Threatplane Platform Service Definition

Version

Document Version: 1.0
Last Updated: January 2026

1. What the Service Is

Threatplane is a threat modelling and business-centric risk assessment platform. It enables organisations to conduct effective cyber risk assessments, prioritise security initiatives, and align security efforts with business needs.

The platform is used across multiple sectors including banking, luxury retail, transport, health and academia.

Key capabilities:

- Visual threat modeling with Draw.io and Lucidchart integration
- Automated threat assessment using industry methodologies and intelligence
- Risk assessment linking threats to business impact and controls
- Controls assessment evaluating security measures across technology architecture
- Prioritised remediation roadmap for systematic security improvements
- API integration enabling custom workflows, SSO, and automation
- Webhook support for GitHub, Slack, and development tools
- Architecture scoping for cloud, on-premises, SaaS, and AI boundaries
- Asset inventory capturing systems, APIs, supply chain, and business processes
- RROC framework translating controls into business risk metrics

2. Data Backup, Restore and Disaster Recovery

We host our services on public cloud providers with a resilient architecture that includes multi-region deployment as standard. All critical parts of our service are built on downstream cloud services that also utilise this pattern.

Our platform is hosted via leading cloud providers which utilise extensive physical safeguards to ensure resilience against hardware failure, network and power disruption.

Backup frequency:

- Starter plan: Daily backups
- Higher plans: Higher backup frequencies and flexible restore options

More information available on request.

3. Onboarding and Offboarding Support

Onboarding

For all customers we provide an online self-paced onboarding process designed to bring new users to the point they can confidently use the platform to create new assessments, see risk assessment outcomes and address risks/compliance gaps.

Our higher plans also include an optional threat assessment masterclass. This equips users with the theory and practical skills to fully make use of the advanced features those plans provide. Users learn to assess cyber threats and capture and analyse business risk. These masterclasses can scale to any team size and are delivered in an efficient, information-dense manner.

Support is available through all our plans for users of the platform. This includes asking questions of our in-house team of expert threat modellers to aid your assessments and keep quality high.

Our higher plans also include credits for our team to get involved directly in your assessments, either in a delivery or quality assurance/validation role.

Offboarding

All models are exportable in PDF and Excel format via the dashboard. We can also bulk-export data for you via a support ticket at any time.

We include bulk data export in PDF/Excel at no additional cost. If you require migration to a different platform we are able to provide this service at additional cost.

4. Service Constraints

New users are required to complete a small onboarding phase prior to use to ensure they can realise the benefits the platform offers. Support is available from us throughout to help embed this at any point.

System requirements: Chrome or Firefox

Customisation: Not available

Mobile access: Not designed for use on mobile devices

5. Service Levels

Availability

We guarantee 99.9% availability across our platform.

Our SLA cannot cover outages caused by factors beyond our reasonable control:

- Third-Party Vendors: issues attributable to external providers, including Supabase, AWS, Cloudflare, GCP, Azure, GitHub, or similar providers
- Integration Partners: failures related to third-party partners or other external service failures
- General Factors Outside Our Control: force majeure, internet service provider outages, or other issues outside our reasonable control
- Customer Actions or Inactions: resource limitations, misconfigurations, or failures to follow operational guidelines. Also includes issues caused by customer equipment/software, or account suspension/termination

Support Response Times

Business hours are defined as 9am-5pm UK time and exclude bank holidays.

Starter plan (business hours)

- Urgent: 24 hours
- High: 24 hours
- Normal: 48 hours
- Low: 72 hours

Plus plan (business hours)

- Urgent: 24 hours
- High: 24 hours
- Normal: 48 hours
- Low: 72 hours

Advanced plan (business hours)

- Urgent: 1 hour
- High: 2 hours
- Normal: 8 hours
- Low: 24 hours

6. After Sales Support

Support Channels

Email/Ticketing support: Yes, at extra cost. Response within 48 hours. Users cannot manage status and priority of support tickets.

Phone support: No

Web chat support: Yes, 9 to 5 (UK time), Monday to Friday. No AI chatbot. Web chat is accessible from the application once the user has logged in.

Onsite support: Yes, at extra cost

Support available to third parties: Yes

Support Tiers

PLATFORM ONLY is designed for organisations comfortable with threat modelling and risk management and are largely self-serve. Working hours support for platform issues and feature requests.

ENHANCED is for organisations looking to build threat modelling capability but require hands-on support from our team to achieve this. We provide extensive training, consultancy and support.

FULLY MANAGED is for organisations who are keen to adopt threat modelling and its benefits, but rely on our expertise for the actual building and maintenance of the models. We provide a complete threat modelling and risk assessment service to your organisation. Minimal skills or time are required from your teams.

7. Technical Requirements

Browser Support

- Microsoft Edge
- Firefox
- Chrome

API Access

- API available: Yes
- API capabilities: Read threat models, Update threat models, Reporting (control gaps, threats, risk assessment)
- API documentation: Yes (HTML format)
- API sandbox/test environment: No

Authentication Methods

- Multi-Factor Authentication (MFA)
- Identity federation with existing provider (for example Google apps)
- Limited access over government network (for example PSN)
- Dedicated link (for example VPN or bonded fibre)
- Username or password

Data Import Formats

- CSV
- Draw.io (XML, SVG & PNG)
- LucidChart
- Visio

Data Export Formats

- CSV
- PDF
- Excel
- Google Sheets

8. Outage and Maintenance Management

We host a public status page that tracks outages and other disruption. Users can request notifications via this for ongoing updates via email, Slack or Teams.

Incident Management

We follow SANS Institute incident response methodology, progressing through identification, containment, eradication, recovery and lessons learned phases. Users can report incidents via either email or reporting directly in the platform. We provide regular updates on selected incidents via our status page and via email.

Protective Monitoring

We use our threat modelling to inform logging and alerting at key data entry/exit points and critical services throughout our architecture, enabling early detection of anomalous activity and potential compromises.

Our team responds to security alerts within 4 to 8 hours on standard plans. Advanced plan customers receive a higher tier service with response times under 2 hours.

9. Hosting Options and Locations

Cloud Deployment Model

- Public cloud
- Private cloud

Data Storage Location

- United Kingdom
- User control over data storage and processing locations: Yes

Multi-cloud Support

Yes

Scaling

We regularly monitor resource usage and initiate optimisation and scaling where necessary. Our Advanced Plan includes an optional dedicated tenant which guarantees independent resources for your users. We also support on-prem/self-hosting deployment scenarios.

10. Access to Data (Upon Exit)

All models are exportable in PDF and Excel format via the dashboard. As our platform integrates draw.io directly, you are also able to export diagrams to various formats as supported by draw.io.

Our support team can also perform a bulk data export for you via a support ticket to these formats where required.

We include bulk data export in PDF/Excel at no additional cost. If you require migration to a different platform we are able to provide this service at additional cost.

11. Security

Data-in-Transit Protection

Between buyer and supplier networks:

- TLS (Version 1.2 or above)
- Where the customer deploys to their own cloud environment or on-prem, they will have an additional array of options to control and secure traffic flow which we can assist with

Within supplier network:

- TLS (Version 1.2 or above)

Data-at-Rest Protection

Physical access control, complying with SSAE-18 / ISAE 3402

Datacentre Security

Complies with a recognised standard, for example CSA CCM v4.0 or SSAE-18 / ISAE 3402

Penetration Testing

- Frequency: At least once a year
- Approach: 'IT Health Check' performed by a CREST-approved service provider

Access Control

We operate on a strict need to know basis across all business operations. Support staff can only access customer accounts when explicitly authorised by the customer, who maintains full visibility of when access is granted and at what level.

Customer data is automatically segregated within our platform through deny by default permissions and row level security. Users can only access data where explicitly granted, preventing accidental or unauthorised cross account exposure.

All customers and plans have granular control over access permissions within their account, allowing them to configure different levels of access for different areas of functionality.

Access restriction testing frequency: At least every 6 months

Vulnerability Management

We conduct threat modelling to proactively identify risks beyond known vulnerabilities, informing our security priorities. Our tiered infrastructure places services behind managed load balancers, providing protection against network level and data parsing attacks.

We monitor threats through GitHub Dependabot, which alerts us to vulnerabilities in our dependencies. Key framework dependencies are kept current, with roadmap items created to resolve any blockers preventing immediate upgrades.

Our automated testing and deployment pipeline enables rapid response to security issues. When a vulnerability requires patching, we can test, validate and deploy fixes to production within hours of a fix becoming available.

Configuration and Change Management

All code and infrastructure changes originate from our formal product change process, ensuring traceability from requirement to deployment. Every modification is version controlled in Git with complete history, providing full auditability of who changed what and when.

Changes require peer review and must pass automated tests before merging to the main branch. Our CI/CD pipeline enforces these gates, blocking deployment until all checks succeed.

We maintain segregated development and production environments. Infrastructure is managed as code through Terraform, ensuring idempotent deployments with full audit trails and the flexibility to roll back to any previous state.

Governance

- Named board-level person responsible for service security: Yes
- Software Security Code of Practice compliance: 12 of 14 requirements met, targeting full compliance in product roadmap
- Government security clearance: Up to Developed Vetting (DV)

Information Security Policies

We operate the following policies:

- Acceptable Use Policy (including AI governance)
- Network Security Policy
- Access Control Policy
- Data Management Policy
- Remote Access Policy
- Vendor Management Policy

All policies are kept under regular review. This aligns with our wider approach to business strategy, workforce planning, technology evolution and risk management.

Audit Information

- User activity audit information: Available via support team
- User audit data retention: At least 12 months
- Supplier audit data retention: At least 12 months
- System logs retention: Between 6 months and 12 months

For more information, visit the Threatplane website.