TERAMIND

Insider Risk Management, Employee Monitoring & Productivity Optimization

Through **Endpoint Telemetry**

About

Since 2014, over 10,000 organizations around the world have trusted Teramind to provide insider threat management, data loss prevention, and business process optimization through behavioral user data. By harnessing behavior analytics, our award-winning platform has helped enterprises in finance, retail, manufacturing, energy, technology, healthcare, and government optimize their workforce and protect their businesses.

Platform Security

Teramind is committed to protecting its platform and the data it collects.

Certifications and Frameworks

Teramind follows the most rigorous security controls and frameworks, and is certified by Bureau Veritas for its achievement in meeting international security standards.

- **ISO 27001:2013 Certification**

  ISO 27001 is the international standard for best practices in information security. Organizations with ISO certification, like Teramind, have proven through audit a demonstrated, ongoing commitment to the highest standards in data security and privacy.

- **ISMS Framework**

  Information Security Management System (ISMS) best practices ensure the confidentiality, availability, and integrity of all of our IT assets. Nodes and repositories where data is hosted and stored are sensibly protected from threats and vulnerabilities.

- **NIST Frameworks**

  The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides strict guidance for private sector organizations in the US on how to best prevent, detect, and respond to cyberattacks. Teramind applies this framework to customer data processing and internal business processes.

Data Storage

Teramind uses the latest and most secure data storage practices to ensure customer data is stored safely and securely while still being accessible.

- 256-bit AES encryption for all Teramind data, including customer data, at-rest.
- Encryption in motion to protect data being transmitted from network to public nodes.
- SSL with 4-key system and Active Validation for all HTTPS interactions.
- 256-bit AES end-to-end encryption for all endpoint – server communications.
- TLS with a 4-key system and Active Validation for all Active Directory LDAP connections.
- Active Directory integration capability.
- Role-based access control (RBAC) options and features.
- Multi-factor authentication (MFA)/Two-factor authentication (2FA) options.
- Adherence to GDPR's Right to Erasure for EU citizens' personal data.
- Deletion upon customer request policies.
- Session recordings stored for a period of six months, after which it is deleted.
- Programmatic deletion of session recordings.

Secure Deployment

The data centers and storage used by Teramind for its On-Premise and Cloud deployments feature rigorous controls and compliance, offering uncompromising security.

Data Centers

Teramind Cloud deployments are hosted on multi-homed Tier-3 data centers. Tier-3 data centers are designed to handle large businesses and mission critical applications, and meet the strictest reliability requirements that provide the following:

- PCI accreditation.
- Multi-ISO certification.
- Maximum 1.6 hours of downtime per year.
- 99.982% uptime
- PS 951 certification.
- Multi-node architecture that ensures 99.82% SLA.
- N+1 Fault Tolerant, minimum 72-hour power outage protection.

Platform Security Measures

Teramind's security extends beyond its certifications and frameworks to include other company-wide measures that protect the platform, our customers, and their data.

- **Red Teaming & Penetration Testing**

  Regular ethical hacking and cyberattack simulations identify vulnerabilities and security gaps, test incident response, and asses potential risk.

- **Redundancy & Backup**

  Failover measures ensure server and deployment health while daily back-ups keep data secure.

- **RTO & RPO**

  Teramind sets the industry standard for fastest recovery time objective (RTO) and recovery point objective (RPO) for both its systems and customer support.

Company Security Measures

Our top-down security approach ensures not only the security of customer data but also the security of our own business processes.

- **HR Security**

  Background checks, contracts & NDAs, role-based access controls as well as industry-leading and proprietary product development controls bolster staff-level data security.

- **Network Security**

  Intrusion detection, port blocking, DDoS attack response, and FTP/SSH sessions provide additional security to our network.

- **User Activity Monitoring**

  As an endpoint monitoring provider, we utilize our own product to monitor data usage and activity.

TERAMIND

Request Your Custom Demo Now

Get Demo