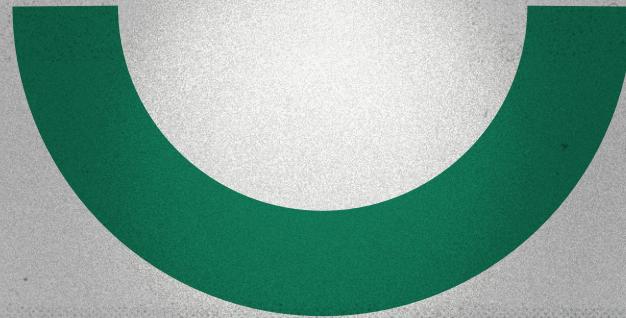


Win 8 IT Projects with SASE



Secure Access Service Edge (SASE) is a modern solution to enterprise network and security needs. The evolution of cloud computing and social change have inverted the direction of digital traffic, turning it outwards to the public internet instead of inwards to the organizational data center. This has created new network and security complexities that existing point solutions cannot solve.

SASE is a converged, cloud-based network and security architecture for modern enterprises. It secures global WAN connections, ensures high cloud application performance and enables fast and secure access from all edges.



Let's look at eight different changes and challenges that are driving SASE adoption globally.

1

Enabling the “Branch Office of One”

Mobile devices and continuous connectivity have enabled employees to stay always-on and work from anywhere at all times. This ability has turned them into a “branch office of one”, i.e a fully functional business unit, consisting of one person.

COVID-19 has accelerated this trend, with the major shift to remote work. This structure is expected to stick.



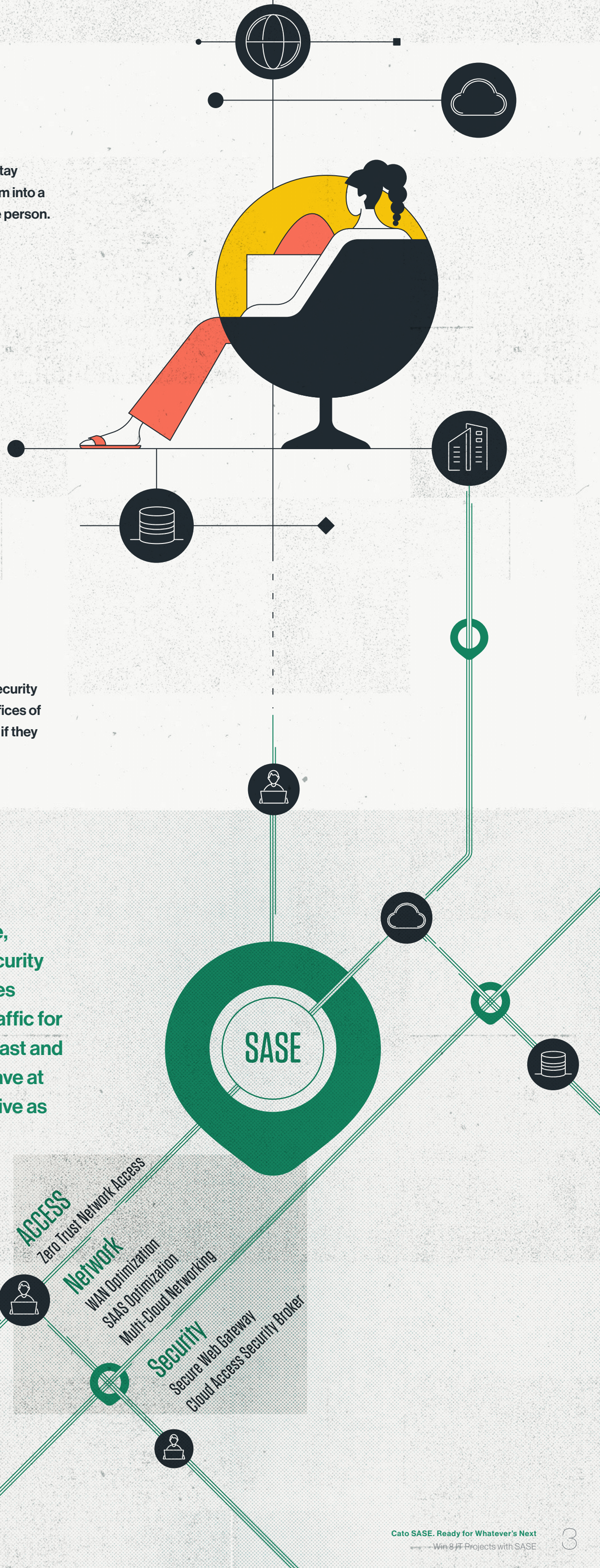
According to McKinsey, 52% of employees would prefer a more flexible working model after the pandemic.

The majority would like to work from home at least three days a week.

With remote work becoming a standard part of company culture, IT and security teams need to find network and security solutions for all these “branch offices of one”. And, enabling these employees to work seamlessly and securely, as if they were sitting in the office, is essential for ensuring business continuity.

How SASE Helps

SASE supports employees working from anywhere, with the same scalable cloud infrastructure and security policies as on-premises employees. SASE optimizes traffic to any edge while continuously inspecting traffic for threats and access control. All users get the same fast and secure network and application experience they have at the office. This ensures they can be just as productive as on-premises employees (and even more).



2

Direct-to-Internet Branch Access

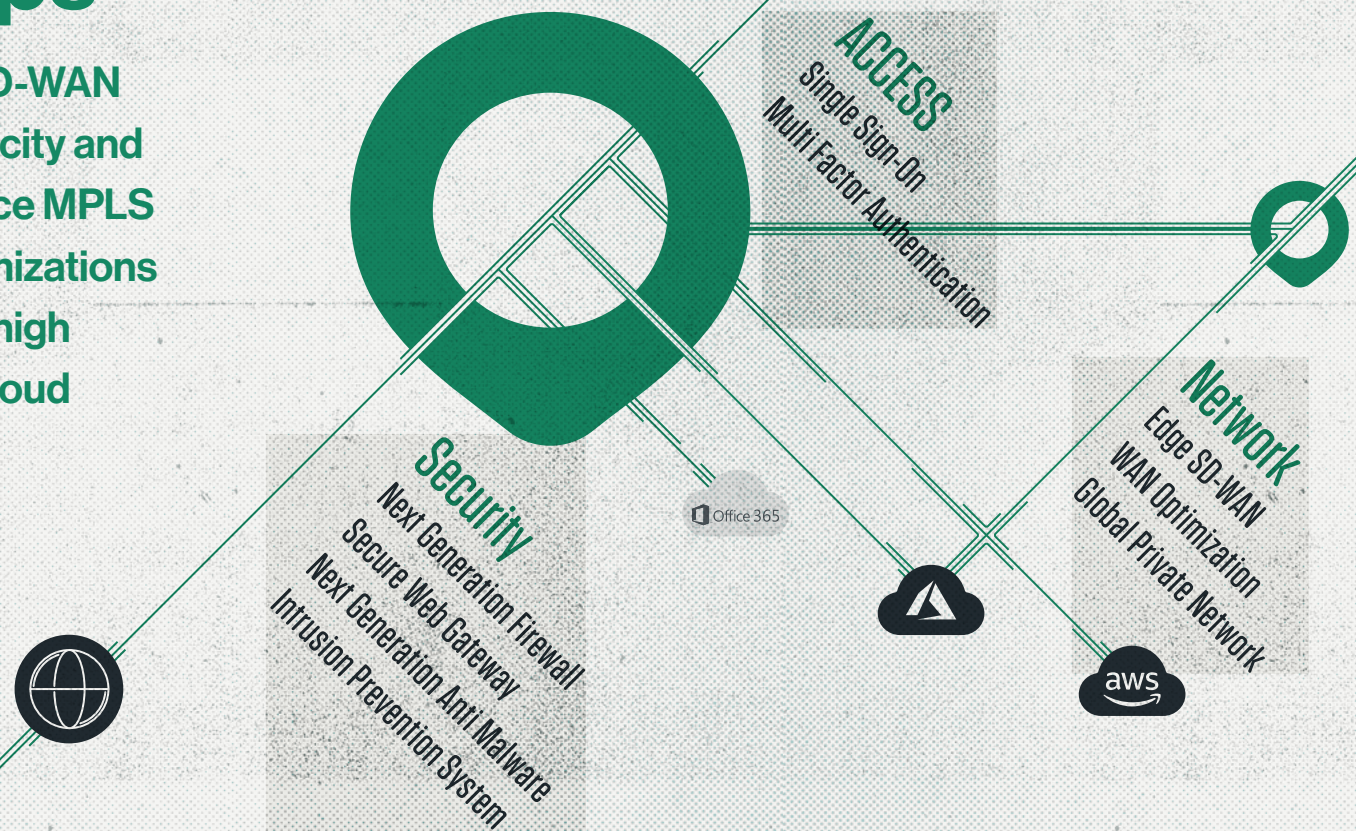
Alongside the emergence of the “branch office of one”, traditional branch offices are evolving as well. Branches with hundreds of employees sitting together no longer operate as a cohesive business unit. Instead, each employee acts as an independent unit – communicating with others across the world and connecting to global cloud infrastructures, platforms and applications. This has turned branches into a collection of users, who, to some extent, are “branch offices of one”, sitting together.

IT and security are required to provide high speed and optimized access to the public network and SaaS applications, to all users and at all times.



How SASE Helps

SASE provides enterprises with SD-WAN capabilities for their last-mile capacity and a global private backbone to replace MPLS and the erratic Internet. WAN optimizations and a managed backbone ensure high performance from the branch to cloud applications, and at a lower cost.

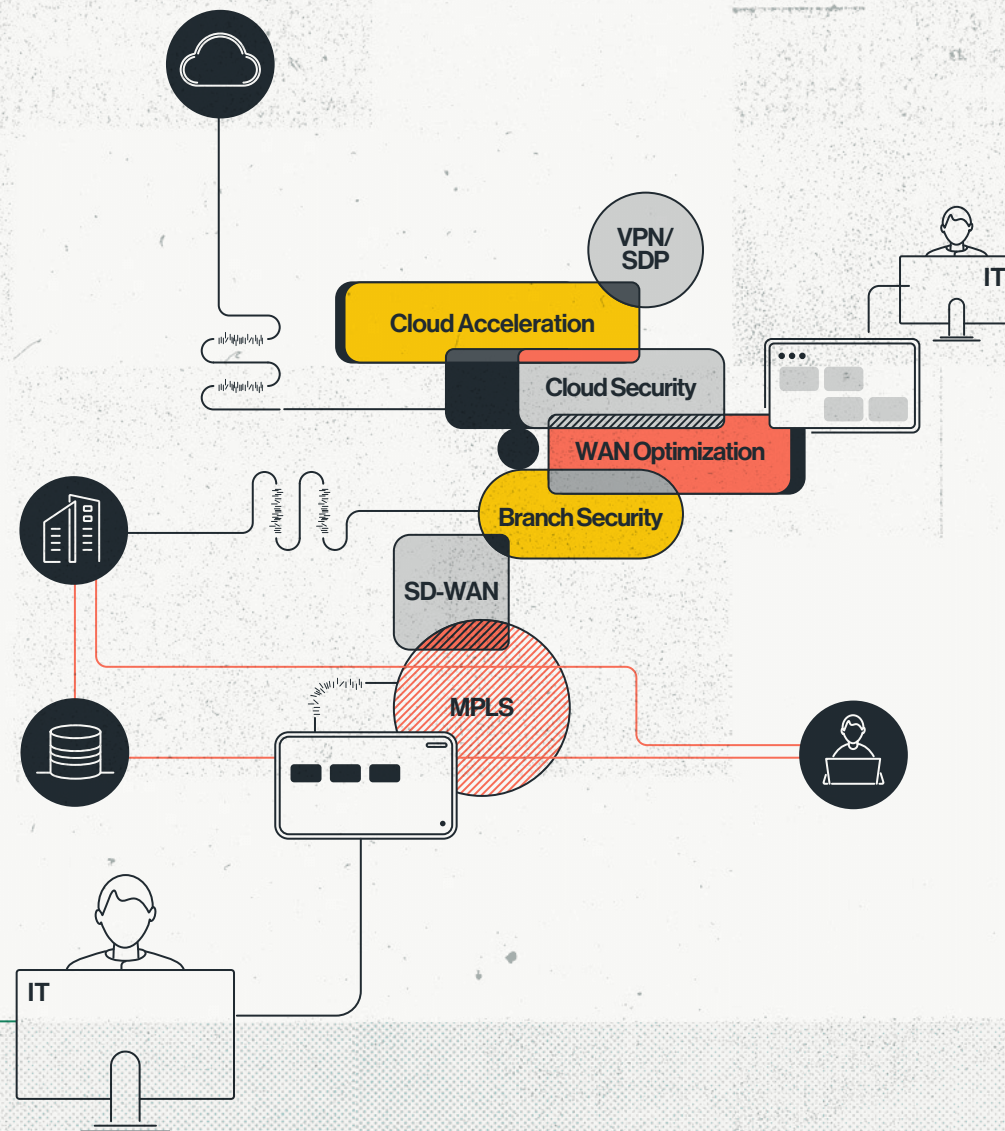
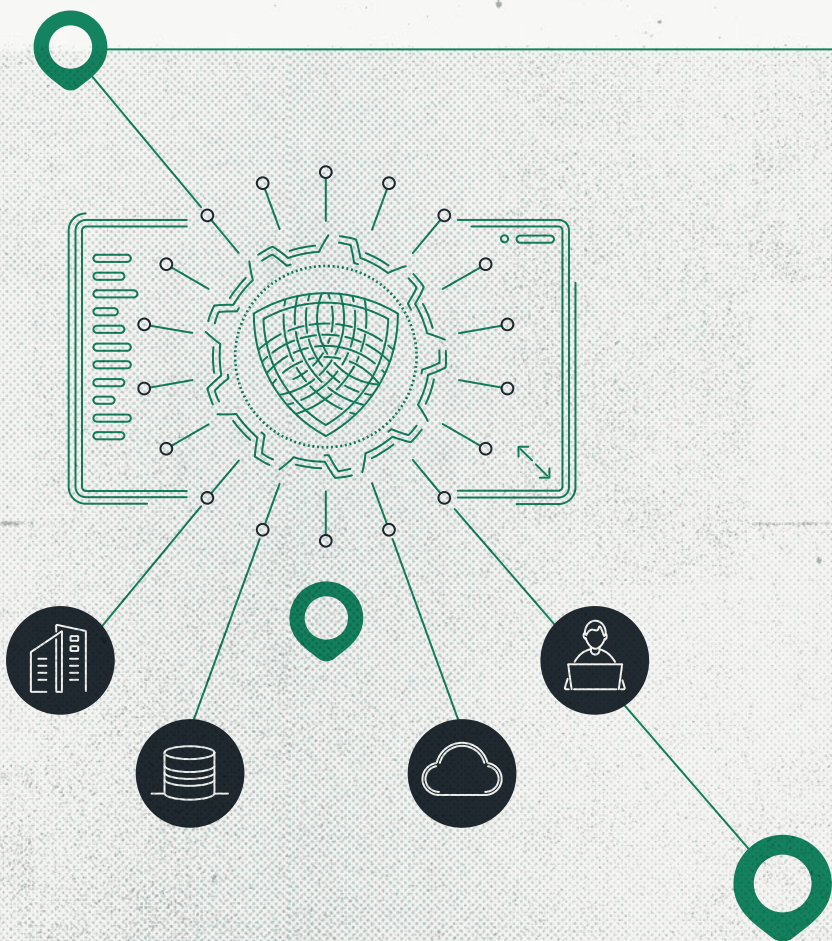


3

Consolidating Vendors

With so many point solutions and vendors to choose from, IT and security teams are struggling to figure out which solution can address their current and future needs. Once they choose vendors, managing one box for secure web gateway, another for firewalls, a third for remote web access, etc., creates a lot of overhead and complexity.

This process is time-consuming, and can potentially impair the ability to derive value from each solution. In addition, integrating these solutions that were not built to work together, can create cyber security gaps. This puts the organization at a security and business risk.



How SASE Helps

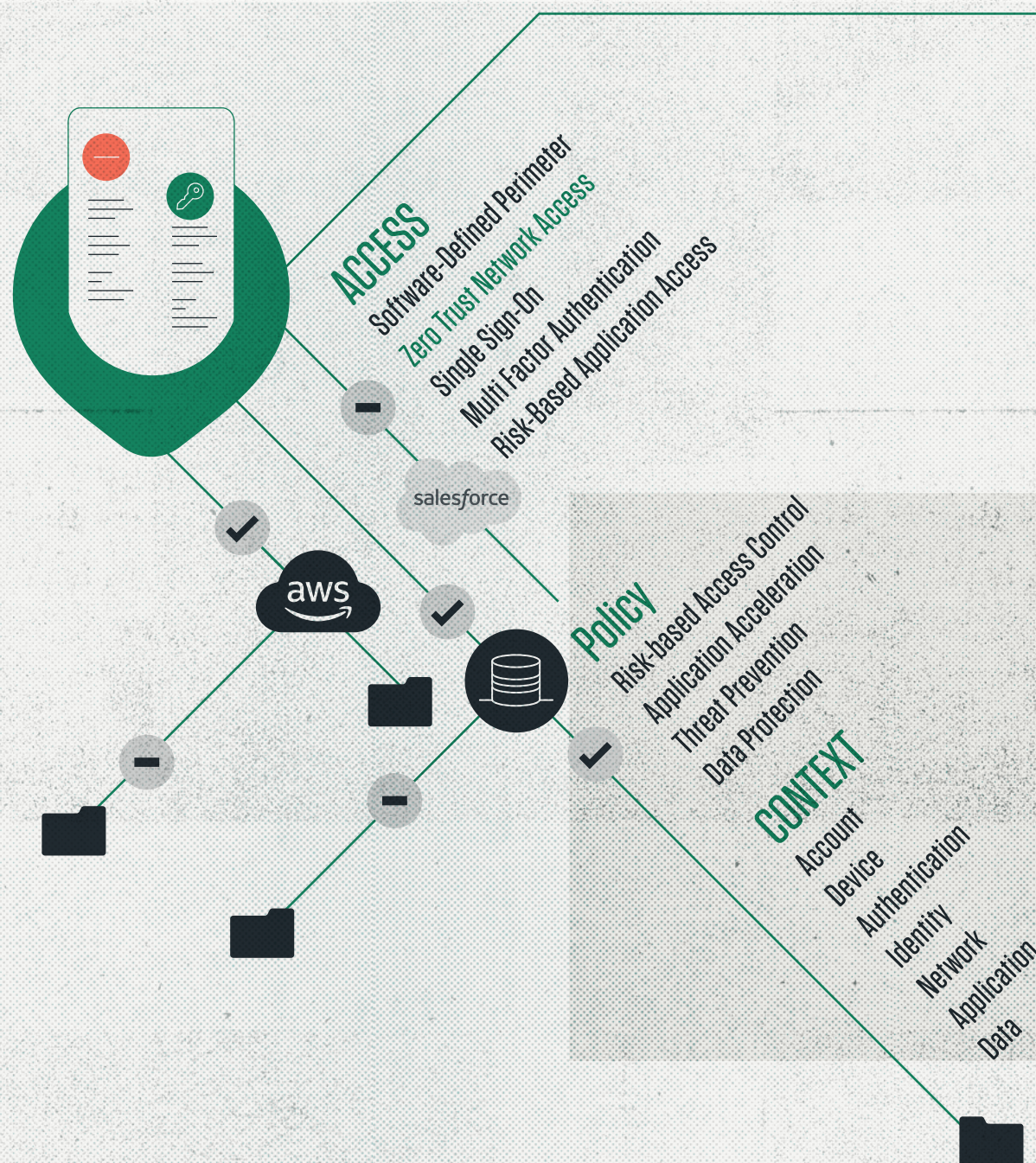
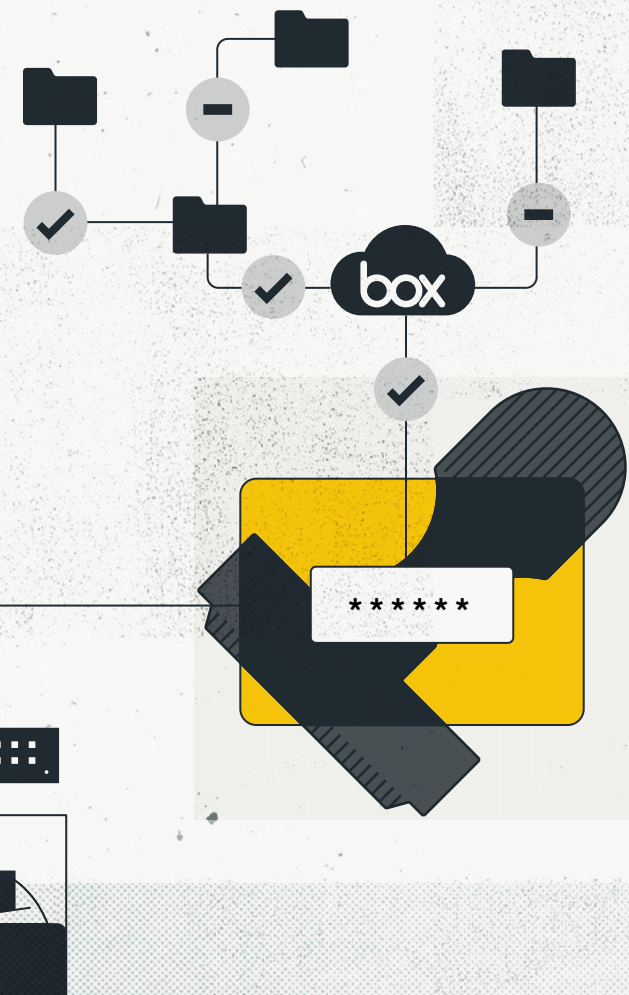
SASE simplifies management by providing a single, converged solution for all network and security needs, today and tomorrow. A single console is used for configuration, management and reporting – for all network and security functions. This improves visibility, enables optimization and troubleshooting, saves time, and lets IT enforce a single set of policies across the entire network.

4

Adopting Zero Trust

As networks evolve and with identity becoming the new perimeter, a zero trust strategy is becoming more essential and prevalent. The zero trust security model ensures no user or device is granted access to any asset or app based on their IP or network origin. Instead, they are continuously authenticated beforehand. This ensures that attackers from both outside and inside the network have no access to sensitive data.

This change requires a shift in the IT and security mindset, from securing physical locations to connecting and securing users and devices.



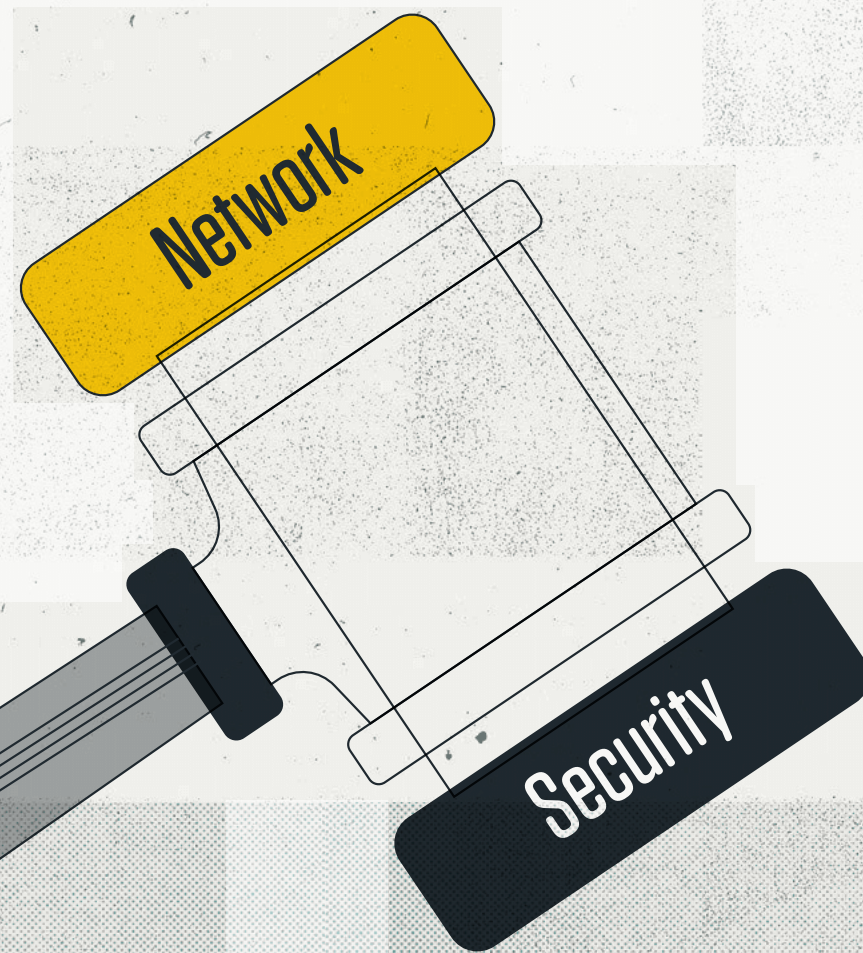
How SASE Helps

SASE uses ZTNA (zero trust network access) to limit users to the resources they're allowed to see. By using a simple client software or clientless browser access, users connect dynamically to the closest SASE PoP, where traffic is routed optimally to the data center or application, and users are automatically protected by corporate security policies. Remote access becomes easy to implement and easy to secure.

5

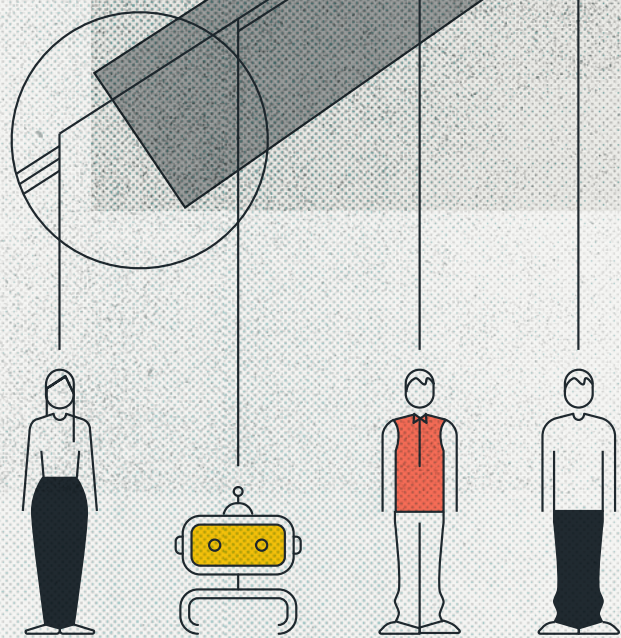
Aligning Network and Security Policies with Business

As the perimeter dissolves, IT and security teams are required to rethink their connectivity and security strategies. Connecting IP addresses and locations is no longer sufficient. Instead, they are required to manage roles, jobs and people. This requires a broader policy that is connected to the business process. The scope of IT's role has expanded and requires to adapt accordingly.



How SASE Helps

SASE provides a global network of PoPs and the entire network and infrastructure can be easily managed from a single console. This global control and visibility provides IT with the capabilities needed to make and execute business decisions.

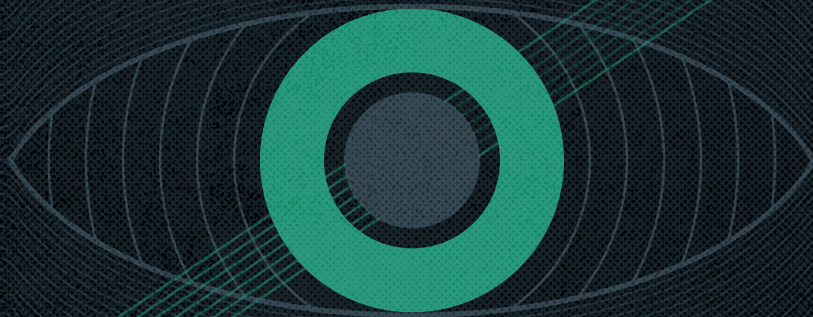


Changes and challenges that are driving SASE adoption globally

6

Data Visibility, Control & Threat Protection Across All Channels

The modern digital business needs network and security policies to be enforced, across all users, applications, and locations. Gaining consistent visibility into all these channels to maintain control and protect against threats is a huge challenge.



How SASE Helps

SASE's converged security stack enables full data visibility for consistent policy enforcement and threat protection for all edges, anytime and anywhere.

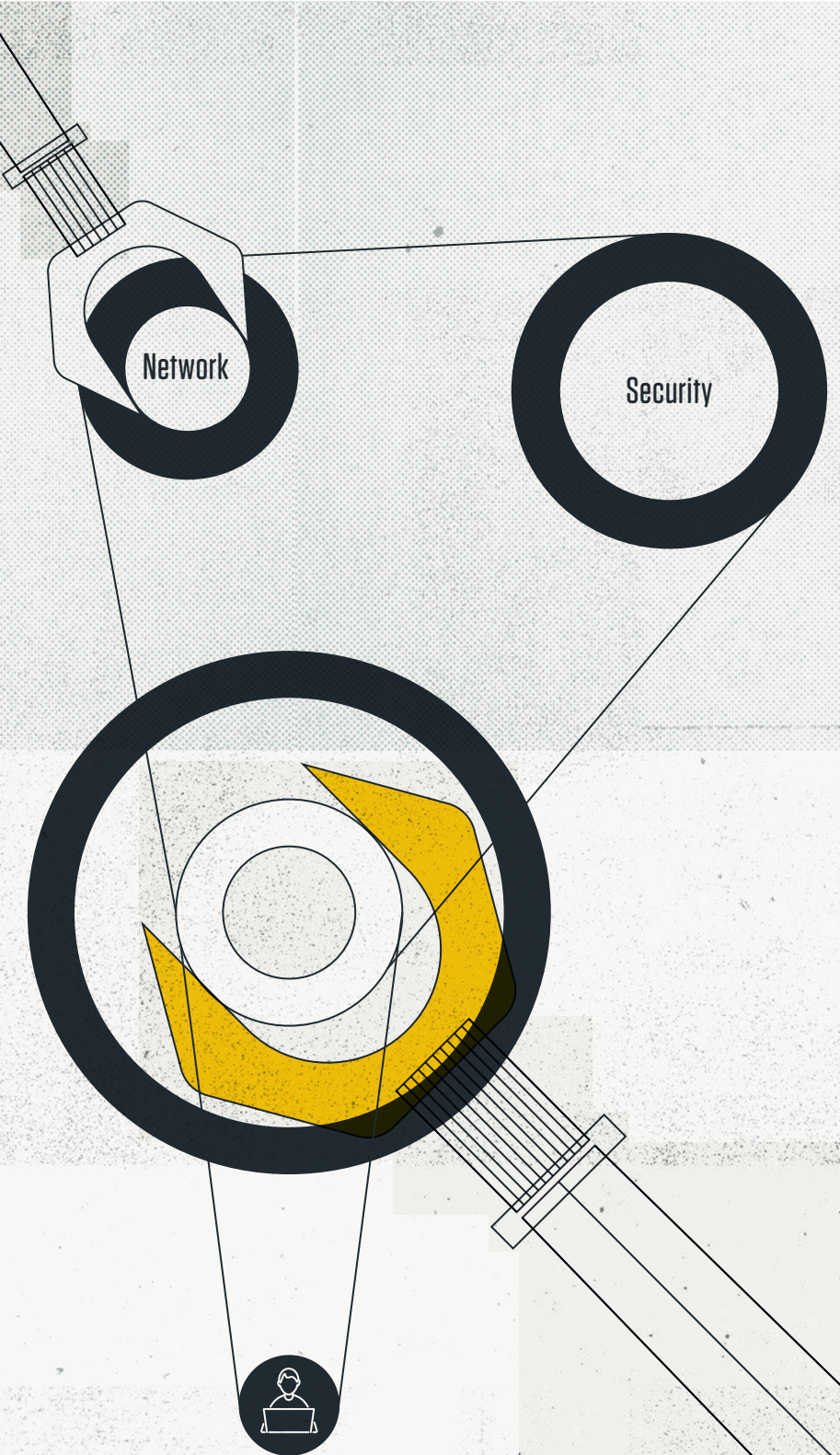
7

Consistent User Experience

Providing a simplified and successful user experience is essential for the adoption of new solutions and for business continuity. This is important both for IT and security teams, and for the organization's employees. A frustrating user experience, as the one that accompanies connecting to a VPN, can hamper business agility and slow down productivity.

How SASE Helps

SASE provides a superior user experience both for IT and employees. For example, the insights screens SASE provides into network issues such as jitter, packet loss, and latency makes troubleshooting simpler and more convenient for IT. As a result, IT can configure the network and provide a better user experience for end users.



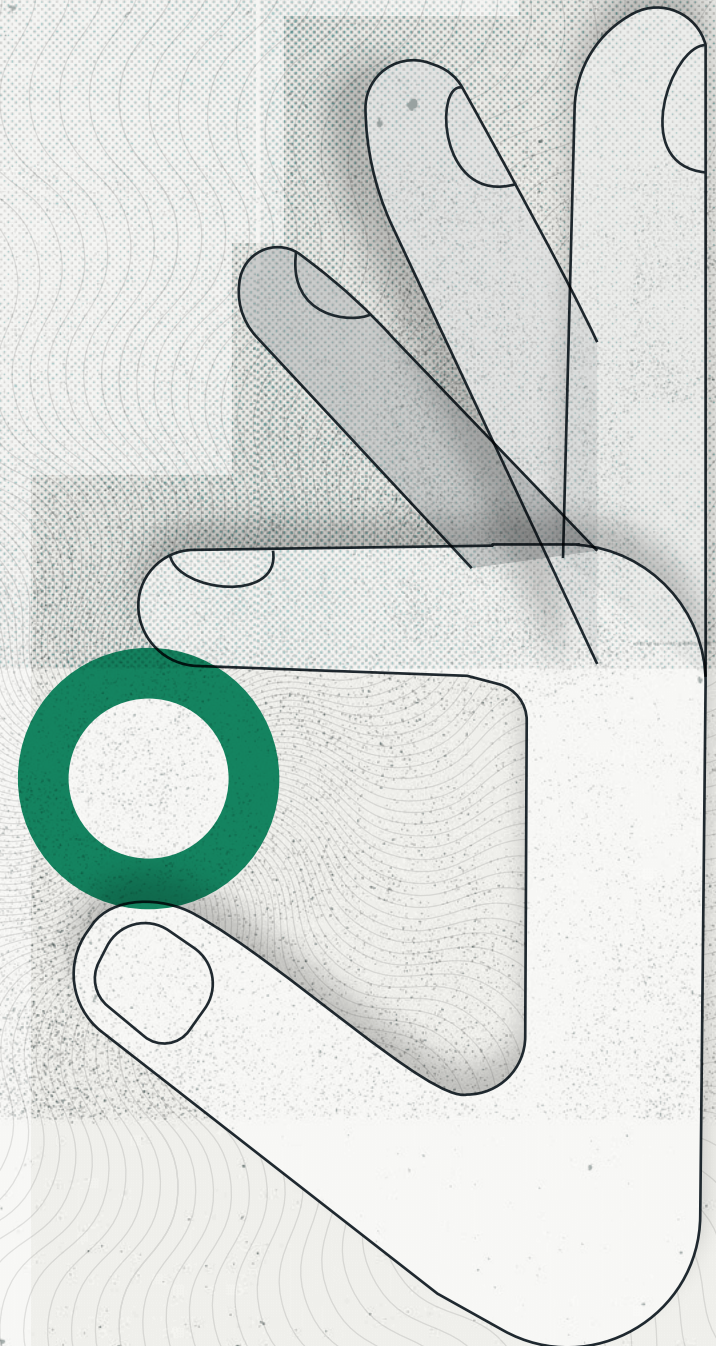
8

Digital Dexterity

Organizations today need to be able to quickly adapt their technologies and infrastructure, so they can support business changes with speed and agility. For example, if a business needs to add new offices, onboard employees, conduct M&As and enhance partnerships – IT and security need to accommodate. While point solutions might help with bits and pieces, IT and security teams need a holistic solution that can also evolve with the business requirements.

How SASE Helps

SASE services are delivered in the cloud and can scale easily to answer any requirements, on the spot, globally. SASE enables adding new edges that can connect anywhere across the globe, 24X7. This provides a network and security solution to any expected or unexpected need.

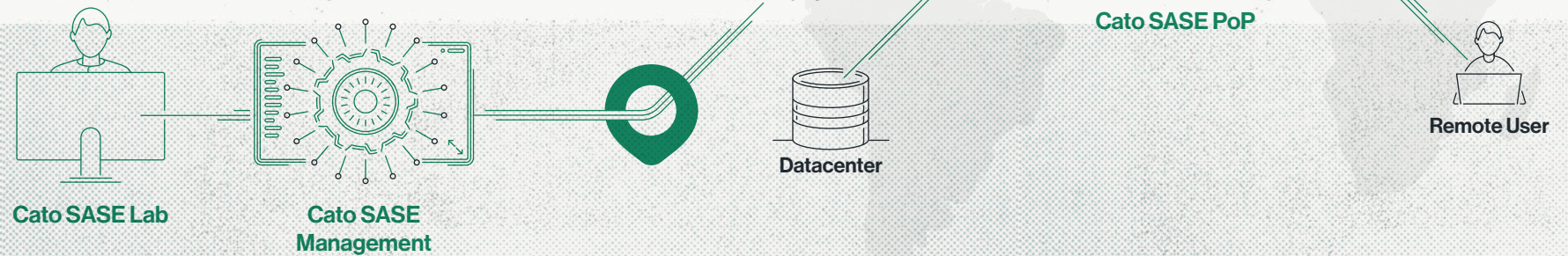


Conclusion

Global digital transformation is driving the adoption of agile solutions that can provide secure, global access with high performance. However, IT and security teams are realizing that point solutions not only fail to answer their needs, but add to network complexity, as well.

These changes are driving the adoption of SASE, the convergence of all network and security functions into a single cloud service that drives the simplicity and agility modern businesses require.

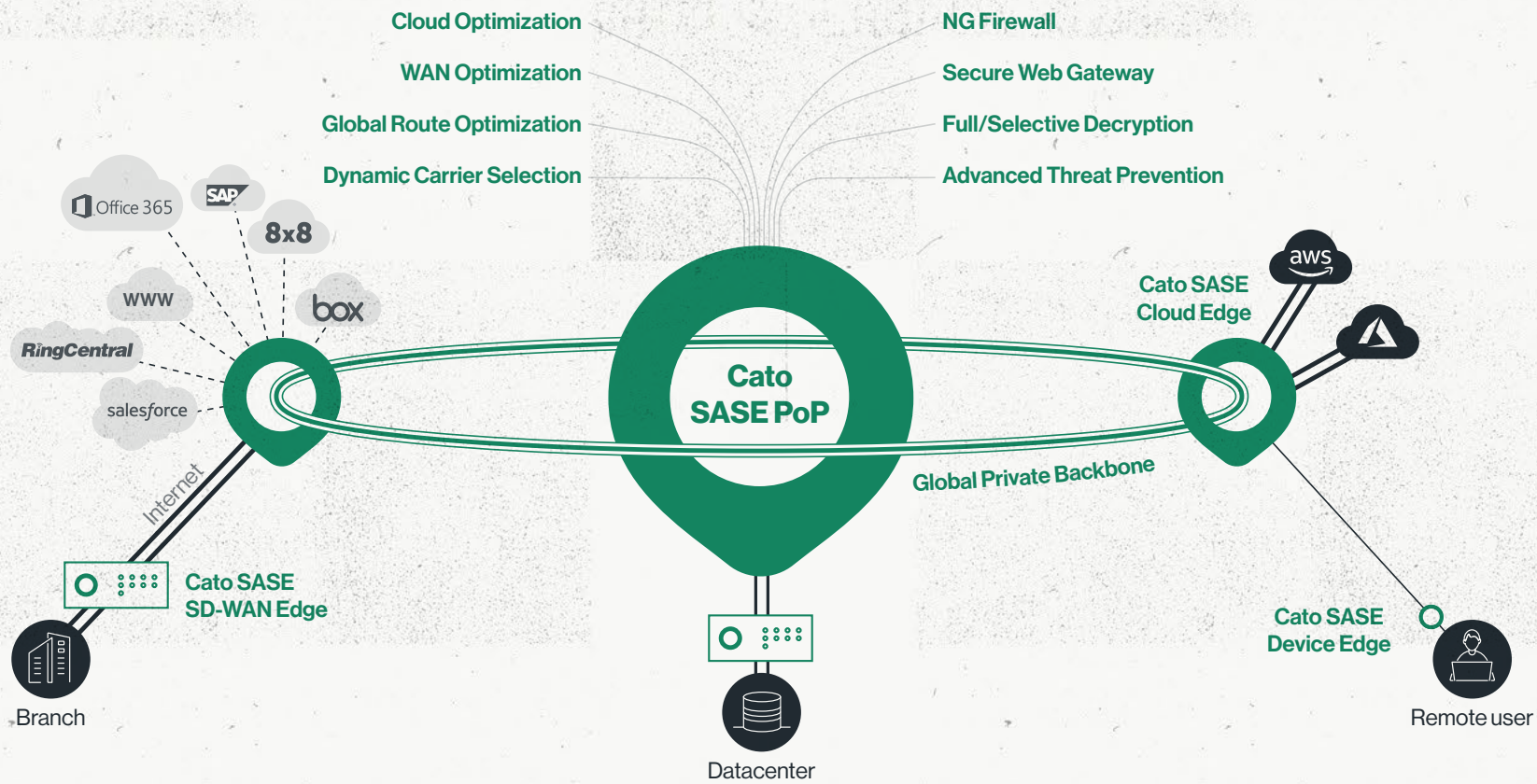
With SASE, IT and security teams can adapt easily and quickly to the evolving needs of their business, as they support the digital workforce anywhere and anytime, and deliver optimized performance and advanced security that promotes growth and ensures business continuity.



About Cato Networks

Cato is the world's first SASE platform, converging SD-WAN and network security into a global cloud-native service.

Cato optimizes and secures application access for all users and locations. Using Cato SASE Cloud, customers easily migrate from MPLS to SD-WAN, improve connectivity to on-premises and cloud applications, enable secure branch Internet access everywhere, and seamlessly integrate cloud data centers and remote users into the network with a zero-trust architecture. With Cato, your network and business are ready for whatever's next.



For more details, please contact your
Bytes Account Manager
 Email us on tellmemore@bytes.co.uk
 Call us on +441372 418500



Cato SASE. Ready for Whatever's Next

Cato SASE Cloud

- [Global Private Backbone](#)
- [Edge SD-WAN](#)
- [Security as a Service](#)
- [Cloud Datacenter Integration](#)
- [Cloud Application Acceleration](#)
- [Secure Remote Access](#)
- [Unified Management Application](#)

Use Cases

- [MPLS migration to SD-WAN](#)
- [Optimized Global Connectivity](#)
- [Secure Branch Internet Access](#)
- [Cloud Acceleration and Control](#)
- [Remote Access Security and Optimization](#)
- [Flexible Management](#)

