INTERMEDIA
CLOUD COMMUNICATIONS

PTS

GUIDE

Intermedia Triple Shield Security™

INTRODUCTION

As cyberattacks become more sophisticated and hackers more aggressive, business communications such as telephone calls, voicemails, text messages, video meetings, customer interactions and file sharing are increasingly targets of attacks. (Emails remain one of the top vectors.) Communicating, collaborating and sharing information are at the heart of every business and hybrid work is driving a growing reliance on cloud technology to connect key stakeholders within and beyond the organization. Your organization's ability to withstand security attacks and avoid breaches is critical to the ongoing success of the business. That's why your cloud communications provider should be as focused on security as they are on industry leading product innovations.

INTERMEDIA
TRIPLE SHIELD
SECURITY™

THE NEED

The conversations taking place in your company and with your customers cover so many topics that should remain confidential, from product development and customer information to employee data, company strategy, and more. In short, your company's intellectual property (IP) is threaded throughout the communications between your employees, customers and suppliers. All of this information is valuable to cybercriminals who will use it against you if they gain access.

You might not realize the scope of the IP footprint created by business conversations that are vulnerable for bad actors to steal and use for malicious purposes. It's not uncommon for an unknown phone caller to join an audio or video conference to listen in on a company meeting. The history of chats and emails can virtually live forever on phones, PCs or company servers. And what about secure files containing contracts, customer or employee information, confidential presentations and more? Are they really secure?

The moment any technology is offered on the open market, cybercriminals are looking for weaknesses to exploit. Your business communications provider plays a pivotal role in helping keep your proprietary data safe. If you are not working with a supplier who is continually advancing security as the product evolves, you are at risk.

THE SOLUTION

With Intermedia integrated cloud communication solutions, you get access to continuous state-of-the-art business communication tools that include the latest advances in security at their core, and at an affordable price. Intermedia integrated cloud communications tools give small and medium-sized businesses the kind of reliability and security enjoyed by the biggest Fortune 500 companies. Our Triple Shield Security takes a multipronged approach to protecting your confidential information.

Triple Shield Security – from Intermedia

Not all cloud service providers offer equal security. As a cloud service provider with over 25 years of experience, we place the highest priority on security and have invested heavily in our certified information security staff and security technologies to stay ahead of increasingly sophisticated cybercriminals. Our Triple Shield Security protects customer data through layers of security technology that encompass three main points of potential vulnerability – protecting user access, securing applications, and defending data and the cloud infrastructure.

74%

of breaches involve the human element.

Verizon Data Breach Investigation Report, 2023

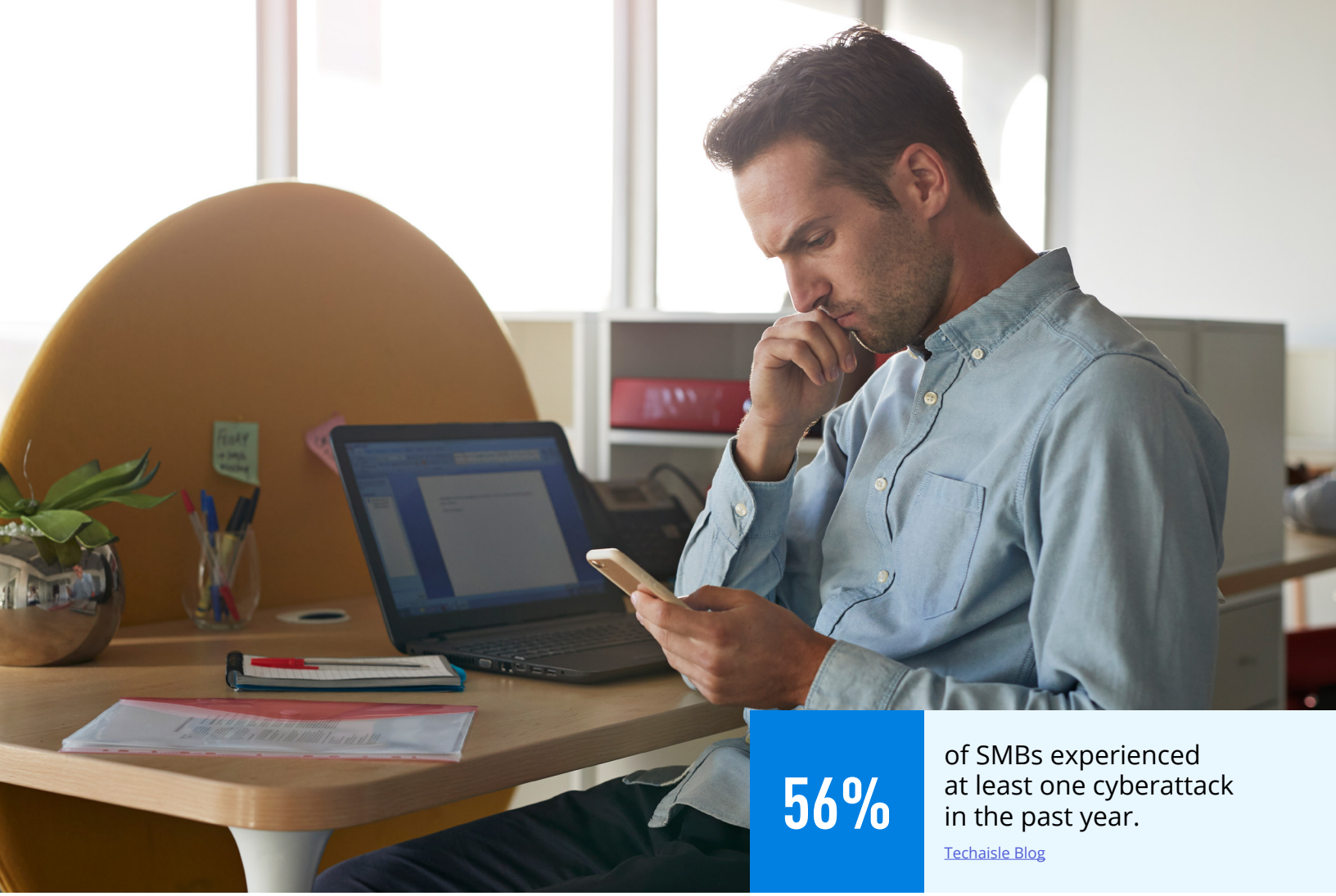
INTERMEDIA TRIPLE SHIELD SECURITY™

1 | USER ACCESS SECURITY

User and administrator access – whether from laptops, desktops, smartphones, or even desk phones — if misplaced, misused, or compromised — can become the access point for cybercriminals to access your entire company's proprietary data.

That's why user and administrative credentials are a primary target for hackers. Compromised access is frequently used by hackers for lateral movement to get access to other users and other systems, and administrative access is among the most prized target for hackers.

Intermedia's user access security shields your company from unauthorized access, regardless of device or location. Easy-to-operate access controls allow your administrators to better manage user security — whether through authentication, sophisticated password management, geo-fencing, suspicious login or account compromise detection.



56%

of SMBs experienced at least one cyberattack in the past year.

Techaisle Blog

INTERMEDIA
TRIPLE SHIELD
SECURITY™

2 | APPLICATION SECURITY

Data is particularly vulnerable when it flows between the safe confines of your secure cloud and your users' mobile and desktop applications. Cybercriminals can exploit vulnerabilities of in-transit data across complex environments and applications for malicious intent.

Intermedia's Triple Shield Security helps you foil attempts to access your company at the application layer. We employ encryption, both in-transit (using TLS encryption) and at-rest (using AES 256-bit keys), as an essential component of our "secure-by-design" product architecture to help keep your data private and secure. Data encrypted while at rest includes voicemails, call recordings, meeting recordings/chat/notes, chat and SMS history, chat attachments, and files. Applications are penetration tested and reviewed against NIST and ISO security standards.

$3.3M

average cost of a data breach for organizations with <500 employees.

IBM Security – Cost of a Data Breach Report 2023

INTERMEDIA
TRIPLE SHIELD
SECURITY™

3 | CLOUD SECURITY

Our cloud is hosted in geographically dispersed, highly secure and monitored datacenters by certified tier-three providers. All of the datacenters are either ISO 27001-certified or are subject to regular SOC security audits.

Network-based monitoring detection systems are configured to detect attacks or suspicious behavior, and vulnerability scans are performed to identify potential weakness in the security and confidentiality of systems and data. We also run advanced, next-generation antivirus technology across our systems to help detect and deter malicious computer usage that often cannot be caught by conventional methods. The technology monitors for unusual patterns and behaviors, alerting security engineers of suspicious activity, 24x7. This endpoint technology can also help prevent attacks against vulnerable services, data-driven attacks on applications, host-based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (e.g., viruses, Trojan horses, and worms).

IMPORTANT SECURITY QUESTIONS TO ASK

#	QUESTIONS	ANSWERS FOR INTERMEDIA
1	Are passwords checked to make sure they haven't been compromised?	When passwords are set, reset or recovered, they are validated to prevent the use of previously compromised passwords. Administrators can require this check and can also require all users to change their passwords at the next login if there appears to be a risk of compromise.
2	Are users and administrators notified about suspicious login attempts?	When a login to a user's account occurs from a location that the user has never signed in from before, notifications are sent to the user and administrator using default and alternative email addresses so that users and administrators can take immediate action.
3	Can suspicious geographies be locked out from accessing services?	Country-based access controls provide protection against logins from specific geographies and IP addresses that are not appropriate access points for your organization and users.
4	Do privileged accounts require 2 Factor Authentication (2FA)?	Administrative accounts are required to use 2FA to protect against compromises to these privileged accounts.
5	Can user accounts require 2FA?	Administrators can also require 2FA for user accounts to access mobile, web and desktop applications.
6	Are shared files and links automatically scanned for malware and viruses?	Files shared and stored are scanned for malware and viruses during uploads and updates to protect users. Links shared in SMS are also scanned and users are alerted to potential threats.
7	Are all communications and data encrypted?	Encryption is used both in-transit (using TLS encryption) and at-rest (using AES 256-bit keys), as an essential component of our "secure-by-design" product architecture to help keep your data private and secure. Data encrypted while at rest includes voicemails, call recordings, meeting recordings/chat/notes, chat and SMS history, chat attachments, and shared files.
8	Are desktop and mobile apps penetration tested?	We perform regular penetration testing and/or red team assessments on our applications and systems infrastructure using respected independent cybersecurity consultants on at least an annual basis.
9	Are datacenters SOC audited or ISO-certified with current reports available?	All of the datacenters used to deliver the Intermedia services are either ISO 27001-certified or are subject to regular SOC security audits. Each datacenter is closely monitored and guarded 24/7. Secure access is strictly enforced using the latest technology, including electronic man-trap devices between lobby and datacenter, motion sensors, and controlled ID keycards. SOC reports are available on request.
10	Is a certified security team monitoring suspicious activity?	A dedicated, full-time staff certified in information security is involved with all aspects of security, including log and event monitoring, penetration testing, incident response, managing endpoint protection, vulnerability management, perimeter defense, service and architecture testing, and source code reviews.

If your cloud communications provider cannot answer yes to most or all of these questions, your data may be at risk. Reach out to us today to learn more about our Triple Shield approach to securing your business communications.

Professional Telecommunications Services, Inc.

(800) 365-1085

ask@ptscinti.com

www.ptscinti.com