Unified Communications:
Comprehensive Security

TRIPLE GUARD SECURITY™

KEEP YOUR BUSINESS COMMUNICATIONS SECURE

You can feel confident that your private data is safe. Our Triple Guard Security takes a multipronged approach to protecting your business data with technologies that address three potential points of vulnerability – protecting user access, securing applications, and defending the cloud infrastructure. Our system utilizes state-of-the-art technologies designed to constantly monitor for, and defend against, malicious intruders.

Our security platform provides comprehensive security features that are constantly evolving in order to respond to, and help mitigate, potential threats. The platform capabilities and the technologies it employs are regularly examined and reviewed by our security team to help ensure an extremely secure communications and collaboration experience that can be trusted to protect you and your businesses.

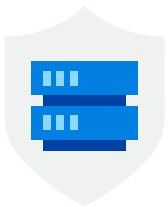Infrastructure & Network Security

Data Protection & Privacy

Phones/Devices/ App Security

Monitoring & Detection

Security Compliance

INFRASTRUCTURE & NETWORK SECURITY

We invest considerable human and capital resources to help ensure high levels of security and protection that give you peace of mind. We understand that if you're to trust us with your communications and data, you need to understand how we'll protect it. Vigilance is essential to keeping your business safe.

Highly Secure Datacenters
Our cloud is hosted in geographically dispersed, highly secure and monitored datacenters by certified tier-three providers. All of the datacenters used to deliver our Unified Communications, Contact Center and Archiving services are either ISO 27001-certified or are subject to regular SOC security audits.

Each of the world-class datacenters that are used in the delivery of services also adhere to adheres to strict standards in physical security. 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 key-cards.

Infrastructure Protection
System and network security is important to us and our customers. In order to maintain a secure infrastructure, the platform is supported by several layers of security controls in operation. These controls include processes for managing user

access to critical systems and devices, formal policies for authentication and password controls, and configuration standards for firewalls. Secure VPN and two-factor authentication (2FA) are widely utilized across the infrastructure to prevent unauthorized access.

We also implemented several monitoring controls to identify potential security threats and notify its personnel of the severity of the threat. Firewalls are in place and configured to prevent unauthorized communications. 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, end point detection and response (EDR) technology across our systems to help detect and deter malicious computer usage that often cannot be caught by conventional methods. The technology uses AI-powered detection and monitors for unusual patterns and behaviors, alerting security engineers of suspicious activity, 24x7.

We utilize a combination of commercial and proprietary security tooling to assist with threat and vulnerability management; security information event management; identity, access, and password audits; secrets and key management; managed detection and response; secure development lifecycle; managed security operations; and bug bounty programs. We also 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.

Other security highlights:

• Commercial-grade edge routers are configured to resist IP-based network attacks

• We subscribe to Distributed Denial of Service (DDoS) protection through a leading provider of network security

• Our production network is physically and logically separated with highly restricted access and multiple authentication levels

• Operational functions include monitoring, system hardening, and vulnerability scans

Employee Security

Our employees, regardless of role, undergo rigorous background checks. Employee access to systems, applications and networks is strictly controlled using two-factor authentication and role-based access control. Access to servers is restricted to a limited number of authorized engineers and monitored regularly.

Dedicated Security Staff and Monitoring

We employ a dedicated, full-time security staff who are certified in information security. This team 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.

DATA PROTECTION & PRIVACY

We are committed to protecting the privacy of your data and making sure you have full visibility regarding where and how it's used. Your cloud contains extremely valuable and confidential content, including intellectual property, customer data, financial information, and sensitive personal data. You need to have confidence in how it's stored and managed.

Locations of Data Handling/Storage
We maintain datacenter locations in the Eastern and Western United States, Canada, the United Kingdom, Germany, Australia, and Japan. With respect to user content that is processed through the service, we generally aim to handle and store such data in the customer's geographic region, when possible.

In instances where a particular service is not able to be serviced through a datacenter in a customer's geographic region, the user content will generally be handled and stored in the datacenter closest to the customer's location.

Data Encryption
Data encryption protects sensitive customer and call data from unauthorized access. In addition, numerous national, local, and industry regulations regarding customer and patient privacy mandate encryption of data. 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 shared files.

PHONES / DEVICES / APP SECURITY

Encryption technology is important to keep conversations and data secure from prying eyes. However, encryption only tells part of the story. We have several technologies designed to keep intruders from accessing your internal systems and apps.

Secure Handset Protection
To verify that phones and devices are secure from cyber threats and attacks like eavesdropping, we require strong passwords on all SIP endpoints. Each device is securely provisioned using "HTTPS" with mutual authentication to prevent intrusion.

Authentication for Apps
Desktop and Mobile Apps allow users to use their business phone system while working remotely or on-the-go. These apps can require a username and password and can also be enabled with 2-factor authentication for access.

Google Chromium Browser Security Platform
The Desktop App is built using Google Chromium browser technology. It makes use of the very latest security enhancements available and is updated regularly to keep current with the latest security patches. Chromium's architecture focuses on preventing attacks from persistent malware, transient keyloggers, and file theft.

MONITORING & DETECTION

Automated 24/7 Toll Fraud & Threat Detection
We monitor call patterns to international (and high-cost) locations on a constant basis and consistently look to improve our fraud monitoring systems.

If any customer exceeds the call thresholds for any international areas, we will disable international calling and notify the purchaser, informing them that international calling has been disabled based on possible fraudulent activity. To protect the customer, we will not re-enable international calling until the account holder has given us authorization.

Spam Caller Protection*
Every account is enabled with Spam Caller Protection – helping to keep you and your employees free from calls originated by autodialers and known fraudsters. It allows administrators to decide how to route these calls. Depending on your organization's preferences, you can tag these calls in the Caller ID screen, send them to voicemail, or block them. This protection extends to every device, including the Desktop and Mobile Apps.

*Currently only available to customers located in the United States

SECURITY COMPLIANCE

SOC 2
SOC 2 is a technical audit specifically designed for service providers who store customer data in the cloud. We have a SOC 2 report from an independent auditor that has validated that, in their opinion, our controls and processes are effective in minimizing risk and exposure to this data.

PCI-DSS
The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store, or transmit credit card information maintain a secure environment.

The payment processing system that supports services has passed these strict testing procedures and is compliant with PCI DSS. This helps ensure that your payment information will not be accessed by unauthorized parties or shared with unscrupulous vendors.

GDPR and Other Privacy Regulations

Our team has extensive experience managing a highly secure infrastructure and complying with complex regulations. As noted earlier in this guide, we are committed to comply with the EU's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and other privacy regulations across our services. We maintain a security environment that meets the requirements of the GDPR, and we offer Data Processing Agreements (DPAs) to our partners and customers to help assure them that our processing and handling of their data will meet applicable regulatory standards, including all required security measures.

Healthcare Industry Security Compliance

Countries around the world impose strict legal and regulatory requirements on the handling of medical and other health-related information by healthcare providers. Our robust set of security features enables customers in the healthcare industry to configure the service to help them comply with those stringent requirements. For instance, the solution offers a range of security settings, and a Business Associate Agreement (BAA) is available upon request, to support businesses in their efforts to comply with the administrative, physical, and technical standards required by the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Telecommunications-Related Security Requirements

Consumers are understandably concerned about the security of the sensitive, personal data they provide to their service providers. Many countries' telecommunications regulations include encryption and other security-related requirements applicable to data processed and stored in connection with the services, and we are committed to complying with those requirements wherever we offer our services. As just one example, the United States Federal Communications Commission (FCC) requires carriers like us to establish and maintain systems designed to ensure that we protect our subscribers' Customer Proprietary Network Information (CPNI), and we file an annual certification documenting our compliance with these rules.

SECURITY FEATURES AND CONTROLS

Security Features

- **Calling** – The account administrator can request TLS transport for desktop telephones

- **Mobile Softphone** – TLS transport can be enabled in application settings to enable encrypted signaling

- **Call Recording** – The account administrator can control call recording on a per user basis. Call recording can be activated on demand by the user

- **Voicemail to Email** – Voicemail to email is a convenient feature but for maximum security it can be disabled per user

- **Voicemail Transcription** – Voicemail transcription can be enabled or disabled on a per user basis for maximum security

- **Visual Voicemail** – Visual voicemail is available in the Desktop and Mobile apps and is protected by the same robust access controls including optional 2FA

- **Desktop Softphone** – The Desktop Softphone uses TLS and SRTP to ensure communication is always encrypted

- **Chat** – Chat messages are encrypted both at rest and in transit

- **File Sharing** – Shared data is encrypted both at rest and in transit

- **Online Meetings, Chat, Notes** – This data is encrypted at rest and in transit. WebRTC technology is used to encrypt meetings

- **Integrations** – Integrations vary depending upon the 3rd party system, but typically use REST over HTTPs transport for encryption
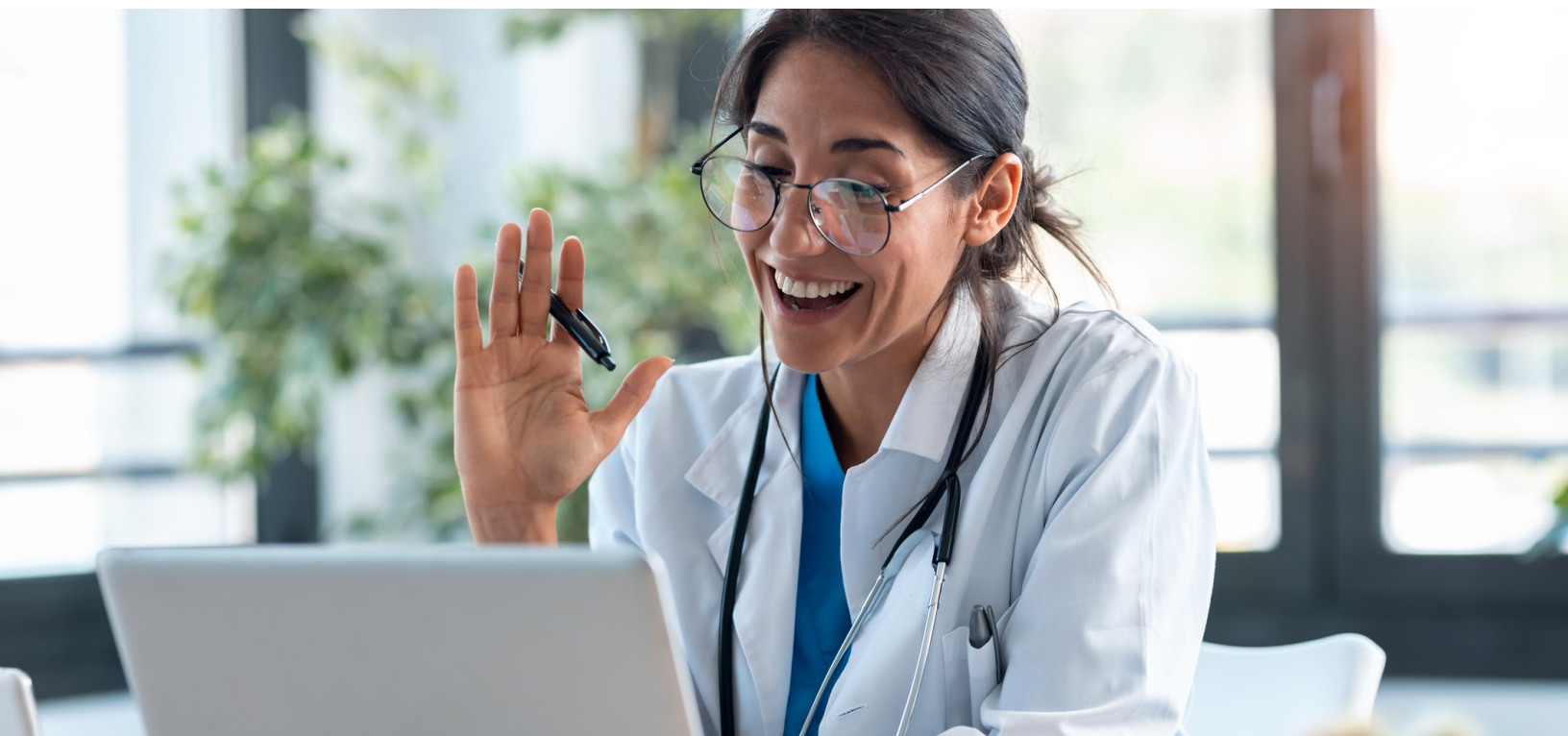
Administrator Control

This integrated cloud communication solutions provides many flexible security features that allow the system administrator granular control over their security policies.

- **Administrator-defined passwords** – The solution supports both user and administrator-defined passwords for access to services

- **No compromised passwords** – Users benefit from password validation services; this prevents users from selecting passwords which are known as compromised

- **Forced password resets** – Administrators can force all users to change their passwords, either for administrative reasons or company policy reasons

- **Custom password policies** – Password policies can be defined to align with existing business practices or policies

- **Flexible password expiration** – Password expiration can be defined to align with existing business practices or policies

- **Dynamic blocking feature** – Administrator-defined policies monitor unsuccessful logon attempts and can dynamically restrict and release user accounts. This feature can be fully customized to align with existing business practices or policies

Two-Factor Authentication

This additional security layer can be activated for Unified Communications, Online Meeting, Contact Center and ShareSync applications. Two-factor authentication (2FA) requires an additional authentication challenge to access services. This feature is fully configurable to suit your business needs.

2FA supports Push Notification via the mobile application, SMS messaging and voice calls. 2FA can be enabled on a per-user or per-organization basis and supports challenges for every login, daily, weekly, monthly or only when logging into services from a new device.

2FA is included with every Unified Communications and Contact Center account.