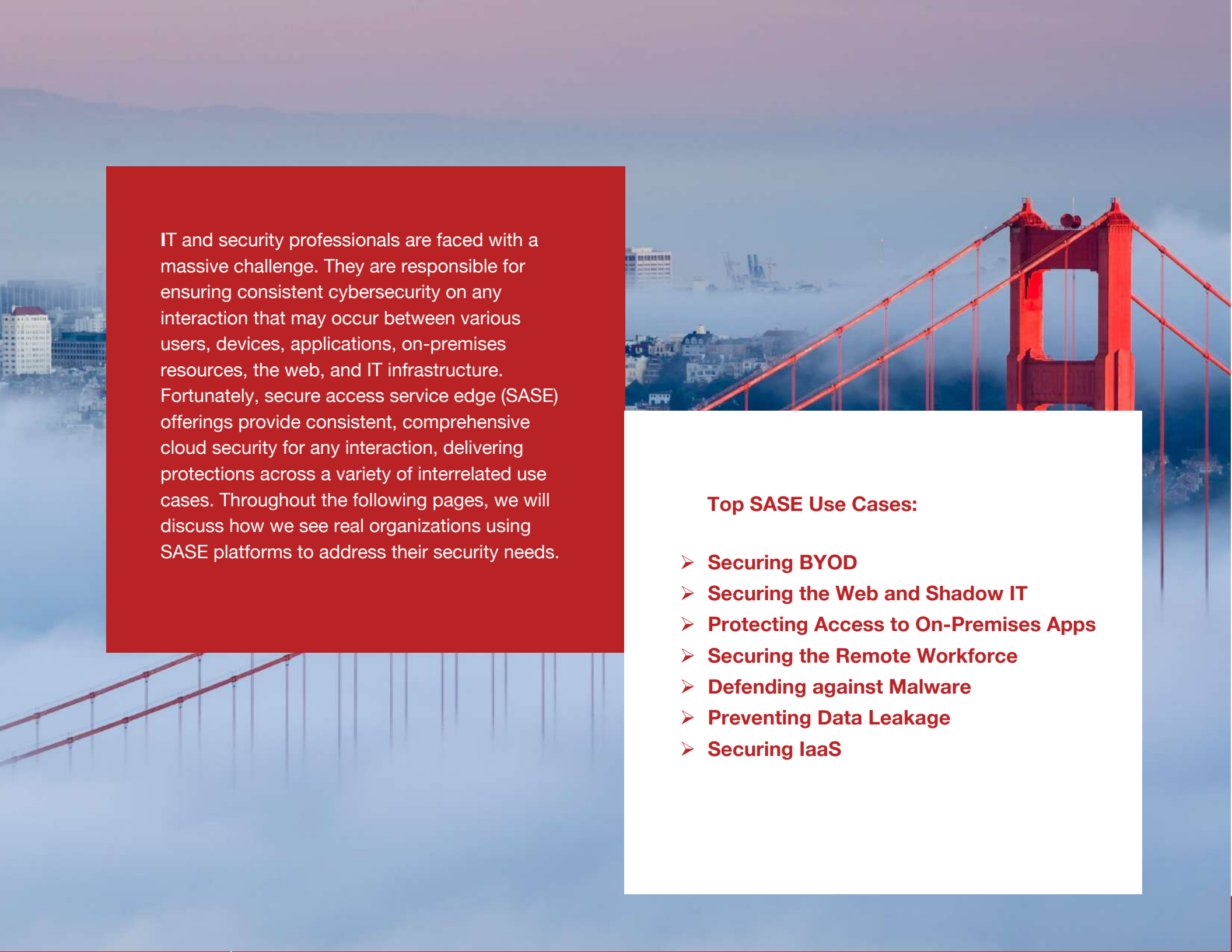




 bitglass

| Top SASE Use Cases



IT and security professionals are faced with a massive challenge. They are responsible for ensuring consistent cybersecurity on any interaction that may occur between various users, devices, applications, on-premises resources, the web, and IT infrastructure. Fortunately, secure access service edge (SASE) offerings provide consistent, comprehensive cloud security for any interaction, delivering protections across a variety of interrelated use cases. Throughout the following pages, we will discuss how we see real organizations using SASE platforms to address their security needs.

Top SASE Use Cases:

- **Securing BYOD**
- **Securing the Web and Shadow IT**
- **Protecting Access to On-Premises Apps**
- **Securing the Remote Workforce**
- **Defending against Malware**
- **Preventing Data Leakage**
- **Securing IaaS**

Securing BYOD

Overview

Bring your own device (BYOD) is a system by which employees perform their work duties from personal endpoints. This requires thorough security, but traditional agent-based tools are poorly suited for the job. Security teams often find it difficult to have access to personal devices, and many don't even have visibility into all of the personal endpoints that are being used for work purposes. Additionally, users are often concerned about agents on personal devices giving IT full visibility into their personal apps and data.

SASE platforms deliver BYOD security through multi-mode cloud access security brokers (CASBs) that provide agentless deployment options. As they forgo agents and leverage reverse proxies instead, these cloud-based rollouts monitor access to only managed IT resources like corporate SaaS and IaaS instances. This means that they give real-time visibility and control over enterprise data on personal devices without monitoring users' personal information.

SASE platforms deliver data protection capabilities like data loss prevention (DLP) and cloud encryption, as well as threat protection against malware and malicious and careless insiders. They also provide visibility through comprehensive logging of all user, file, and app activity, and perform identity and access management functionality like single sign-on (SSO), multi-factor authentication (MFA), and contextual access control. Unintrusive device-level controls are also available, including auto-lock time limits and requiring PIN codes instead of swipe patterns to unlock phones.

Real-World Scenario

Travis, an HR contractor, has his managed laptop break one day while he is traveling. Unable to get an immediate replacement from IT, and needing access to Office 365 to perform his work duties, Travis begins to use his personal iPhone. Because the company he works for uses a SASE platform with agentless CASB functionality, he merely logs into Office 365 via SSO on his iPhone and is granted access. The CASB then agentlessly applies real-time policies to protect sensitive data; for example, by denying access to highly sensitive folders in OneDrive or by encrypting or watermarking downloaded files. With an alternative tool like mobile device management (MDM), Travis' IT department would have to access his device and install an agent before he could use it for work purposes (not to mention that privacy concerns would likely make Travis hesitant to allow this on his personal iPhone).

Securing the Web and Shadow IT

Overview

While the web is an indispensable asset for any organization, it can also disrupt a firm's productivity, leak sensitive data, and enable malware infections. Secure web gateways (SWG), a core component of SASE platforms, are designed to address these needs. SWGs can control access to websites and unmanaged applications by category (gambling, sports, streaming, pornography, malware, phishing, and countless others) and destination trustworthiness. Additionally, uploads of sensitive data to the web can be prevented by automated policies. In other words, these tools block threats, stop leakage, and enhance productivity.

Organizations must consider solutions' architectures when evaluating the SWG components of SASE platforms. Hardware appliance SWGs are costly to buy and maintain, require VPN for off-premises access, and have fixed capacities that make scaling highly difficult. Cloud proxy SWGs don't require appliances, but do require a latency-inducing network hop to the proxy. Additionally, as all traffic is decrypted and inspected at the proxy, including users' personal traffic, user privacy is not respected. On-device SWGs that locally perform decryption and inspection are ideal. This approach circumvents the need for appliances, network hops, and VPNs. This ensures security, performance, and scalability. As only security events are logged and uploaded to the cloud, user privacy is respected, as well.

Real-World Scenario

Consider Jacob, a marketer who is prone to clicking links that he receives via email without any consideration for who the sender is. One day, he receives a message from a convincingly spoofed email account that appears to be a coworker; it contains a link to a spoofed website that is designed to steal his corporate credentials and infect him with malware. Although Jacob does click the link, his employer has an on-device SWG in place that automatically prevents him from reaching his destination; the URL is identified as malicious and an appropriate policy (block) is triggered. Jacob's employer previously used an appliance-based SWG, but found that its fixed capacity created scalability and performance issues that disrupted user productivity as the company grew. With an on-device SWG installed directly on Jacob's endpoint, his employer was able to achieve web security while maintaining a streamlined user experience that didn't impede his productivity or privacy.

Protecting Access to On-Premises Apps

Overview

On-premises applications house large amounts of organizations' most sensitive data. Historically, access to these resources was controlled by requiring employees to use VPN (virtual private network) in order to establish secure tunnels to the network; however, this approach relies upon costly appliances, is not scalable, introduces latency into the user experience, and gives employees unfettered access to everything on the network, violating the core principles of zero trust security.

Zero trust network access (ZTNA) is another critical aspect of SASE. SASE platforms with ZTNA are designed to extend true, zero-trust secure access to specific on-premises resources (rather than open access to the entire network). Ideally, these solutions forgo the use of private data centers and hardware appliances, and are deployed in the public cloud for scalability and performance. Additionally, they should offer an agentless deployment option for browser apps (which is particularly helpful where personal device access challenges the use of endpoint installations), as well as an agent-based option for controlling thick client apps like SSH and remote desktops. Once SASE platforms are deployed, they can then enforce real-time data and threat protection policies in order to defend sensitive or regulated information, block uploads of malware, and extend contextual access to key apps, files, and folders.

Real-World Scenario

While working from home, Samantha, a product manager for a technology company, realizes that she needs access to her employer's on-premises instance of Jira from her personal laptop. With agentless ZTNA in place, she authenticates via single sign-on and accesses the app. She is able to view most of the app's contents, but a preset policy prevents her from seeing mission-critical information remotely on her personal device. Additionally, when she attempts to download highly sensitive files, she is only given read-only access in a browser window that requires additional authentication. This kind of granular data protection is not available with VPN. Additionally, as VPN appliances have fixed capacities and lack the infinite power of the cloud, they are incapable of scaling with organizations as they grow or as more users move off premises. This means that VPN customers have to reactively purchase and install better or additional appliances as they scale, creating an expensive bottleneck.

Securing the Remote Workforce

Overview

Remote work is now the new normal, and organizations around the globe are reaping benefits like enhanced productivity and flexibility. However, it is highly challenging to protect employees working outside of the office and beyond the traditional perimeter defined by firewalls and proxy-based secure web gateways. Fortunately, upgrading to a modern SASE platform allows employees to safely access managed and unmanaged applications, cloud services, websites, and proprietary applications in the public cloud and in private data centers.

While legacy, network-oriented tools like VPNs were once the standard for securing the remote workforce, their cost, complexity, and scalability issues make them a poor choice for securing the remote workforce today. Fortunately, leading SASE offerings circumvent the need for VPN, hardware appliances, and backhauling traffic. Additionally, when they boast a cloud-native architecture, they are able to scale seamlessly as organizations' load profiles change--whether they are growing or their workforce is just shifting geographically.

SASE platforms leverage CASB, SWG, and ZTNA technology to secure remote workers on managed SaaS and IaaS instances, web destinations and shadow IT, and on-premises applications, respectively. From a single enforcement point and in real time, they detect sensitive data, prevent leakage, stop the spread of malware, filter unsafe content, authenticate users, and ensure consistent, granular security for any interaction.

Real-World Scenario

Johan, a sales representative for a large insurance company, works remotely from his home. To do his job effectively, he needs continual access to Salesforce. His employer, aware of the sensitive customer information within its Salesforce instance, encrypts the data at rest via SASE, and requires remote employees to undergo multi-factor authentication (MFA) before they can view it. One day, Johan decides to store some of his client quotations in his personal Google Drive for easy access; however, he is instantly prevented from uploading the files, which contain PII, by his on-device SWG (a core component of leading SASE offerings). This on-device approach to web security is the ideal fit for remote workers, as it doesn't require latency-inducing network hops, performance bottlenecks at on-prem appliances, or productivity-inhibiting VPN. With SASE, Johan's organization is able to detect and remediate inappropriate uploads and downloads of PII in real time and wherever its workforce goes.

Defending Against Malware

Overview

Threats like malware are the scourge of the modern enterprise. In recent years, worldwide infestations of ransomware like WannaCry and Petya brought countless organizations to their knees. Security teams need advanced threat protection (ATP) solutions in place for every attack vector that could be targeted by malware. Given the realities of cloud, BYOD, and remote work, ATP is no longer just for the perimeter or the endpoint. As SASE platforms ensure consistent security for any interaction in the cloud, in the web, and in on-premises resources, they are the ideal tools for comprehensive ATP. They take a three-pronged approach to blocking malware with CASB, SWG, and ZTNA functionality, and typically leverage integrations with leading AV providers like CrowdStrike and Cylance in order to identify zero-day threats.

SASE platforms prevent malware from spreading across organizations' managed SaaS, IaaS, and on-premises applications. They block threats in real time as they are uploaded to applications or downloaded to devices, and remediate threats already at rest by crawling apps' contents. Some SASEs can do this agentlessly, meaning that they can defend against malware even on personal devices. In order to address another key link in the attack chain, SASE is also designed to block threats on the web. If users attempt to click on malicious URLs that would take them to websites designed to infect their devices with malware, then access to said websites will be blocked.

Real-World Scenario

Christina works in finance for a large pharmaceutical firm. Her organization uses a variety of cloud and web applications, spanning Office 365, Slack, and G Suite. One morning, she works from home on her personal laptop which, unbeknownst to her, is infected with malware. When she attempts to share an infected file with a coworker via Slack, her employer's SASE platform agentlessly blocks the upload to the app and explains that the file contained malware. Later that day while working from her managed laptop, she receives a spoofed email from what appears to be IT, stating that her Office 365 credentials have expired. Without thinking, she clicks on the URL in the email to reset her password. Fortunately, her employer's fully featured SASE includes an on-device SWG that prevents her from accessing the malicious web destination which would have infected her with malware. In a world with personal devices, infinite threats, and dynamic remote workforces, organizations need agentless security for BYOD as well as on-device SWG functionality that forgoes the use of VPNs and appliances.

Preventing Data Leakage

Overview

Organizations are full of sensitive and regulated data; from personally identifiable information (PII) and payment card industry data (PCI) to protected health information (PHI) and beyond. If this information leaks, it can harm data subjects (exposing them to identity theft and spear phishing schemes), lead to regulatory noncompliance and the incurrence of corresponding fines, breed legal battles with high fees and penalties, and create a loss of brand reputation that impacts overall business success.

A key purpose of SASE platforms is to prevent leakage in a consistent, comprehensive fashion regardless of the app, device, or attempted action. This is achieved through an integrated approach that encompasses the capabilities of complementary technologies like CASBs, SWGs, and ZTNA. Consequently, SASE platforms provide a single dashboard for configuring policies that are enforced consistently wherever data goes--across managed apps, the web, and on-prem resources. They secure data at rest in managed cloud apps through DLP capabilities like quarantine and encrypt, and prevent leakage at access with real-time capabilities like redact and DRM. Should users attempt to exfiltrate data through a website (whether personal email, Dropbox, or something else), then the uploads will be prevented in real time. Finally, when it comes to securing on-premises applications, SASE platforms can prevent users from accessing or leaking sensitive files by applying granular policies like those mentioned above.

Real-World Scenario

Kaito is a physician for a healthcare firm. While collaborating with a colleague, he decides to download some of a patient's PHI from an internal application onto his personal device so that he can send it to his peer's personal email for her inspection. However, the healthcare firm has a SASE platform that identifies the sensitive information, determines the data shouldn't be on an unmanaged endpoint, and blocks the download. Next, while using a managed device, Kaito tries to upload the patient's record to his personal Dropbox instance so that he can access it on his personal phone. Upon accessing Dropbox, he is presented with a coaching reminder from IT to use his organization's secure OneDrive instance. He disregards the message, but when he attempts the upload, the sensitive data pattern is detected once again, and the leakage is prevented in real time. Only SASE platforms can prevent leakage in this consistent, comprehensive fashion.

Securing IaaS


Overview

Infrastructure as a service is one of the fastest growing segments of cloud computing. Due to IaaS platforms like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), organizations are leveraging cloud-based infrastructure that is outside the reach of traditional, perimeter-based security tools. While IaaS platforms provide some native security and compliance features (such as admin transaction logging), there are manifold gaps. The good news for the enterprise is that SASE is perfectly suited to secure IaaS instances. This is largely accomplished through capabilities that find their roots in cloud access security broker technology.

SASE platforms take a three-pronged approach to IaaS security. First, they crawl data at rest within offerings like AWS S3 in order to identify sensitive data that has made its way into the platform. If sensitive data is discovered, it can then be encrypted according to preset policy in order to prevent unauthorized viewing and usage. In addition to data at rest, SASE offerings also secure access to custom applications built on IaaS platforms. Access can be governed by contextual variables like user group, device, location, and even custom factors. Finally, cloud security posture management (CSPM) tools scan IaaS instances for misconfigurations as defined by compliance frameworks (including the CIS Benchmark, HIPAA, and PCI DSS) in order to prevent leakage and noncompliance; for example, by detecting public-facing buckets that contain confidential information. Once issues are identified, they offer custom-tailored remediation steps and even automatic remediation.

Real-World Scenario

While in a hurry to get home one day, Sawraj, an AWS administrator at a security company, accidentally makes an S3 bucket that contains proprietary information public facing. As he rushes to his car, a sticky note with his AWS credentials falls off of his laptop and onto the ground, where it is later grabbed by an employee of a competitor. Fortunately, Sawraj's employer has a SASE platform in place. Through CSPM, it quickly detects and automatically remediates the bucket's misconfiguration. Later that night, when the competitor attempts to use Sawraj's credentials to log in, the platform recognizes that the access is occurring on a new device, in a new location, and at an unusual time of day. Consequently, it enforces step-up, multi-factor authentication, requests an SMS token that is sent to the real Sawraj's phone, and successfully prevents the malicious actor from gaining access.



Secure access service edge platforms provide a comprehensive, integrated approach to security. As the matrix of interactions between users, devices, SaaS apps, on-premises resources, infrastructure, and the web becomes increasingly complex, using a SASE offering is the ideal way to solve a broad set of security challenges in a consistent fashion. With SASE, a single dashboard can be used to configure data and threat protection policies that are enforced automatically wherever data goes.



Top SASE Use Cases

About Bitglass

Phone: (408) 337-0190
Email: info@bitglass.com

www.bitglass.com

Bitglass' Total Cloud Security Platform is the only secure access service edge offering that combines a Gartner-MQ-Leading cloud access security broker, the world's only on-device secure web gateway, and zero trust network access to secure any interaction. Its Polyscale Architecture boasts an industry-leading uptime of 99.99% and delivers unrivaled performance and real-time scalability to any location in the world. Based in Silicon Valley with offices worldwide, the company 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.