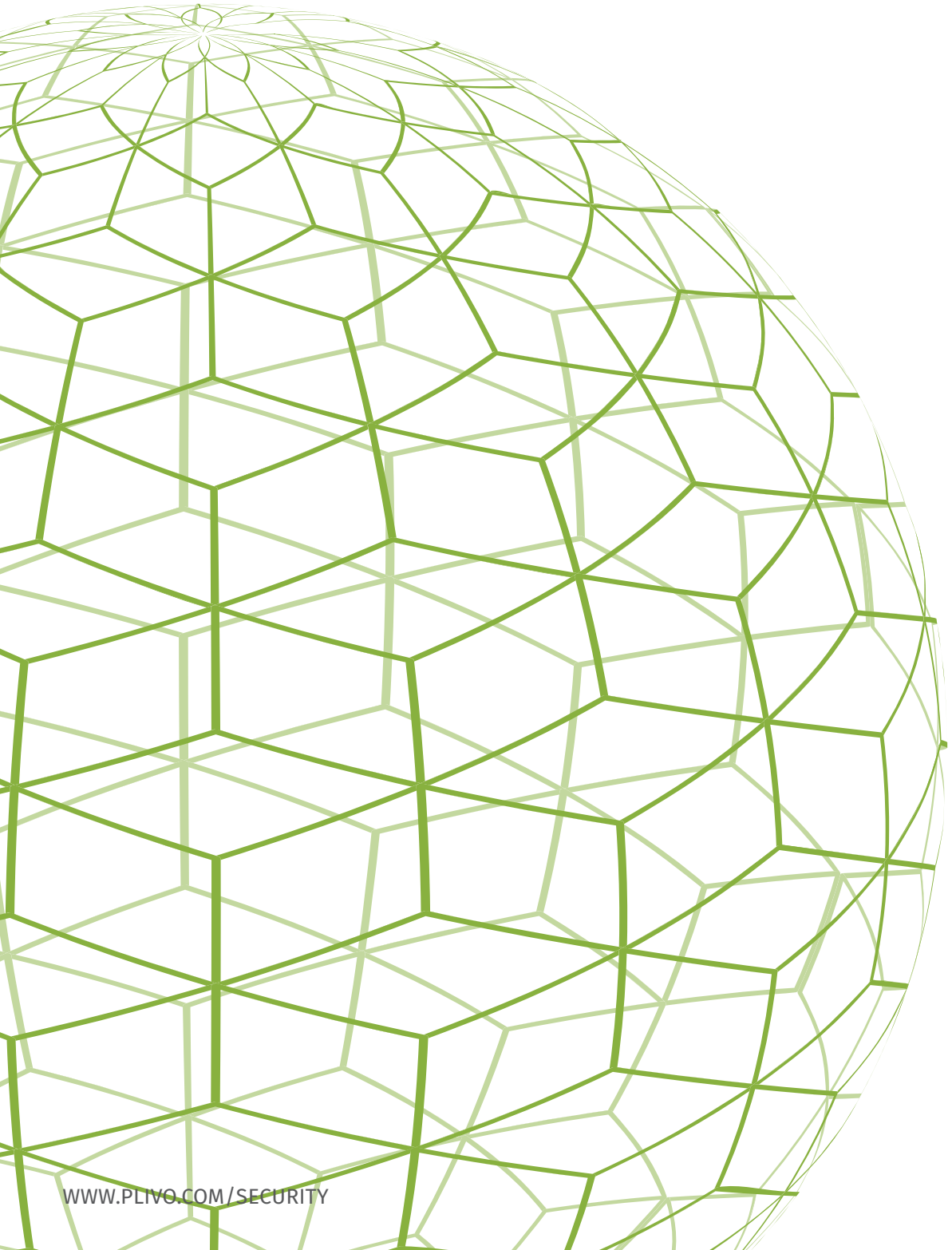
Secure Cloud Communications: Overview of Plivo's Security Architecture and Policies

Build your company on a resilient and highly available communications infrastructure



WWW.PLIVO.COM/SECURITY

plivo

Enterprise Security for Your Cloud Communication Backbone

Plivo delivers scalable cloud communications with comprehensive security at all levels

"We built our infrastructure on Plivo because reliability is at the core of our product. Plivo gave us all the security features that our enterprise solution needs to provide our customers with the best service possible."

- Augustus D., CEO, CallHub

Security is a top priority for Plivo. As an infrastructure company, we are at the core of many businesses around the world. This is why we have used the best security practices and policies to ensure that our network is secured physically, virtually, and that our customer's data and payment information are both private and secure. Our security architecture can be segmented into 5 main components:

Plivo's security practices and policies offer a transparent look into our operations and the support that we offer our customers:

Network Security

Enterprises and SMBs all depend on our network reliability and uptime. This is why our dedicated team guarantees 99.95% uptime by deploying the latest technology and best practices to keep our platform online and performing optimally.

NETWORK FIREWALLS

Each system uses firewalls to restrict access to systems from external networks and between systems internally. To mitigate internal and external risk, access is restricted to only the ports and protocols required for specific business needs.

FULL REDUNDANCY

Redundant links re-route traffic over backup networks in under 2 seconds in case of backbone failover. Multiple instances and redundant servers with active pairs are also triggered automatically in case of failover.

OPTIMIZED LOAD BALANCING

Distributed workloads across multiple resources optimizes response times, maximizes throughput, and avoids single failure points.

CARRIER REDUNDANCY

We aim to connect to multiple carriers in each country. At a minimum, we connect to at least 2 local carriers in each country. In case 1 carrier fails, our systems automatically load balance and diverts traffic through other reliable carriers.

CLUSTERED INFRASTRUCTURE

Automated systems deploys new code to clusters in real time to ensure smooth transitions between software updates with no downtime

Application Security

Thousands of applications communicate with Plivo through our APIs securely and efficiently. At Plivo, we provide three primary methods for application security and authentication.

MULTI-FACTOR AUTHENTICATION

To prevent unauthorized account access, each session requires the account username and a strong passphrase for access to each Plivo account. All accounts also require a phone number verification delivered through a SMS text message or a voice call to the user's phone in order to activate new accounts.

AUTH TOKENS AND IDS

HTTPS & unique AUTH ID & AUTH Tokens for every user to ensure the right people have access to your account. This external service authentication can be renewed at any time by generating a new authentication token through the Plivo GUI. We recommend regenerating your auth tokens on a regular basis to ensure that your authentication is never compromised.

TLS ENCRYPTION

All web session traffic between your application and Plivo is encrypted using TLS (transport layer security) to protect all of your data. The TLS protocol provides data encryption and authentication between your application and our servers and prevents third parties from stealing information.

Physical Security

All of our data centers and hosting partners are housed in state-of-the-art facilities with industry standard access controls and physical security measures.

24/7 SURVEILLANCE

Dedicated 24/7 state-of-the-art electronic surveillance and physical security measures at all of our server locations, including foot patrols, security logs, and perimeter inspections.

PERSONNEL AUTHORIZATION

Only authorized Plivo personnel are granted access credentials to our data centers. Every access is also logged and reviewed to ensure that our systems are not breached by internal threats.

HVAC AND POWER STABILITY

All of our facilities offer 100% power and HVAC functionality in any given month with dedicated trained specialists that monitor and maintain hardware components on-site at each of our 5 global points of presence.

SECURITY LOGS

All activity on our servers are logged to produce historical reports that enable system change tracking, security analysis, and compliance auditing.

Data Security and Privacy

Our powerful APIs can log and record important user data so that our customers can accurately assess platform behaviors. However, this information can be sensitive as well. This is why we've taken extra precautions to mitigate the risk and threats to our customer data (e.g., account information, call logs and recordings). For customers with sensitive data, Plivo's API also offers a "no log" option, where SMS messages and DTMF are not saved on our systems at any point. Please refer to the Message API and the <GetDigits> XML documentation for more info.

LIMITED ACCESS

Plivo's policies and procedures limits and logs all external and internal access to customer data and requests management approval prior to access. Internally, only select Plivo employees that deal directly with valid customer tickets are permitted to access customer data. These select groups include, customer support, development, and security teams.

BACKUP ENCRYPTION

Regular backups are performed on all Plivo customer data, including account information, call logs, sms logs, and call recordings. All backups are stored redundantly and are encrypted using a 256-bit Advanced Encryption Standard (AES-256), one of the strongest encryption standards available for electronic data.

Payment Security

Security, especially when it comes to payments is a critical component for our customers. This is why we use an industry leading payment platform for all of our transactions.

PAYMENT ENCRYPTION

To ensure that we deploy the highest security measures, we do not store any credit card information on our servers. Instead, all credit card information are encrypted with AES-256 and handled by our payment platform vendor. In addition, decryption keys are stored on separate machines, and the infrastructure for storing, decrypting, and transmitting credit card information runs on a entirely separate hosting infrastructure with a separate secured set of credentials.

PCI COMPLIANCE

Our payment platform vendor is PCI DSS (Payment Card Industry Data Security Standard) compliant. This means that they are validated and held to the same industry standards as all major credit cards including Visa, MasterCard, and American Express.

Operational Transparency

Plivo adheres to high operational standards and provides policies and practices for security audits, incident response, and privacy. Plivo's network status and incidence reports are available in real-time to the public at https://status.plivo.com/.

TRANSPARENT INCIDENT RESPONSE

As part of Plivo's service-level agreements to all customers, Priority 1 (i.e., Business Critical) incidents are monitored and responded to 24/7 and 365 days a year. Our dedicated team also monitors our infrastructure through NOCs (network operations centers) and uses third-party notification and alert systems to identify and manage threats.

PRIVACY POLICY

Plivo's privacy policy is publically accessible via https://www.plivo.com/privacy/ and adhered to by all Plivo employees. As well, only Plivo employees that require customer data access as part of their job function are permitted to access customer data. These select groups include, customer support, development, and security teams.

Regulatory Compliance

Plivo supports many businesses that are compliant with HIPAA Privacy and Security Rules. Even though Plivo is not a covered by HIPAA, our HIPAA-compliant customers have used the following techniques to ensure that they continue to operate under HIPAA Privacy and Security Rules.

SECURE APPLICATION URIS

SIP URI for applications should not be set to "Public". This will ensure that only secure interactions with the proper authentication credentials have access to your applications.

ENCRYPT TRANSMISSION

Ensure that web session traffic between your application and Plivo is encrypted using TLS and transmitted over secure networks.

DISABLE LOGGING

To ensure that protected health information is never transmitted, we recommend turning off logging for DTMF and SMS text messages, as well as using a separate developer account for debugging purposes. Live applications that need to be HIPAA compliant should have logging disabled. Please refer to the Message API and the <GetDigits> XML documentation for more info on disabling SMS and DTMF logs respectively.

The above recommendations is not meant to be a comprehensive list and does not replace official HIPAA standards and guidelines. Please seek legal counsel if you have an application that requires HIPAA compliance.

Let’s Get Started

Contact us at sales@plivo.com

Plivo is a leading cloud API platform and global carrier services provider for voice calls and SMS. Plivo’s mission is to simplify global telecom and enable access to high quality cloud communications at a low price. Currently, Plivo has one of the largest Tier-1 coverage areas in the industry. 1000’s of businesses from SMBs to large enterprises already trust Plivo as their global communication provider.