Introduction

Deskpro's mission has always been to help make communication more effective, efficient and easier using our helpdesk software. Alongside constantly improving and adding features to Deskpro, the security of your data has always been a priority for us. Whether you choose to deploy your helpdesk on the Cloud or On-Premise, we are committed to protecting and securing your data.

Organizational Security

Deskpro is committed to constantly maintaining knowledge of the evolving application security landscape and ensuring that security best practices are up-held across the whole organization.

Our security measures include company, product and hosting compliance with ISO27001, CSA Star, GDPR, HIPAA, PCI, EU-US Privacy Shield, G-Cloud & Cyber Essentials Plus.

We provide customers with a vast array of customizations within the product, to help you adhere to any auditing and certifications your organization's helpdesk may need to be compliant with.

This also includes customers being able to choose how to deploy Deskpro, either on Cloud or On-Premise (self-hosted), and where your data is stored.
For our cloud hosting, we use industry-leading AWS. You can view their security page here.

Protecting Your Data

What does 'Security' at Deskpro actually mean?

The aim of Deskpro's security practice is to prevent any unauthorized access to customer data.

We are always looking at ways in which we can improve the security of Deskpro. Working with you, certification bodies and across every team here at Deskpro, taking exhaustive steps find and mitigate risks.

Regular management security reviews are in place to address any areas that we believe can be improved upon and further secured. Implementation of this may be through new security certification, compliance or 3rd party testing to ensure best practices and improve security across the whole of Deskpro.

Physical Security

Facilities

Our cloud service data-centre provider (AWS) operate state-of-the-art, ISO 2700, PCI DSS Level 1, HIPAA, EU-US Privacy Shield & SOC 2 Type compliant data centres. Each facility is equipped with an uninterruptible power supply (UPS) and backup generators, incase of power disruption.

Automated fire detection and suppression systems are installed in networking, mechanical, and infrastructure areas. All AWS data centres are constructed to N+1 redundancy standards.

On-site Security

Our data centre facilities have 24/7 on-site staff, biometric security procedures, and round-the-clock surveillance monitoring maintain protection against unauthorized entry and physical security breaches. They also require background checks for all employees as part of pre-employment screening processes.

Server Monitoring

AWS' Global Security Operation Centres conducts 24/7 monitoring of data centre access activities, with electronic intrusion detection systems installed in the data layer. Systems constantly monitored by Deskpro Security Team.

Location

Deskpro offers deployment of cloud accounts onto data centres located in either the US, UK or EU. Customers can choose which region they wish to exclusively host their data in.

Responsible Disclosure

We do our absolute utmost to ensure that all aspects of the security of Deskpro are heavily tested and looked at multiple times by our QA team. Occasionally vulnerabilities can occur.

Deskpro has a bug bounty program that allows external security experts to safely test the product for anything that does unfortunately get missed. Allowing us to swiftly fix the vulnerability issue. You can view our responsible disclosure policy here.

Encryption

Data in Transit

Any data that is transmitted into and from the Deskpro platform is transferred and encrypted using industry best-practices. Transport Layer Security (TLS) 1.2 protocols with a 256-bit encryption cipher and SSL are used to protect your data in transit.

Data at Rest

All customer data stored on AWS servers, is safeguarded by 256-bit Advanced Encryption. Storage of attachments is provided off-site along with full daily backups.

Network Security

Dedicated Security Team

Deskpro has a Security Team that are distributed across the globe. They provide 24/7 monitoring and response to security incidents and alerts.

Firewalls

Deskpro's public facing network is protected by Cloudflare Enterprise which acts to filter all incoming traffic from the internet. Public facing email servers are protected by AWS Shield, which similarly monitors and filters incoming traffic from the internet. No other services or access is provided to the public internet.

Architecture

Within Deskpro's internal private network that is not accessible from the public internet, we employ AWS security groups and IAM controls to lock-down communication between components so access to services must be granted explicitly on an as-needed basis. We make it impossible for systems to interact with each other without our explicitly configuring it and planning for it.

Protection / Intrusion Detection

Intrusion Detection and Prevention systems monitor and/or block malicious traffic and network attacks across ingress and egress points of application data flow. They monitor and/or block malicious traffic and network attacks. Alerts are generated if predefined thresholds are exceeded, alongside 24/7 monitoring.

DDoS Mitigation

Deskpro system audit logs are always maintained and checked for anomalies, and we use contracted third-party DDoS providers to protect from distributed attacks. Including both AWS Shield Guards and CloudFlare.

Least Privilege Access

Access to hosting servers and live environments are provided on least privilege access. A very limited number of employees have access to live environments, that also require multiple levels of security access.

Security Incident Response (Team)

Deskpro monitors cloud service 24/7 and has a response team on call 24/7 to respond to security incidents. Our hosting providers, AWS, also provide 24/7 global monitoring and support for the multi-location datacentres that are used for Deskpro Cloud.

Platform/Product Security (in Deskpro)

Deskpro provides security features that you and your admins can configure to suit the level of security that you require.

Single Sign On (SSO)

Admins can configure multiple options for SSO to the Deskpro platform, including OneLogin, Okta, SAML and JWT authentication. There are different configuration options available for SSO enabling you to customize how it interacts with agents/users.

Two Factor Authentication (2FA)

Deskpro allows 2FA to be configured when using SSO for both admins and agents. A variety of apps are supported for 2FA including Authy, LastPass, Microsoft Authenticators and Google Authenticators. By enabling 2FA on your account, it provides an extra level of security to prevent someone else logging into your account as you.

API Security & Authentication

The Deskpro API is a REST-based API that runs over HTTPS and secured by SSL. API requests can only be made by verified users. Authentication can be done using OAuth, username and password authentication or using the API token.

Custom Password Policies

Customizable Password Policies can be enabled for both agents and users. This includes the ability to set minimum password length, forbidding password reuse, mixture of numbers and characters and forcing users to change their password after a certain amount of time.

Audit Logs

Full audit logs of every single action taken within your helpdesk software environment, can be viewed and accessed by Admins. They provide records including type, action, performer and timestamp that it was executed. Full activity logs for agents can also be viewed by Admins. This means that if there is an internal security breach or unauthorized changes made to the software, you will be able to see exactly who, what and when the changes were made.

Product Security by Deskpro

Billing Security

Deskpro doesn’t store credit card data. We use external PCI compliant services (Spreedly and Stripe) to provide billing services. Your credit card data momentarily passes through our servers, and for this reason we are verified as Payment Card Industry Data Security Standard (PCI DSS) compliant.

Quality Assurance (QA)

We have a dedicated Quality Assurance (QA) department that tests, reviews and triages our code base. For every update or release to the software, testing is performed by development, support and QA teams with a multi-level approach.

Separate/Different Environments

There are separate environments for both staging and testing. These environments are separated both logically and physically from the live-production environment. No customer data is used in testing or development.

Penetration Testing

Deskpro is tested with unit testing, human auditing, application penetration testing, static analysis and functional tests. Third party penetration testing is also completed on an annual basis.

Endpoint Security

Workstation Set-up

Before anyone joins Deskpro as an employee, their workstation is set-up and configured to comply with all of our security policies. These policies require that all workstations are configured to a high level and complying with security certification standards such as ISO27001 & Cyber Essentials Plus. You can view our standards here.

Each workstation has data encrypted at rest, strong passwords (managed by a secure password management vault), location tracking enabled and screens automatically turning off when idle.

Monitoring

A central management system is used to monitor, track and report on malware, unauthorized software and removable storage devices. This is to ensure that all workstations are up to date with patches and security. We also have a strict no-removable storage device policy.

Any mobile devices (phones or tablets) used for work purposes are part of a mobile device management system for location tracking, secure passwords and SSO.

Training

All members of staff are trained at least annually on security best practices, confidentiality of data protection and cyber security measures. New hires undergo training as part of their on-boarding process and constantly maintain knowledge of the evolving application security landscape.

Background Checks

For all new employees, Deskpro performs background checks. These are done in accordance with local laws and are also performed for contractors and cleaning crews. Background checks include verification for Criminal, Education and Employment.

Confidentiality

All new hires are screened during the hiring process. On commencement of employment at Deskpro, employees, contractors and cleaning crews are required to sign a Non-Disclosure and Confidentiality agreement. This is also up-held post-employment contract.

Sensitive Information Access

Provisioning

Only certain people within the organization are given access to sensitive information. It is on a need-to-know basis with role based permissions, to enable employees to perform their job to the best of their ability.

Our access control policy is implemented internally and within Deskpro we have multiple levels of security clearance. Some access, such as extended support or screen-sharing scenarios is performed on a client-agreement basis.

Authentication

To increase the security even further, Deskpro uses Two Factor Authentication (2FA) for systems that contain sensitive or personal data.

The use of Single Sign On (SSO) for employee's enables management to disable or change access to all applications instantly. This is used when an employee leaves Deskpro or their access needs to be removed.

Password Management

As part of our internal password policy, Deskpro requires all employees to use an approved password manager. This is to ensure passwords are strong, kept in a secure location, regularly changed and not re-used. Where necessary, the password manager alerts users to any potential password risks to maintain high-level security at all levels.

System Monitoring, Logging and Alerting

Deskpro constantly monitors the servers, workstations and mobile devices utilized for work purposes across the company using best in class technology. This is to maintain a comprehensive overview of the security and infrastructure across all departments and employees.

Access logs and any high-level administrative logins or system changes on all of the live production servers for Deskpro are kept for a minimum of two years.

Full production logs are available to security personnel with the appropriate security clearance for analysis and detection of potential issues.

Data Retention and Disposal

We retain daily backups of all databases. All attachments are stored in Amazon S3, which includes high-availability backup services - we maintain our own backup servers too, just in case.

Should you no longer wish to use Deskpro, we maintain backups of your accounts for 60 days - after which your data is completely deleted from all our systems.

Any hardware no longer in use is fully wiped, and disposed of using regulated disposal service in accordance with ISO27001 compliance.

Availability & Security Incidents

Uptime

Deskpro maintains a high level of availability on the cloud platform, averaging over 99.9%. There is a publically available status page, where you can check the status of the cloud software and its components here.

Redundancy

Our hosting services provide redundancy either with backups in separate availability zone within a single region. Or replication across regions. Data centres are designed to N+1 redundancy standards.

Responding to Security Incidents

We have established procedures and policies with regards to responding and communicating about security incidents from our Security Team.

The level of the security incident, will dictate how we communicate and respond to our customers. If a security incident does occur, you will be kept updated via our Customer Success team. They will be on hand to help and support you through the incident regarding updates.

All of our procedures and policies regarding responding to security incidents are evaluated and updated on at least an annual basis.

Disaster Recovery and Business Continuity Plan

In the case of an emergency or critical incident at any Deskpro premises, a business continuity plan has been put in place.

This was created so that we can continue to function as a business for our customers, no matter the scenario. The business continuity plan is tested and checked on an annual basis for applicability and any additional improvements that could be made.

Vendor Management

In order for Deskpro to run efficiently, we rely on sub-service organizations to help us deliver our service.

When selecting a suitable vendor for a required service, we take the appropriate steps to ensure that the security and integrity of our platform is maintained. Every sub-service organization is heavily scrutinised, tested and security checked prior to being implemented into Deskpro.

In any situation where the use of one of these sub-service organizations could potentially impact the security of Deskpro, we take appropriate steps to mitigate the risk. This includes establishing agreements and ensuring that they are compliant with relevant certifications or regulations, such as GDPR.

Deskpro monitors the effectiveness of these vendors and they are reviewed annually to confirm their continued security and safeguards are being upheld. You can view a list of our current sub-service organizations here.

External Validation

Security Compliance Audits

Deskpro is always actively searching, monitoring and improving our security set-up. This is through regular checks and assessments from both our internal security team and 3rd party assessors.

All results are shared with the management team and discussed in-depth at security management reviews. Recent security audits and certifications include ISO27001, PCI, Cyber Essentials Plus, HIPAA, G-Cloud 11 & GDPR. You can view our list of certificates here.

Penetration Testing

Independent penetration testing by a certified CREST CHECK 3rd party is carried out on at least an annual basis. The penetration tests performed are focussed on security, infrastructure and product. Results of these tests are shared and acted upon by both the Security and Higher Management teams.

Our annual testing also includes both external and internal network vulnerability scans, with certification for Cyber Essentials Plus. All 3rd party penetration tests are carried out by consultants certified to CREST standards.

Customer Driven Audits (and Penetration Tests)

We appreciate that in certain circumstances, an organization may require further audits or penetration testing to be conducted, before purchase of Deskpro can be made. We welcome customers to perform their own penetration testing on Deskpro environment. If you wish to arrange one, please contact support for scheduling this, and for further pricing.

Conclusion

Security is not just about secure software, it is something that we strive for excellence in across the company as a whole.
We understand that when you become a customer of Deskpro, it is critical to ensure trust between us and you.

If you have any questions, concerns or would like to know more please contact support at support@deskpro.com or visit our support portal at support.deskpro.com.