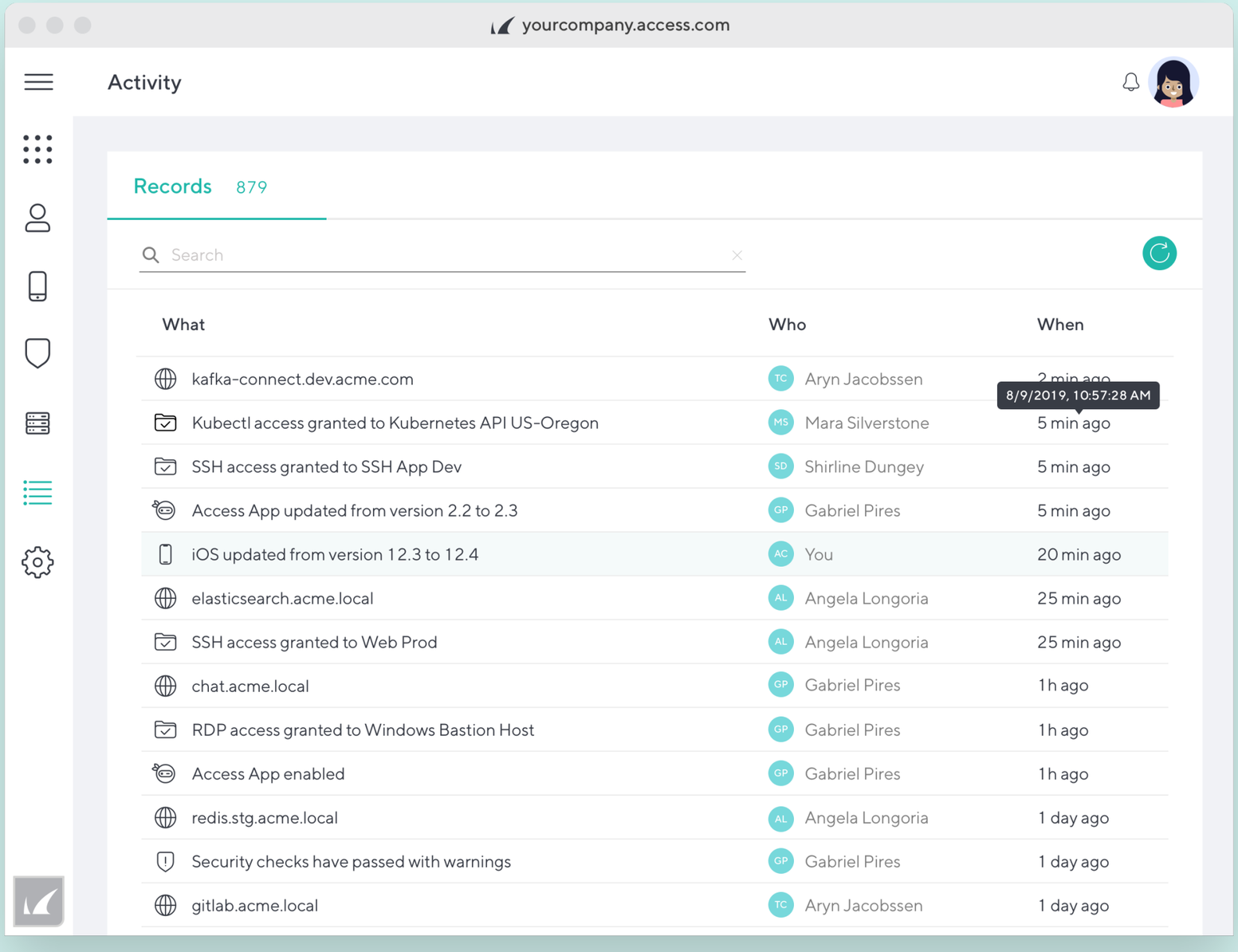
3.
Secure access

System of record for app and workload access

Streamline audit and compliance reporting.

Track and observe users and devices accessing your on-premises apps.

Get useful insights into endpoint telemetry, define access policies, continuously monitor device security posture, and more.



4. Protect from cyberattacks

Protect from phishing, malware, ransomware, credential theft, compromised Wi-Fi networks, and various other cyber threats.

5. Improve your productivity

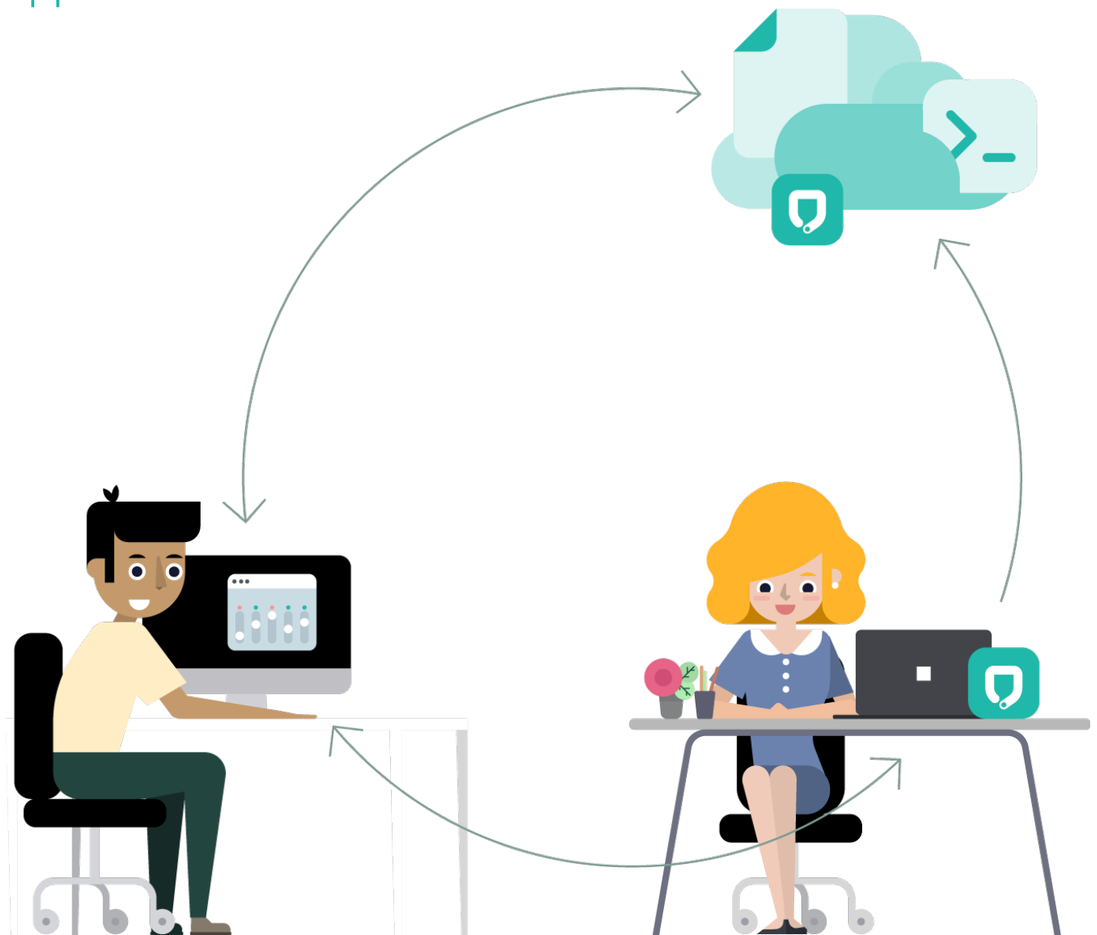
Block intrusive ads and privacy-evading trackers and enjoy an interrupted online experience.

Quickly and easily access company resources without the usual VPN delay and focus on your work.

An increasingly decentralized world is driving digital transformation and challenging the status quo. Barracuda CloudGen Access is the new standard for Zero Trust secure access.

Barracuda CloudGen Access helps organizations mitigate risks while adapting to the new nature of work and IT, powering their journey to the Zero Trust Architecture. Our innovative approach is driven by patented technology that enables secure, reliable and fast access to any on-premises, cloud or hybrid app or workload.

Barracuda CloudGen Access eliminates security risks associated with traditional VPN access, while protecting user identities from account takeover attacks.



Secure devices and improve productivity with Barracuda CloudGen Access

More information on how Barracuda CloudGen Access implements Zero Trust to enhance security and productivity.

Learn more on Barracuda CloudGen Access documentation.

Barracuda

barracuda.com sales@barracuda.com