

DILIGENCE

Product Security Overview

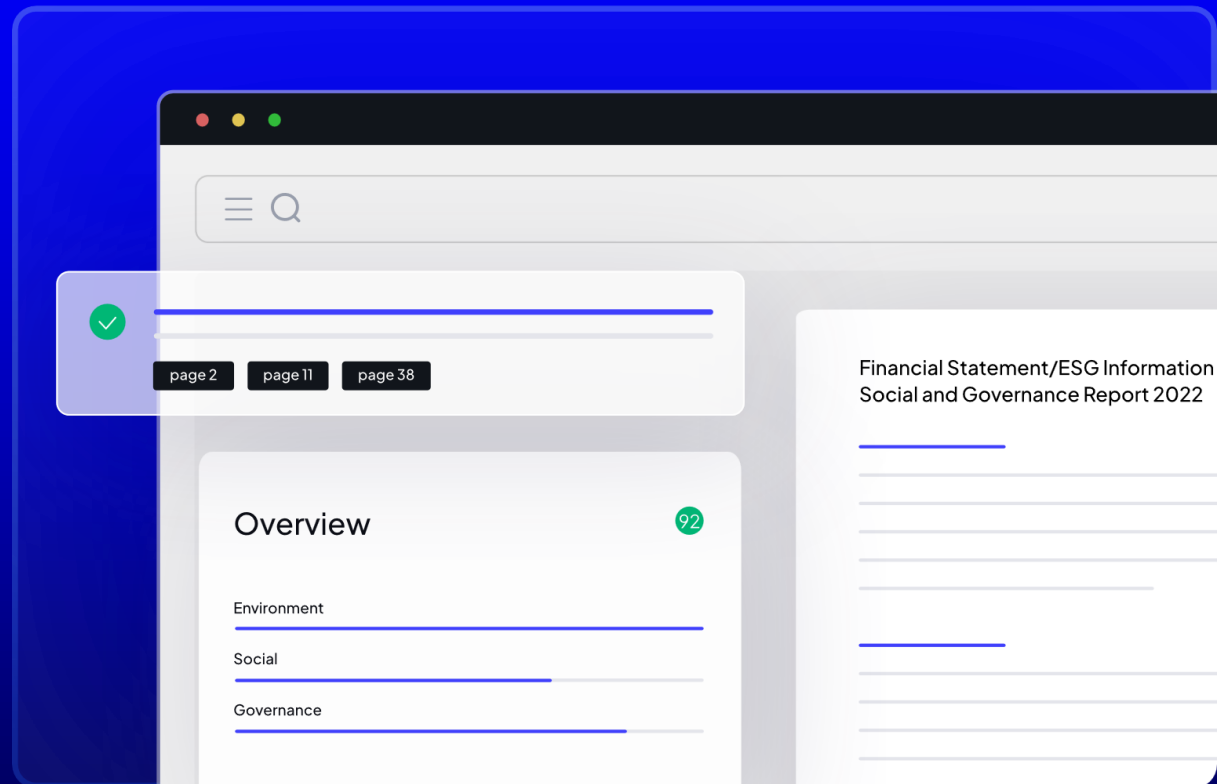


Wizpresso Diligence is a governance, risk, and compliance (GRC) platform that tracks regulatory frameworks across jurisdictions and converts circulars and standards into actionable checklists for reporting and operational compliance. It performs automatic gap analysis on documentation—including disclosures, policies, procedures, and evidence—to identify risks, ensure alignment, and generate audit-ready reports.

Diligence streamlines workflows for compliance, risk, legal, audit, ESG, and IR teams, reducing risks and costs while boosting transparency.

Visit <https://wizpresso.com/products/Diligence>

WIZPRESSO



Cybersecurity Overview

The **Wizpresso information security program** is designed to protect your data. Our program follows the defense-in-depth concept: securing your data at every layer.

Control Layer

Cybersecurity measures secure our application, infrastructure, data, and network.

Governance Layer

Dedicated information security functions, policies, and procedures to monitor system breaches, malfunctions, disruptions, or attacks. Our security program is regularly reviewed, and all staff undergo rigorous screening and training.

Audit Layer

All systems and processes are periodically reviewed and tested by 3rd party security partners. Wizpresso is ISO27001: 2022 certified.



Cybersecurity Architecture

By implementing a set of controls, including policies, processes, organizational structures, software functions, and settings, we ensure our systems meet enterprise-grade security best practices and standards. Controls have been established to minimize risk and protect information assets required to meet the operational, financial, and regulatory requirements to safeguard client data and privacy.

Our controls target to achieve the following:



Security

to prevent unauthorized access to sensitive information



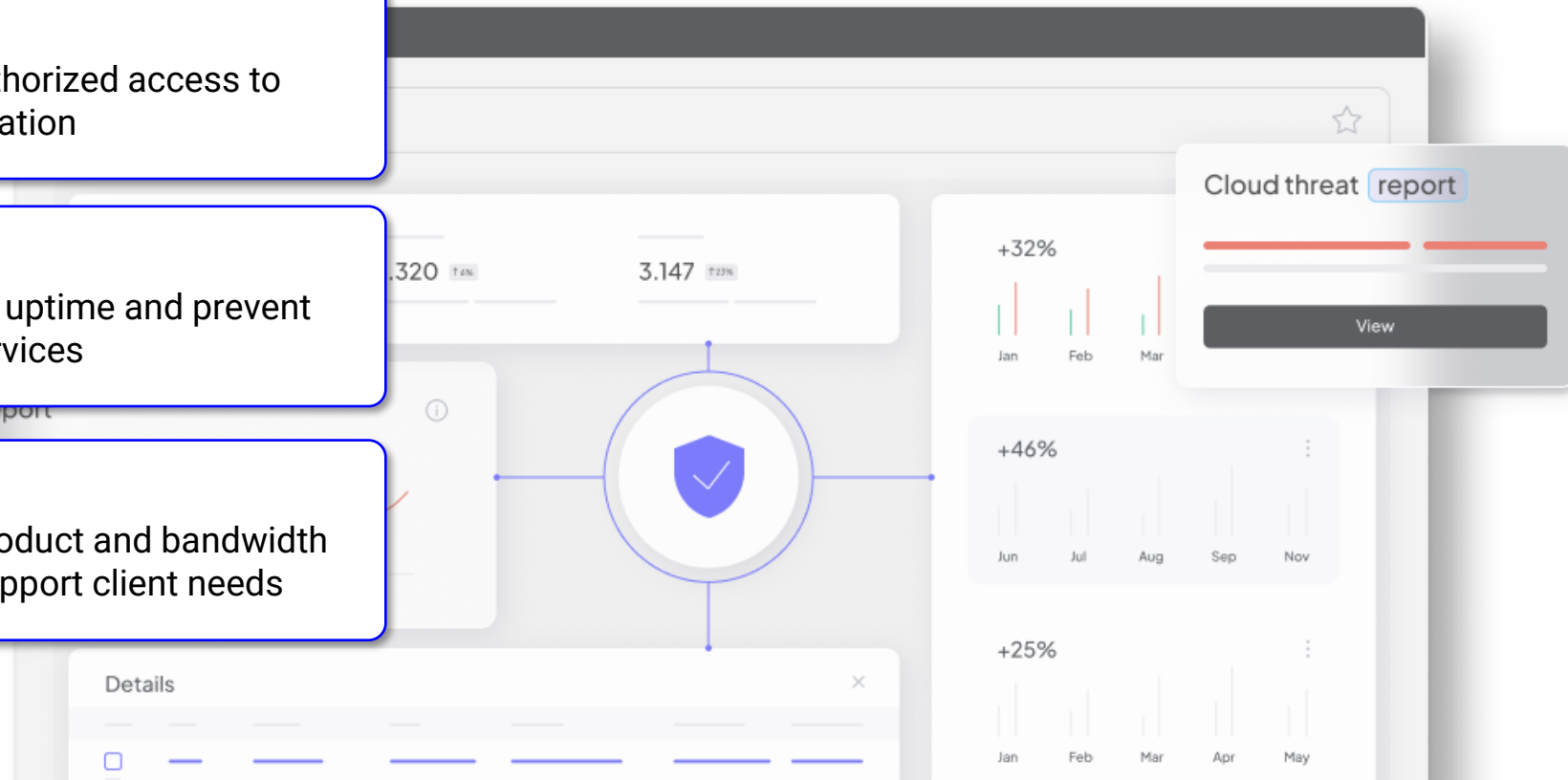
Availability

to ensure 99.9% uptime and prevent disruption of services



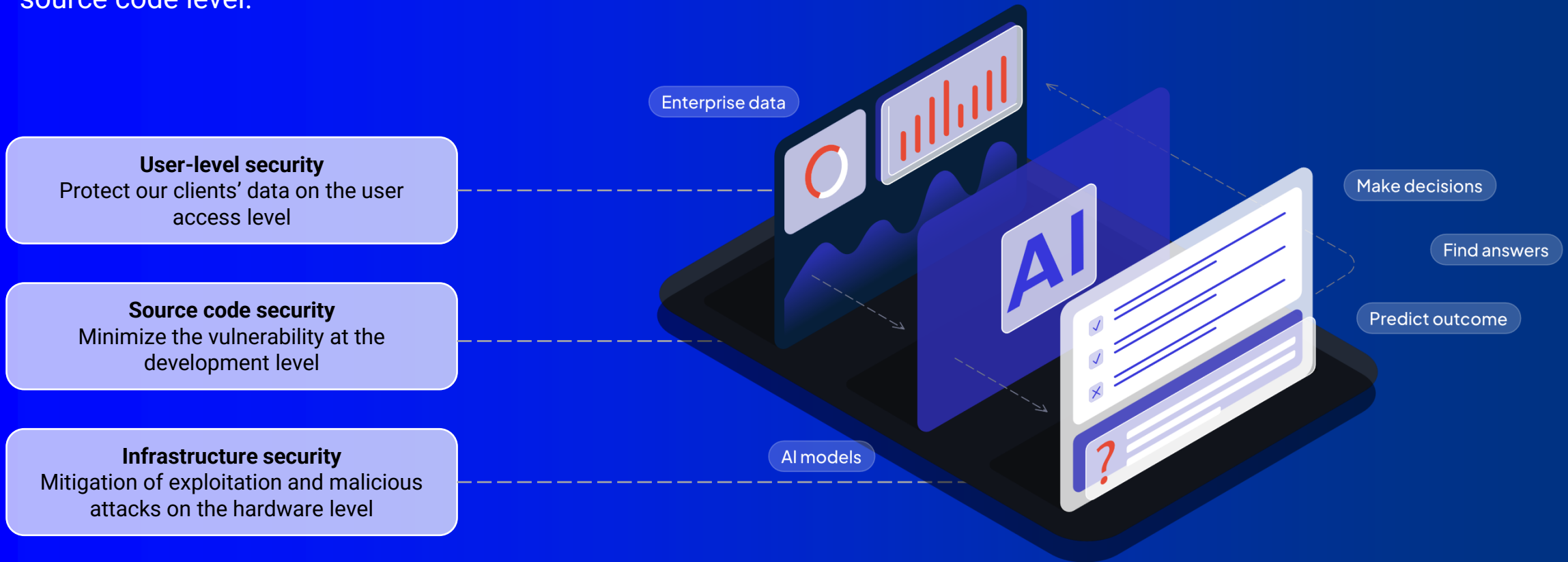
Efficiency

to ensure our product and bandwidth is scalable to support client needs



Governance Controls

Wizpresso’s robust governance ensures that our software is secured by design throughout the product lifecycle. By integrating security practices into the product development environment, we lay a firm security foundation at the source code level.



Cybersecurity measures

Wizpresso ensures the integrity of client data and access through industry standards and best-in-class security provisioning. The table below highlights our cybersecurity commitments for our cloud software services.

| Security | Status | Description |
|------------------------------|--------|--|
| Database encryption | ✓ | Data at rest is encrypted with the AES-256 standard |
| Data encryption in transit | ✓ | Data in transit is end-to-end encrypted with AES-256 standards. All connections use TLS/SSL encryption (version TLS 1.3) |
| Document encryption | ✓ | Document data is scanned and encrypted with the AES-256bit |
| Key management encryption | ✓ | Cryptographic keys encrypt data using FIPS 140-2 Level 3 certified cloud-based hardware security modules |
| Multi-factor authentication | ✓ | Identification management using phone-based or app-based OTP supported |
| Single sign-on | ✓ | Identification management integrated with Active Directory supported |
| Penetration testing | ✓ | Exhaustive annual test by 3 rd party with priority remediation of any security vulnerability issues |
| Application security testing | ✓ | Performed continuously on software with priority remediation of any security vulnerability issues |
| Vulnerability assessment | ✓ | Application and source codes are scanned before deployment and at least annually |
| Threat management | ✓ | Infrastructure is protected by threat detection services to monitor our servers against unauthorized behaviour |
| DDoS Protection | ✓ | Web application is protected by DDoS protection service 24/7 to safeguard against network and transport layer DDoS attacks |
| Firewall | ✓ | Firewall to protect our application or APIs against web exploits and bots that may impact availability, compromise security, or consume excessive resources. |
| Backup Protocol | ✓ | Comprehensive backup and recovery process to retain snapshots of data every 24 hours |
| RTO/RPO | ✓ | Multi-availability zones to ensure RTO/RPO is in minutes |

Security Statement

Diligence offers an easy-to-use interface that makes compliance workflows smoother, faster, more efficient, and more secure.

Wizpresso understands the importance of maintaining a comprehensive and robust Information Security Program that spans software, hardware, network, and data security , solely focused on safeguarding our products and our clients' data. Wizpresso aims to be a trusted partner to our clients.

Contact Us

support@wizpresso.com

+852 9677 3662