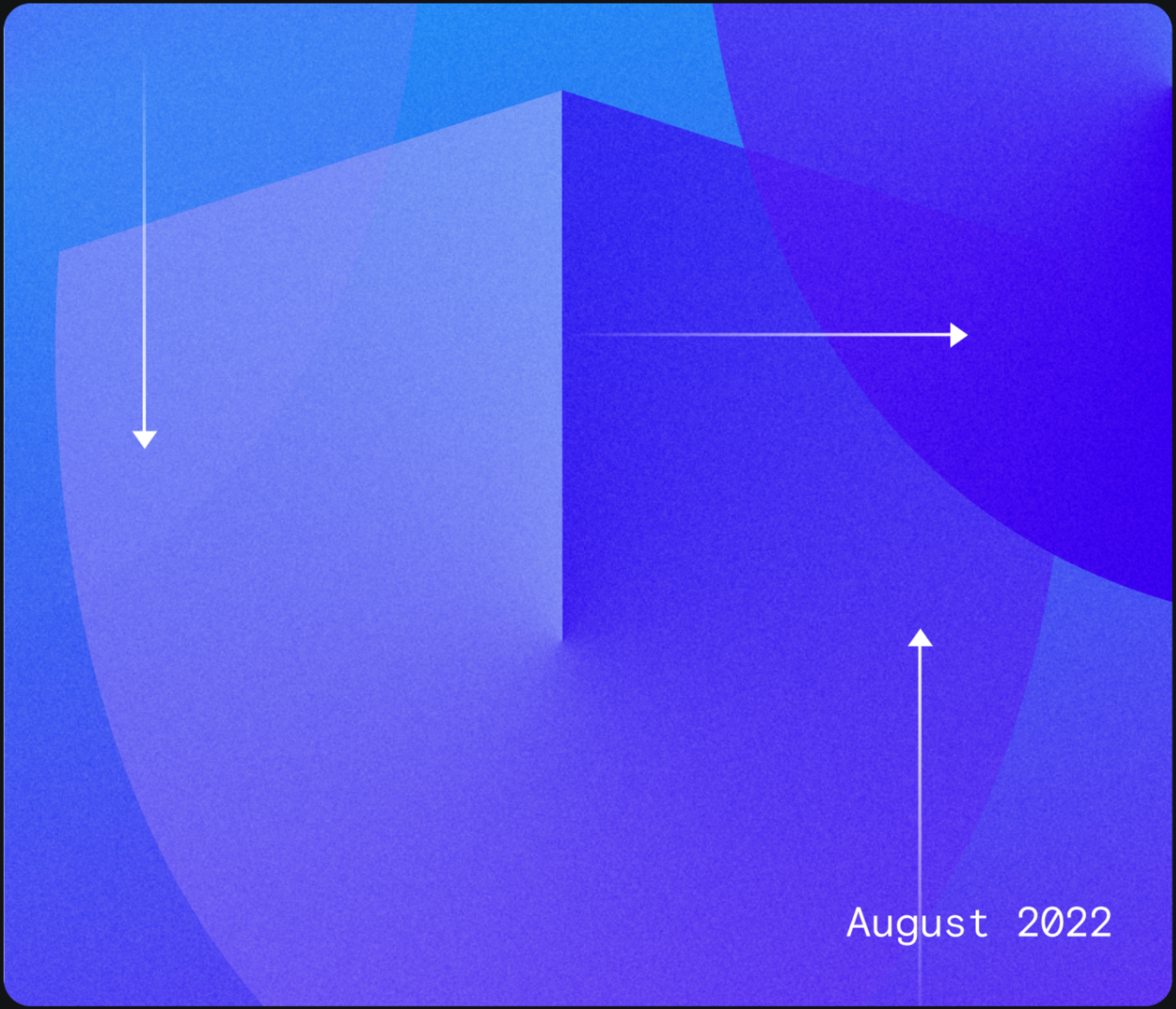
Twingate

Twingate Security Whitepaper



August 2022

Thanks for your interest in Twingate

Twingate helps organizations to improve information security in their organizations by providing a better, simpler approach to securing access to their private network resources and applications. However, to deliver on that promise, we're cognizant that we must first ensure that our own security practices are in order. Customers entrust us with gatekeeping their most sensitive and confidential information, and therefore information security is core to our business and a constant priority that each one of us at Twingate takes seriously.

This document contains information that is intended to provide customers and prospective customers with transparency on and confidence in Twingate's security posture, practices, and processes. While this document represents Twingate's security at the point in time it was last updated, ensuring information security is an ongoing process of continuous improvement, and it is something we do not stop assessing and bolstering.

This document is divided into two main parts. The first describes how Twingate is securely architected from a product perspective, and the second describes Twingate's information security practices generally.

If you have any unanswered questions, you can contact us using the contact details at the end of this document.

About Us

Founded in 2019, Twingate helps organizations to secure and manage access to their resources in a world where people work from anywhere. Twingate aims to make implementing Zero Trust principles accessible to all organizations by providing a secure access solution that doesn't compromise on security, usability, or performance.

Twingate is operated by a globally distributed team of seasoned professionals working in engineering, product management, customer support, and business operations with a long track record of successfully delivering leading enterprise technology solutions. Our team comes from companies like AT&T, Dropbox, Microsoft, OpenDNS/Cisco, Slack, and Sophos. Twingate is backed by investors including WndrCo, BOND, 8VC, Green Bay Ventures, SignalFire, and Dropbox founders Drew Houston and Arash Ferdowsi.

Who uses Twingate?

Twingate is trusted by some of the most innovative, fast-growing companies around the world. Most of our customers are facing similar challenges: juggling efforts to rapidly scale their teams while dealing with the security and operational issues posed by relying on outdated or cumbersome technology. Our customers come from a wide range of industries, including highly regulated ones such as financial services, healthcare, and legal services.

What services do we provide?

Twingate provides a secure access platform that replaces legacy VPNs with a modern Identity-First Networking solution that combines enterprise-grade security with a consumer-grade user experience. It can be set up in less than 15 minutes and integrates with all major cloud providers and identity providers. Twingate helps companies move towards a more secure architecture by enabling all network requests to be screened with the question: “Should *this user* on *this device* under *this context* be allowed to access *this resource*?” Twingate ties every network event to an identity—user, device, and service—giving businesses unparalleled control and visibility over activity across their entire network.

Twingate is delivered as a software-as-a-service (SaaS) product, with downloadable software components that are installed on end user and other devices.

Last updated on August 12, 2022[1]

[1] This document may not be distributed by the intended recipient to third parties without the prior written consent of Twingate. While every effort is made to ensure the information in this document is current and accurate, this information is provided “as is” without any warranty, express, implied or otherwise, regarding such information’s accuracy or completeness. Any practices or policies described in this document are subject to change without notice.

Product Security

1.1. Product Architecture & Design

Overview of Approach

Twingate was designed from scratch to be a foundationally secure solution for modern “work from anywhere” workforces. Modern workforces are becoming increasingly dispersed:

- more **users** are working from remote locations like homes and public venues;
- user **devices** are dispersing among desktop and mobile devices, and work-issued and personal devices;
- **applications** are moving from on-premises to being housed in the cloud or provided by third party SaaS providers; and
- **networks** are increasingly cloud-based and/or managed by third parties.

As a result, the traditional IP address-based, fixed perimeter approach to securing networks and applications does not meet today’s security or usability demands. Twingate’s answer is an approach based on Zero Trust Access concepts that we call Identity-First Networking.

Identity-First Networking

The premise behind Twingate’s Identity-First Networking model is to rethink the base assumptions around networking for the needs of the modern workforce. The dispersal and abstraction (for example, via Infrastructure-as-Code frameworks like Terraform) of users, devices, applications, and networks means that a different approach is needed.

Our identity-first approach starts by asking a simple question: “Should *this user* on *this device* under *this context* be allowed to access *this resource*?” If the answer is no, the network request is not allowed to leave a device. Because network connections are never allowed to enter your network without an identity attached to an explicit authorization, there is no longer any question of who a network connection belongs to and why it was authorized.

This link between network request origination and identity makes it significantly easier to understand activity inside your network. Gone are the days of whitelisting IP addresses, maintaining complex subnet assignments and VLAN segments, or manually piecing together network events across physical networks. Using Twingate, you can give users the flexibility that they need to work from anywhere while remaining confident that every network connection is authorized and audited against a user's identity.

Zero Trust Access (ZTA)

Twingate's architecture has been designed in accordance with key ZTA concepts:

1. Every request to a private resource should be authenticated and authorized based on real-time contextual information, such as user identity, device posture, and other attributes like time, location, etc.

2. Users should only be able to access the minimum resources necessary (principle of least privilege).

3. Events should be extensively logged to support monitoring, detection, investigations, and other analytics.

At a high level, these principles manifest themselves in some of the following ways in our product:

- No single Twingate component can independently make a decision to allow traffic to flow to a secured resource on your remote network. User and data flow authorization is always confirmed with multiple components running multiple checks. Moreover, user data flows and user authentication flows are handled by separate components and require separate validation checks.

- We delegate user authentication to a third party identity provider (IdP), which creates a separation of concerns that provides an additional layer of security.

- We support extensive logging, providing enhanced visibility that helps administrators to monitor, troubleshoot and investigate activity throughout their networks and endpoints - including both unauthorized activity, and activity by individuals who are authorized to access a resource but may be acting outside the bounds of their business authority.

- User data flows are encrypted end-to-end from Client to Connector and typically do not need to transit Twingate infrastructure. Even when network conditions require those data flows to pass through a Relay (a type of component residing in Twingate-controlled infrastructure), Twingate has no ability to decrypt such data. (Encrypted transports never have an intermediate termination/resumption at a Relay.)

- Our lightweight client applications are designed to be always on in the background.

From the customer's perspective, our product architecture provides additional security benefits as it relates to:

- **hiding networks** - Twingate does not publicly expose an access point into your network to facilitate secure remote access to resources inside it. This means customer networks can remain invisible to the public internet, if desired, and free from opportunistic probing from would-be attackers

- **enabling granular access controls at the port level** - this helps to reduce the blast radius of incursions, in contrast to VPNs that provide access to entire networks

- **centralized access management of all private resources** - this helps IT teams to audit and maintain access lists in response to personnel changes

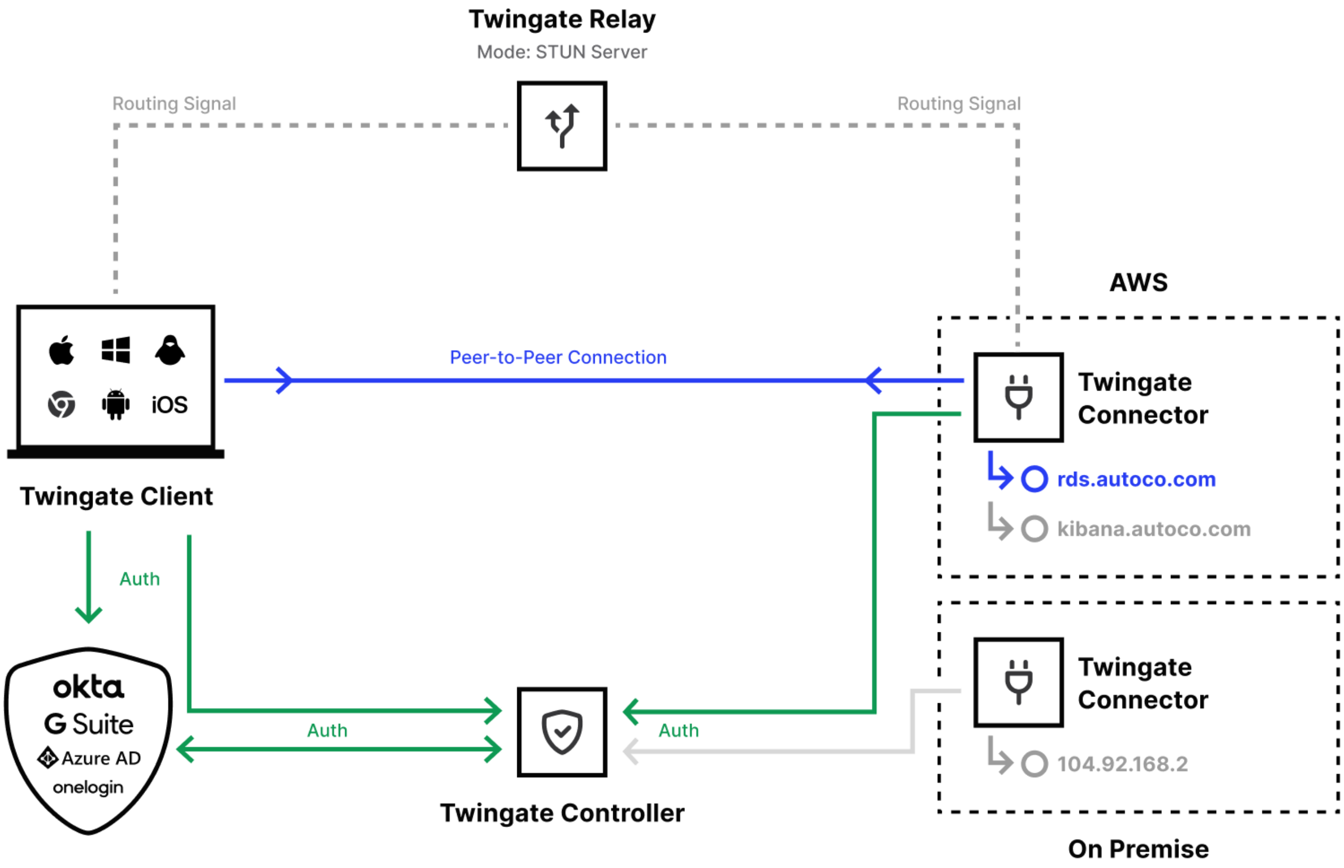
- **centralized logging of all network activity -** identity-indexed logs and analytics can provide deep insight into who is doing what throughout the entire enterprise network

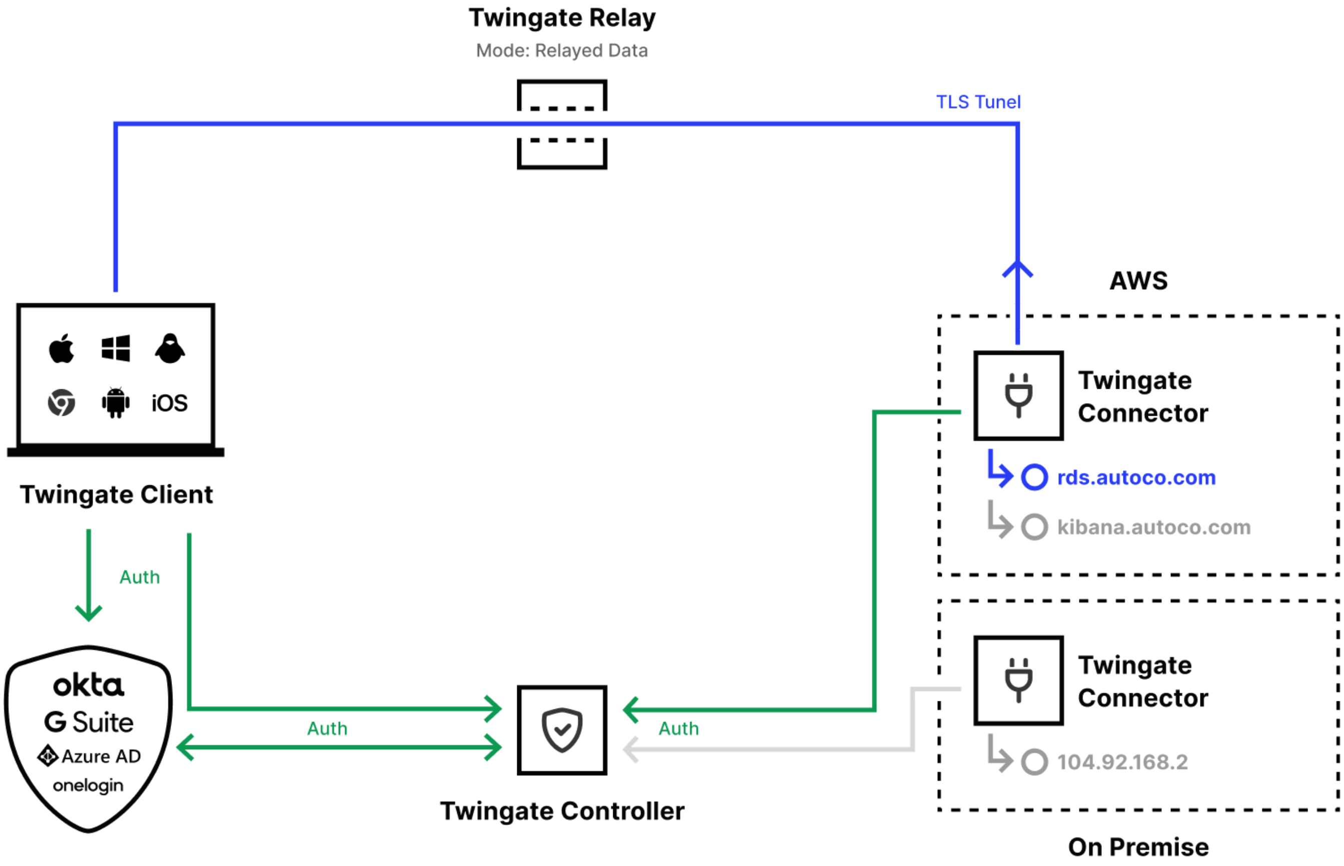
- **better usability for administrators** - solutions that are easier to configure and maintain are less error prone and more effective

- **better usability for end users** - an easy-to-deploy, always-on solution that "just works" and stays out the user's way promotes adoption and avoids the common problem with VPN clients where users switch them off because they disrupt or slow their internet connections

Architecture & Component Overview

This section provides a high level overview of the major components that make up Twingate's architecture and how they interact. Twingate's architecture is explained in depth in our Documentation, which we highly recommend that you review for a more thorough understanding of the security underpinning Twingate.





Twingate secures access to resources on customers' remote networks. Twingate is composed of four main components that work together to ensure only authenticated users are able to access the resources that they have been authorized to access. With Twingate fully configured, the end result is that authorized users can connect to any resource without needing to know anything about the underlying network configuration or even what remote network the resource resides on. The four main components are:

- **Controller** - the central coordination component for Twingate. The Controller is a multi-tenant component operated by Twingate that performs several responsibilities, including storing customer configuration information that is managed by a web-based admin console, registering and authenticating Connectors, issuing signed authorizations to Clients successfully making connection requests, delegating user authentication to an identity provider, and distributing signed access control lists to Clients and Connectors.

- **Client** - a software application that is installed on end user devices. The Client acts as a combined authentication and authorization proxy for user requests for resources secured by Twingate. Network routing and authorization decisions take place at the edge within the client. Read more about the Twingate Client.

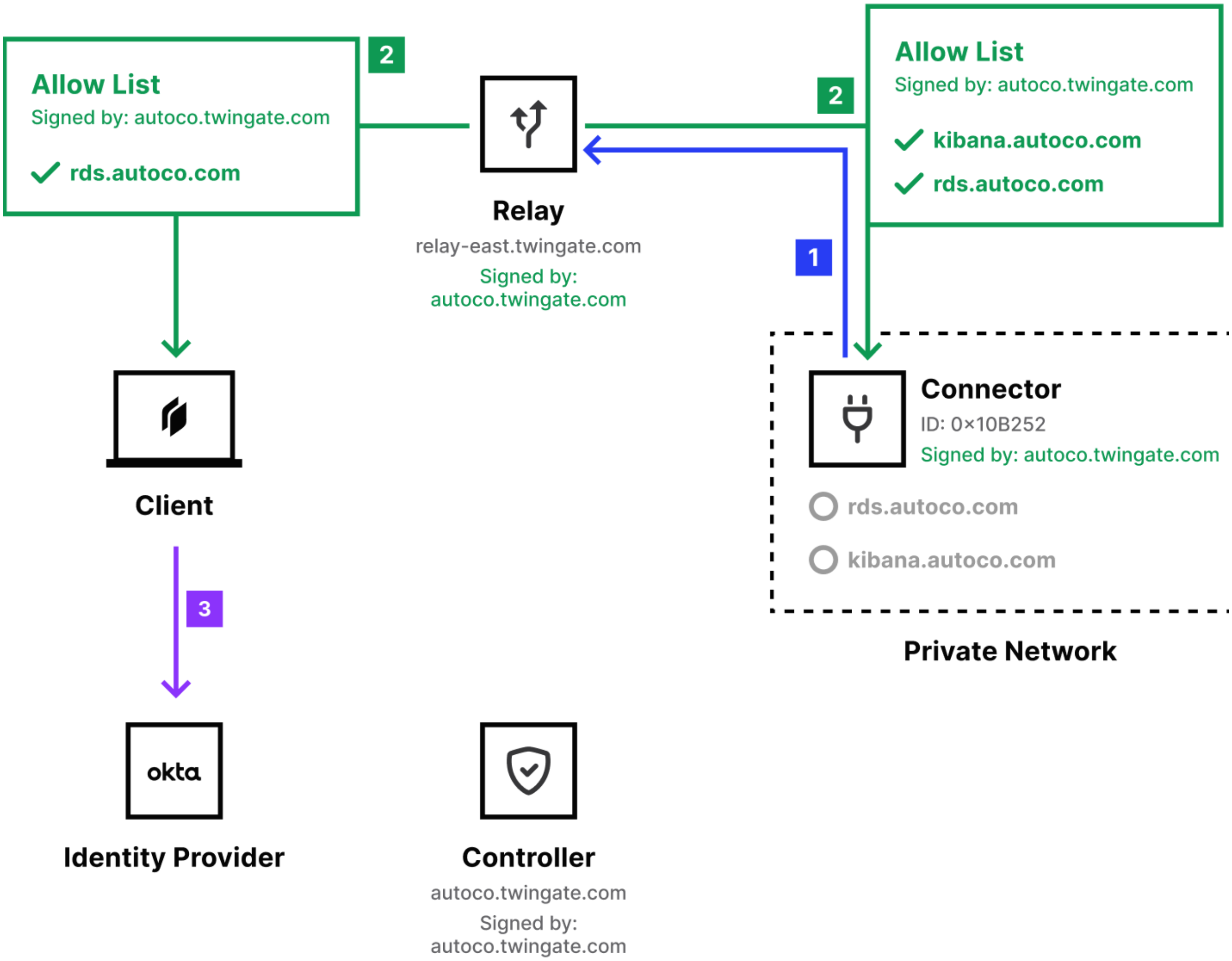
- **Connector** - a software component that is intended to be deployed on a device behind the firewall of a remote network. Connectors only initiate outbound connections to the Controller and Relays through which communications with Clients are established. Read more about Connectors.

- **Relay** - geographically distributed clusters that are operated by Twingate. Relays serve as a registration point for Connectors and a connection point for Clients looking to establish connections to Connectors. Read more about Relays.

- **Signaling servers** - geographically distributed listeners that help facilitate peer-to-peer connections between Clients and Connectors. Signaling infrastructure does not handle data and only exchanges public network addresses.

The Client and Connector components reside on customer-controlled devices and infrastructure, and the Controller, Relay, and Signaling server components reside within Twingate-controlled infrastructure.

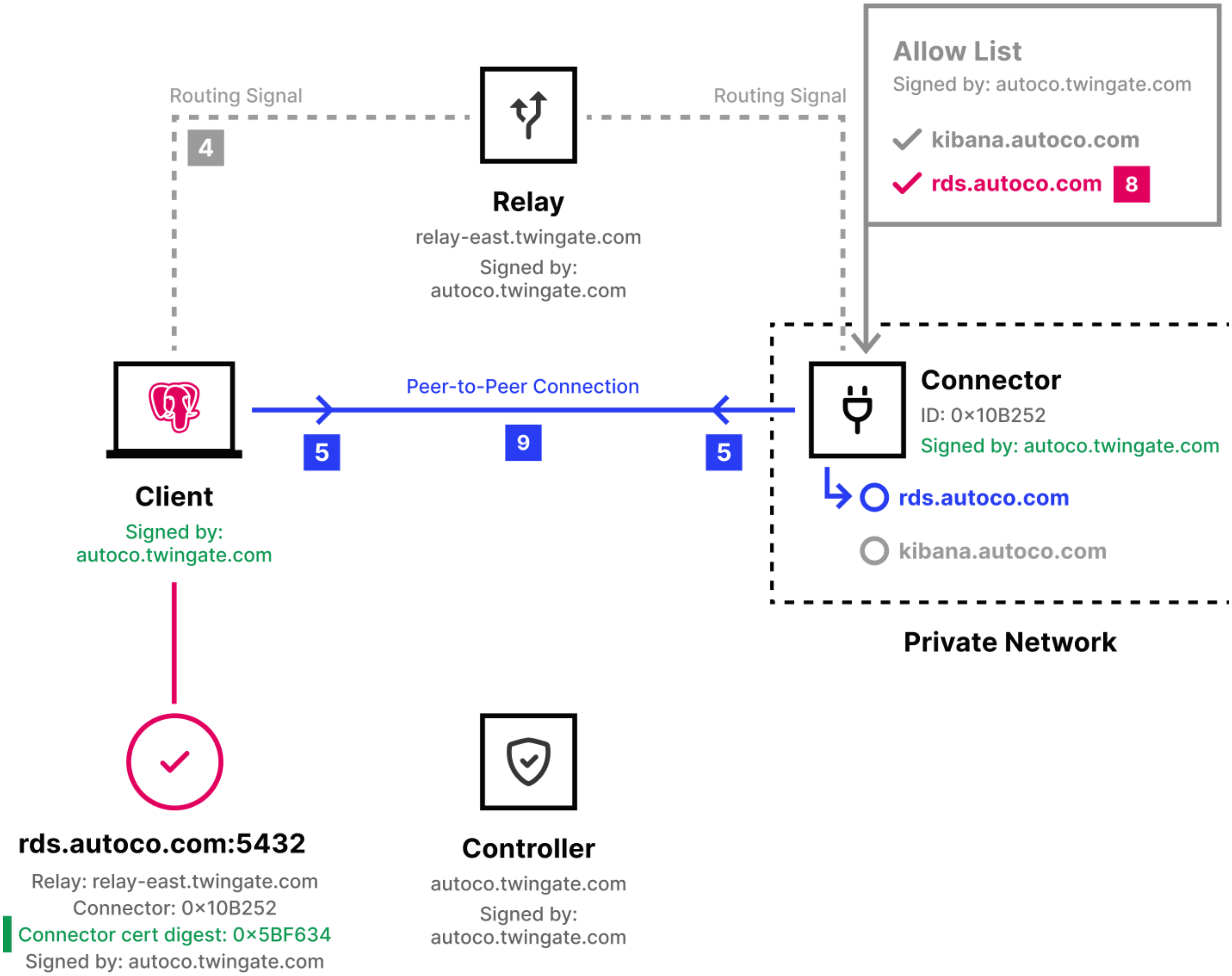
The following diagrams explain how various components exchange information in a secure manner to facilitate a connection from a client to a specific resource on a remote network:



1. **The Connector registers itself with the geographically nearest Relay.**
   The Relay receives no information about the Connector other than a randomly generated ID and its signature, signed by the Controller. The Relay allows the Connector to register only if its signature is signed by the same Controller.

2. **The Client and Connector each receive allow lists for traffic forwarding.**
   The allow lists are specific to each component. The Client's allow list corresponds to what the user is allowed to access, and the Connector's list is scoped to what Resources have been configured by an administrator. Both allow lists must be signed by the same Controller.

3. **The Client is authenticated by a third-party identity provider, providing additional defense in depth.**



4. **The Client initiates a request for a peer-to-peer (P2P) connection to the relevant Connector.**
   The Signaling server facilitates this process by exchanging a set of candidate public addresses for the Client and Connector to each other. The components then attempt to use these public addresses to establish a P2P connection.

5. **If the Client and Connector are able to initiate a P2P connection, a TLS-encrypted tunnel is established with no intermediate components in the data path.**
   This process may be unsuccessful depending on the network configuration on either the Client or Connector side. In this case, the Client falls back to a Relay-based connection to set up a TLS tunnel with the Connector. The Relay only facilitates this connection and cannot "see" any of this data flow.

6. **The Connector validates that the Client request is signed by the same Controller.**
7. **The Client validates that the Connector signature matches what was provided by the Controller.**
8. **The Connector validates that the destination address is in its allow list.**
9. **Once established, traffic flows through the encrypted TLS tunnel to the destination.** DNS lookups and routing are forwarded from the Client and performed by the Connector on the destination network.

1.2. Customer Data

What customer data do we process?

The main types of customer data that Twingate processes are:

- user details (such as email addresses, names, and group membership, but not passwords, since Twingate delegates authentication to third party identity providers);

- infrastructure information (such as network details, resource details, and access control lists); and

- logs (such as crash and error reports for diagnostic and troubleshooting purposes). Twingate components also log events that allow customers to monitor user activity (e.g. user logins and token requests).

User network traffic bound for resources secured by Twingate is normally routed directly between clients and those resources without transiting any Twingate infrastructure on a peer-to-peer basis. In certain situations, network conditions may not support direct routing and, for technical reasons, Relays are required to facilitate the routing of traffic between Clients and Connectors. When this occurs, traffic transits through Twingate Relays in encrypted form. This data-carrying traffic passes through Relays on a transient basis. Relays do not store traffic or any network-identifiable information. Learn more about Relay Data Privacy.

Twingate may also process customer data submitted by the customer in connection with customer support requests. This may include configuration data, error logs, and other information required to report and diagnose technical issues that the customer decides to provide to Twingate.

Data Segregation

Customer data is logically segregated on Twingate's systems by customer tenant ID.

Data Ownership

Ownership of customer data is retained by the customer.

Data Confidentiality

Under our contracts with customers, Twingate treats customer data as the customer's confidential information.

1.3. Product Performance & Scalability

Service reliability is a core aspect of information security. This section covers service reliability in relation to performance and scalability. For information on service reliability with respect to availability, please see *Infrastructure & Physical Security* below.

We have architected our infrastructure and software to ensure that Twingate is performant and continues to be so even as usage by individual customers or our whole customer base grows. Main ways we achieve this include:

- **Removing the problem of backhauling/tromboning** - instead of routing all traffic through a central gateway that may be geographically distant to origin and destination endpoints, traffic routed via Twingate takes a more direct route, leading to decreased latency for users and bandwidth use for organizations. Twingate Clients automatically and intelligently connect to Twingate Controllers and Relays that offer the best performance depending on where the user is physically located at the time and what resource they need to connect to.

- **Supporting split tunnelling** - any user traffic that an organization chooses not to route through Twingate will bypass Twingate altogether and be handled by a user's device independently. This reduces sending traffic unnecessarily through additional hops.

- **Load balancing** - Twingate handles load balancing at numerous levels. Twingate's Controllers and Relays are located in a variety of locations and geographic regions. As part of infrastructure planning, we aim to distribute them strategically to reduce latency and provide for load balancing in regions where higher traffic loads are expected. For example, in higher traffic regions, we may add additional Relays and balance loads among them. Latency may be further reduced by hosting Controllers and Relays with the same IaaS providers that customers use (e.g. within AWS, Azure and GCP). On the customer side, customers can install multiple Connectors within the same remote network and Twingate will automatically handle load balancing between Connectors for access requests into that particular network. Learn more about Connector Load Balancing & Failover.

- **Handling scaling for customers** - traditional network access security models require organizations to deploy and maintain their own security infrastructure, such as VPN gateways. Scaling that up adds to overheads disproportionately, and ties up resources that can be deployed for other initiatives. Twingate makes scaling easy and unburdens IT departments from needing to worry about it.

- **Distributing authorization processing** - instead of being centralized in one location which acts as a bottleneck, authorization processing workloads are distributed - such as at the Twingate client level - which helps with overall performance.

Information Security Program

2.1. Overview

This part contains a summary of Twingate's information security program. Twingate maintains a suite of written information security plans, policies and procedures that are reviewed on at least an annual basis, and are supplemented by periodic risk reviews that feed into the continual development of our information security program.

2.2. Administrative & Organizational Security

Governance & Responsibility

Twingate's Chief Technology Officer has primary responsibility over Twingate's information security program. Twingate also maintains a cross-disciplinary security team that is responsible for implementing, reviewing, and maintaining its information security program and includes members of senior management.

However, as a security company, Twingate views security as a pervasive issue and therefore as a shared responsibility throughout our entire organization. For example, all of our engineers are required to consider security as a fundamental part of their work, and they do not simply delegate all responsibility to other colleagues who focus more on security.

People Security

Employee Background Checks

All incoming employees in the U.S. are subject to background checks conducted by a third party provider that specializes in background checks. Background checks include: SSN trace, criminal searches (including county searches, multi-state, and national sex offenders public registry) and OFAC/SDN checks.

Outside of the U.S., we conduct background checks on incoming employees in accordance with local practices and subject to local law.

Employee Confidentiality Obligations

All employees and independent contractors are required to sign contracts under which they agree to protect customer and other proprietary information as confidential information. Our employee handbook and security training stresses the importance of maintaining the confidentiality of customer data.

Offboarding Employees

We have documented processes that we follow to ensure that when an employee departs the company, their access is revoked in a timely manner and any company assets they possess are returned or destroyed (whichever is appropriate).[2]

Workforce Security Training

All employees are required to undergo information security training during onboarding. Additionally, employees receive periodic security refresher training and updates about security best practices. Employees are required to review and acknowledge that they have reviewed the company's information security policies and procedures, which include an acceptable use policy for IT resources.

Vendor Management

We work with vendors and service providers who help us to provide our services to customers, such as email service providers, payment processors, and infrastructure providers. Some of these vendors have the ability to access or store customer data, and we adopt a variety of measures to ensure that they only do this in an appropriate and secure manner.

First, we select vendors based on our experiences working with them, their reputation, and an evaluation of how well they meet our business requirements. Second, we perform due diligence on potential vendors, which includes a risk assessment of their security posture. Third, when we engage a new vendor, we ensure that we have a written contract with them that includes appropriate provisions with respect to confidentiality, security, privacy, and service levels, where relevant. In general, vendors are only permitted to use data provided to them (including our customers' data) for the purpose of providing their services to Twingate.

[2] It will not be a surprise that we use our own product to easily manage the removal of employee access to our private resources!

Incident Response Plans & Breach Notification

Twingate has an incident response process that covers several types of incidents, including security and availability incidents. This is a series of documented processes that involve multiple teams, such as security, engineering, customer support, legal, communications, and management staff.

The incident response process covers various aspects from initial response, investigation, notification, mitigation, and remediation.

Should a security incident occur where it affects customers, we will notify the affected customers in accordance with our legal obligations. Please note that it is not always possible to notify customers immediately in the event of a security incident because of the time it sometimes takes to properly conduct an investigation to ascertain what occurred.

Customers can report any actual or suspected incidents to us through our customer support channels.

Insurance

Twingate has a standard suite of insurance policies with coverage that we have assessed is appropriate to our business. Policies include commercial general liability, workers' compensation, E&O (including cyber liability), and D&O insurance.

SOC 2

Twingate undergoes annual SOC 2 Type 2 audits. A copy of our most recent SOC 2 report is available to customers and prospective customers upon request.

2.3. Application Security

Data Protection & Access Control

Access Control

We provision user access to systems based on user roles and the principle of least privilege.

Access to private network resources in our production and other environments is secured using Twingate, with authentication performed by our identity provider's single sign on system with multi-factor authentication enabled. Using Twingate also allows us to exercise granular control over user access rights at the resource level (rather than network level), in accordance with the principle of least privilege, and apply different security policies based on the authenticated identity of the user, device, and context in which access is being requested.

Internal corporate applications use SSO and MFA for authentication where possible, with minimum password complexity requirements enforced.

We also automate our production environment deployment processes which removes the need for manually making changes directly to the production environment. This enables Twingate to avoid granting access rights to human users. Developers do not have direct access to databases containing customer data. Developers generally do not have or require access into production environment servers (including via SSH).

Access Monitoring

We use Twingate and other logging systems to monitor access to various systems and aspects of Twingate infrastructure.

Data Encryption

Customer data is encrypted both in transit and at rest using industry standard encryption protocols and algorithms.

In transit, client app communications are secured over TLS/SSL connections.

At rest, customer data is stored in a Google Cloud Platform managed database encrypted using AES-256 or better, with symmetric keys. The data keys are themselves encrypted using a master key stored in a secure keystore and changed regularly.

We do not use any custom or proprietary cryptographic frameworks or implementations. Note that Twingate does not store any customer passwords.

Data Backups

Automated, daily backups are made of our customer database. Backups are stored for a limited period for disaster recovery purposes and are regularly tested.

Data Deletion

Customer data is permanently and securely deleted upon request and in accordance with any contractual commitments made to customers.

Software Development Methodology & Testing

Software Development

All software code written undergoes a code review by a second person. Changes to production code require at least one person (other than the code creator) to approve and merge such changes via a pull request (PR) mechanism. More than one reviewer may be required depending on the nature of the code change. Additionally, Twingate performs internal and third party security testing, as described in the sections below.

Developers generally do not have access to production systems or data. Customer data is not used for testing.

We generally notify customers of major updates to downloadable software components. Minor updates, such as user interface tweaks, are regularly released without express notification. We recommend customers upgrade to the latest stable versions of Twingate software when they are made available.

Security is an integral part of the software development process and is considered at the design phase through to the testing of production code.

Internal Security Testing

Twingate uses a variety of tools to perform static analysis of code and report issues - both with our proprietary code, as well as vulnerabilities in third party libraries. Vulnerabilities detected are patched in a timely manner pursuant to our vulnerability management policy.

Third Party Security Testing

Twingate works with Hacker House, a reputable third party security specialist company to perform regular security testing on its applications. Hacker House's testing activities extend beyond penetration testing to application security assurance and product analysis, including:

- analyzing Twingate on a component-by-component basis in a "white box" environment;
- subjecting each component to reverse engineering, run time, and static analysis to ensure engineering is performed in accordance with best practice security guidelines;
- performing automated stress testing ("fuzzing"), manual vulnerability discovery, and both run-time and source code reviews; and
- conducting threat modeling.

Penetration Testing Requests

We permit customers to conduct penetration testing on our systems in certain circumstances. Customers must have prior approval from, and give advance notice to, our security team about the timing and scope of a penetration test and may be required to sign an agreement that covers such testing activities. Contact your account manager for more information.

Domain Claiming

Twingate customers may register accounts tied to a twingate.com subdomain specified by them. Under Twingate's Customer Agreement, discretion over subdomain allocation ultimately rests with Twingate and Twingate is empowered to take action to remedy incidents of trademark infringement, spoofing, or other undesirable activity relating to customers improperly claiming subdomain names.

2.4. Infrastructure & Physical Security

Device Security

All end user laptop and desktop computers are required to have anti-virus/anti-malware software installed and full disk encryption enabled. We use mobile device management (MDM) software to monitor our device fleet, enforce security settings, and push software updates. All IT assets issued by the company to employees are inventoried and tracked.

Infrastructure Change Management

Each proposed change to our production environment (including infrastructure changes) must be approved, and each such change and corresponding approval are logged. Our CI/CD pipeline provisions infrastructure changes in an automated manner after they are approved.

Secrets Management

We use a commercially available secrets management system provided by a major vendor to store secrets such as authentication tokens, passwords, API credentials and certificates. Keys are rotated on a regular schedule.

Server Hardening

We use Google Cloud Platform to provide pre-hardened server infrastructure. We interact with servers predominantly by deploying Docker containers orchestrated with Kubernetes.

Physical Security

Twingate has a globally distributed workforce and currently does not have any fixed offices.

Twingate employees are instructed and trained to ensure that their physical working environment is kept secure (whether it is a home, airport, cafe, or other remote location), and that any work equipment is secured appropriately, including when not in use.

Twingate uses Google Cloud Platform data centers which are physically secured by Google.

Availability & Resiliency

Service availability is crucial when our service is required to access mission critical network resources. We ensure a very high degree of service availability by:

- **Using a world-class infrastructure provider** - we use Google Cloud Platform (GCP) to host our core components. The technology that powers GCP is used by Google to support its own applications, which are used by billions of people. Read more about GCP.

- **Using multiple geographically separated data centers** - Twingate's infrastructure is hosted in multiple, physically separated Google Cloud Platform (GCP) data centers for redundancy. This assists with load balancing and mitigates the risk of environmental and other location-specific natural disasters.

- **Implementing a fault tolerant, redundant infrastructure** - our service is provided from multiple data centers which mirror each other's capabilities. If an availability issue arises with one data center, the other data centers will automatically pick up the load. Also read: Relay Reliability & Performance.

- **Providing transparency into service status** - customers can monitor service status and scheduled maintenance periods at status.twingate.com.

- **Providing resilience against DDOS attacks** - we implement certain measures to mitigate the risk of DDOS attacks.

- **24/7 monitoring** - we use a variety of automated tools to monitor our services 24/7 and alert us of any service availability issues.

Disaster Recovery & Business Continuity Planning

Twingate has a written DRP/BCP. Our goal is to ensure that customers always have access to our services whenever they are needed.

Additional Information About Twingate

Compliance & Certifications

For the most up-to-date information about Twingate's compliance with information security regulations, certifications, frameworks, and standards, please visit the Twingate Trust Center.

Contact Us

Twingate is a privately held business with operations in the United States and Israel.

Twingate Inc.

541 Jefferson Ave, Suite 100
Redwood City, CA 94063
USA

Twingate Israel Ltd.

c/o WeWork Azrieli Town
Derech Menachem Begin 146
6492103 Tel Aviv-Yafo
Israel

Online

www.twingate.com
sales@twingate.com
security@twingate.com
support@twingate.com