VIEWPOINT

SIMPLIFY YOUR ENTERPRISE SECURE ACCESS FROM ANY LOCATION ON ANY DEVICE WITH SASE ZERO TRUST

This paper highlights the permanent move towards hybrid working and some of the challenges created for enterprise security teams. Find out why enterprises are moving towards a Zero Trust SASE architecture, such as reducing the risk of cyber-attacks and optimizing costs. Read the paper and gain an overview of the Infosys model, powered by Zscaler Zero Trust SASE technology.

zscaler™

Infosys®
Navigate your next

Introduction

Hybrid working has become mainstream and the need to secure the Work from Anywhere (WFA) workforce is a priority for IT teams. During the pandemic, organizations put in place temporary or short-term measures to enable the staff to be able to continue to work remotely and securely.

> The Zscaler work anywhere dashboard shows that remote workers globally went from 14% of the workforce pre-pandemic to stabilizing around 40% by the end of 2021.[1]

Some organizations have started to encourage staffs to return to the office to foster collaboration and embed company culture, however the trend towards being able to be more agile and work anywhere looks set to stay; the pandemic showed that teams could still be productive and collaborate using virtual tools.

This model of working has proved to be popular with staff, particularly white-collar workers, helping organizations to retain talent and demonstrate their forward-thinking outlook. Some employees have reported that a hybrid approach to working is the equivalent of an 8% pay rise.[2]

Vibrant workplaces, cloudified applications, and digital transformation demand simplified, secured access from any device, any application, and any location, and need to be able to work effectively and scale based on requirements on an ongoing basis.

The hybrid workplace creates additional security challenges for IT teams as not all employees have a secure connection. It therefore becomes a challenge to provide 100% secure access with traditional methods such as VPN. The surface area to protect has widened, creating increased risks and complexities for IT teams.

IT teams need simple secure access services right to the edge that are easy to deploy and manage and are intuitive for end-users, providing a great digital user experience with the option for the business to scale access up or down as needed.

> Gartner predicts that by 2023, 60% of enterprises will phase out most of their VPNs in favor of zero trust network access.[3]

The combination of Secure Access Service Edge (SASE) and Zero Trust is seen as a potential model to adopt for organizations that are accelerating cloud-first digital transformation. SASE has four main traits: it is identity-driven, has cloud-native architecture, supports all edges, and is globally distributed.[4]

Why are enterprises investing in SASE and Zero Trust?

There are several reasons that enterprises are moving away from traditional methods and towards a SASE Zero Trust approach. Organizations require a solution to enable the WFA workforce that is both secure and cost-effective. The risk of a security breach is significant both in terms of the potential cost to the business due to lost productivity and brand damage.

Infosys and Interbrand, a global brand consultancy firm, launched a join study in 2021 titled "Invisible Tech. Real Impact. that examined the long-term impact of data breaches on the value of brands across sectors. The study revealed that:

SASE is one way to mitigate the risk of rising cybersecurity attacks as it places the Zero Trust focus on users and security policies rather than data environments.

> The potential risk in brand value due to data breach to the world's 100 most valuable brands could amount to as much as $223b.[5]

Continuous security controls can be implemented within and outside the perimeter, i.e., across people, devices, data, networks, and workloads. Implementing a SASE architecture enables organizations to minimize threat posture and maximize user experience. Zero Trust-based access provides secure user access with multi-factor authentication. Access can be based on multiple pre-set parameters such as date, time, location, device, etc.

> By 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at year-end 2018 Gartner [6]

Enterprises that are moving to the cloud need comprehensive cloud protection. Customers need a Security-as-a-Service (SaaS)-based architecture that is agile and compatible with on-premise and cloud set-up across multiple clouds. SASE architecture helps accelerate cloud adoption by removing network and security friction through a consolidation and simplification of IT services. By removing the need for device management and separate services, it creates a frictionless and transparent experience for users.

External Document © 2022 Infosys Limited

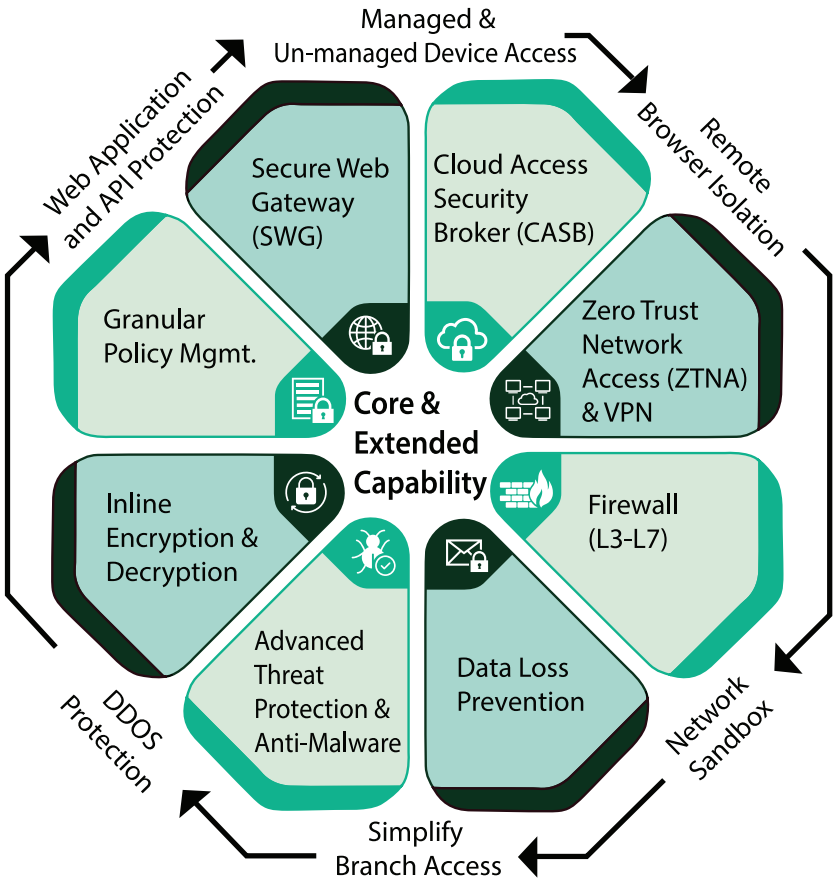
Enable people to work securely from anywhere using Zero Trust SASE architecture

Security is built into the core of SASE architecture. From Secure Web Gateway (SWG) to Cloud Access Security Broker (CASB) and Zero Trust Network Access (ZTNA), all connections are inspected regardless of user, endpoint, app, or encryption.

Uniform protection is provided to users independent of network location, protecting cloud workloads, and automatically remediating cloud security gaps. IT teams can quickly build and deploy access policies based on the applications that communicate, helping to deliver an improved user experience, while protecting the network.

This type of architecture can reduce security risks enabling employees enterprise applications access without placing them on the network, reducing the risk of an inadvertent attack across your corporate network. Direct connections eliminate backhaul traffic need through centralized security controls adding latency and decreasing user experience. As a globally distributed architecture, global coverage further limits the need to backhaul data, improving performance, user experience and reliability for a hybrid workforce.

This model provides improved operational simplicity for IT through increased agility and collaboration among application, network, and helpdesk operations teams. Teams can microsegment enterprise IT assets using remote policies, allowing real-time easy access on a need basis. This reduces the amount of time spent resolving end-user incidents, freeing up resources to focus on strategic digital transformation projects and allowing employees to be more productive.



Infosys SASE Zscaler offering – Comprehensive secure access solution with a cloud first approach

The Infosys SASE solution delivers comprehensive cloud security capabilities in addition to eliminating traditional and high cost on-prem solution components such as firewall, proxy, and VPN gateway. With the Infosys SASE offering, we deliver end-to-end zero trust security, minimize threat posture, and maximize user experience.

- Zero Trust Network Access from Zscaler – enhanced security capabilities with cloud centric security controls applied, removing the need for high-cost complex on premises solutions.
- Security as-a-Service model – the ability to scale controls and extend security to users in all situations, creating a more agile security posture.
- Standardized and simplified – polices and standards enforced across the organization and visualized through a single interface for a real-time view.
- Enhanced user experience – simple lightweight agent on device, with fewer security interventions due to granular policy implementation and improved latency thanks to optimized routing and not needing to backhaul back to a single data center.
- Network simplification – reduce the complexity of WAN and MPLS reliance and drive a digital first approach, accelerating cloud transformation.

Confidently deploy SASE with Zero Trust to simplify IT operations and improve user experience for your hybrid workforce

Build SASE Zero-Trust architecture across the enterprise network, improve productivity, and reduce IT costs and complexity with a platform that is a managed cloud-based SASE service. Enable secure digital transformation without the technical debt of legacy architectures or VPNs.

Reduce risk with a proxy-based architecture that inspects encrypted traffic at scale for threat protection and data loss prevention. The standardization of security controls is critical to ensure users are protected from advanced threats and zero-day exploits.

Secure and future-proof your flexible hybrid workplace and improve user experience. Security policy enforcement is brought closer to users, delivering better performance for users.

> Recent research reports state that companies having the most improved cybersecurity outcomes over the past two years are 5x more likely to have streamlined operations enterprise wide.[7]

External Document © 2022 Infosys Limited

Conclusion

As with any enterprise solution, one size does not fit all, but technology, architecture, and global coverage are key considerations for deploying SASE.

Infosys CyberSecurity assures digital trust by driving a mindset towards 'Secure by Design,' building a resilient cybersecurity program to 'Secure by Scale' and adopting newer technologies to 'Secure the Future.'

Benefit from an industry-leading Zscaler Zero Trust technology solution that can integrate with existing deployments and scale delivered by experts in SASE and managing multi-cloud environments.

To find out more about how SASE with Zero Trust could support your business needs, please email CyberSecurity@infosys.com

References:

1. https://www.zscaler.com/threatlabz/work-from-anywhere-dashboard
2. https://www.economist.com/business/2022/04/09/how-to-make-hybrid-work-a-success
3. https://www.networkworld.com/article/3487720/the-vpn-is-dying-long-live-zero-trust.html
4. https://securityintelligence.com/articles/what-is-sase-zero-trust/
5. https://www.infosys.com/services/cyber-security/insights/brand-impact-databreaches.html https://www.computerweekly.com/opinion/Security-Think-Tank-SASE-will-become-operational-reality
6. https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights/organisational-complexity.html

External Document © 2022 Infosys Limited

For more information, contact askus@infosys.com

Navigate your next

© 2022 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.