Teramind Platform Security

Teramind Platform Ensures Uncompromised Security, Scalability, Reliability and Performance

TERAMIND

Teramind Platform: Ensures Uncompromised Security, Scalability, Reliability and Performance

When you use any of Teramind's products including Teramind Starter, Teramind UAM or Teramind DLP you can rest assured that your data is protected with the best-in-class security standards on a solid platform. This documents describes some ways we provide our customers with a secure, scalable and reliable service.

Teramind is ISO 27001 Certified

Teramind achieved ISO/IEC 27001:2013 certification, the international standard for best practices in information security management systems. The certification demonstrates Teramind's ongoing commitment to following the highest standards in data security and privacy for its products and throughout every level of its organization.

ISO/IEC 27000 family of standards are designed for organizations to manage the security of IT assets information entrusted to a service provider by third parties and customers. ISO/IEC 27001 is the best-known standard in the ISO family providing requirements for an Information Security Management System (ISMS).

To attain ISO 27001 certification, Teramind was assessed by an independent auditor against the framework and guidelines set forth by the International Organization for Standardization for information security management (ISM). Throughout its assessment, Teramind successfully demonstrated a systematic and documented approach to protecting and managing sensitive company and customer information including financial information, intellectual property, employee and customer data, and other information entrusted to it by third parties. The ISO 27001:2013 certification extends to every level of Teramind's people, processes and technology, including its IT infrastructure stack, access control, physical assets, human resources processes and application security.

Interesting facts about Teramind's ISO 27001 certification

- The certification was audited by Bureau Veritas, an internationally acclaimed certification agency established in 1828.
- The newest version of ISO 27001 has 114 controls in 14 clauses and 35 control categories that an organization has to adhere to. These include IS policies, asset management, access control, physical and environmental security, risk management, compliance etc.

Leveraging the ISO framework for our security implementation has provided Teramind with a common language to deploy controls and procedures throughout our organization, while demonstrating to our customers that we have the appropriate controls in place when it comes to the security and privacy of their data.

Check out Teramind's ISO 27001 certification announcement press release.

We Use Certified, Tier-3 Data Centers

Teramind Cloud deployments are hosted on multi-homed, Tier-3 data centers which are designed to meet even the strictest reliability requirements of regulated and mission critical industries including finance, manufacturing, utilities and government.

From a security and compliance perspective, the data centers are accredited for PCI, PS951, ISO and other industry standards. In addition to a physically protected facilities and bespoke rack+cage security, the facilities feature a wide range of access and movement controls and threat detection systems in place (e.g., video surveillance, sensor equipped fence, 24/7 onsite NOC etc.).

Tier-3 data center

- Tier-3 data centers are designed to handle large businesses and mission critical applications.
- Ensure 99.982% uptime.
- Max 1.6 hours of downtime per year.
- N+1 fault tolerant providing at least 72-hour power outage protection.

On-Premise and Private Cloud Deployment Options for Added Control

While Cloud is the easiest deployment option for many organizations, if you prefer more control over your security and compliance, Teramind also offers On-Premise and Private Cloud deployment options.

The On-Premise version of our software has feature parity with the Cloud solution, and it requires minimal IT effort to deploy and maintain. With the On-Premise edition, you get a Teramind server in the form of a self-contained, Linux-based virtual appliance that runs on VMWare, Hyper-V or XenServer.

Alternatively, you can use Teramind's Private Cloud deployment option on AWS, Azure or Google Cloud.

Teramind deployment options

Cloud	Teramind handles all backups, redundancy, automatic updates, and other server tasks.
On-Premise	You get a Teramind server in the form of a virtual machine, which you manage in your data center.
Private Cloud	Similar to the On-Premise edition but instead of your own data center, you use a vendor's such as AWS/Azure.

We Ensure Secure Storage and Access to Your Data

Encryption of data at rest

All customer data, account credentials, system logs, backups and archives including session recordings that are in persistent storage are encrypted with strong AES 256-bit key encryption, the gold standard in cryptography.

Encryption of data in transit

All communication between the Monitoring Agent/endpoints and Teramind server use our proprietary protocol. Teramind policy enforces that all interaction with its servers happen over TLS (for Active Directory LDAP connections) or SSL (for HTTPS) with a 4-key system (private, public, intermediate, root) and an Active Validation policy. Encryption in motion ensures that your data remains secure and protected from snooping or eavesdropping while transmitted across the network and public nodes. We also provide an end-to-end encryption option for extra security and privacy.

User-level data security

Teramind's identity-based authentication and segregated, role-based access control (RBAC) features let you define what data a user or a group can access, edit or view allowing you to protect your data from insider threats and sabotage. 2-Factor Authentication means your credentials don't get misused even when lost or stolen. Finally, Teramind integrates with Active Directory to import your users, OUs, computers, groups and security attributes in a read-only mode with domain authentication simplifying implementing a unified access control policy.

Data retention and deletion policy

Teramind, when deployed using the Cloud option, stores user session recordings for a period of 6 months, and all other metadata in perpetuity for as long as the subscription is active. After this period, or as requested by the customer, the data is programmatically deleted and purged from our system. Additionally, Teramind fully supports GDPR's Right to Erasure (Article 17) when it comes to privacy of personal data for EU citizens.

We Conduct Regular Penetration Testing

Teramind conducts regular penetration testing on the platform and our Cloud instance. This is part of our full security audit practice where we simulate cyber attacks on our systems to identify vulnerabilities and gaps for unauthorized parties to gain access to the system's features and data and our strength to provide defense against such intrusion enabling full risk assessment for our platform and the hosted products.

We Have ISMS Controls in Place

In order for security to be effective, technological implementation alone isn't enough. You need to have good management and the right policies in place too.

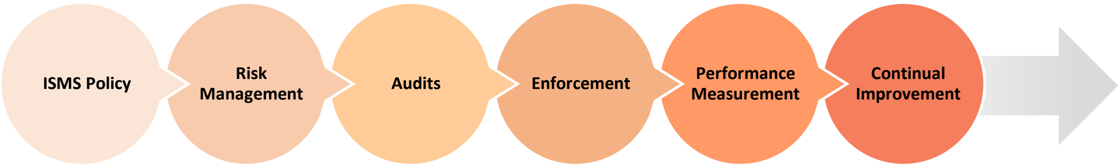
This is why Teramind utilizes Information Security Management System (ISMS) best practices that requires Teramind to put strict controls in place to ensure that it's sensibly protecting the confidentiality, availability and integrity of all our IT assets from threats and vulnerabilities. By extension, this includes protection for nodes and repositories where we host, store and archive our customer data.

A key theme of Teramind's ISMS program is that, its implementation includes not just our products and services but encompasses the establishment, implementation, operation, review, maintenance and improvement of information security at the organizational level. The program applies to all individuals who are authorized to use the information assets of Teramind, including our employees, business associates, support staff, administrators, contractors, and interns.

ISMS and NIST frameworks

- Both of these frameworks involve establishing information security control, but the scopes are a bit different.
- ISMS standards are designed for all types of organizations with a wider cybersecurity coverage.
- NIST is designed with the government security in mind and adopted by Japan, Israel and other governments.
- Together they provide the best combination of information security, risk management and compliance benefits for Teramind and its customers.

Teramind's ISMS Program



The main principles of Teramind's ISMS program is to ensure the confidentiality, availability and integrity of any type of information that we process, store or communicate.

The following table summarizes the ISMS policies and how we implement them to ensure the goals of the program are fulfilled.

ISMS Policies	**ISMS Implementation**
Ensure and manage information security in accordance with the Teramind strategic business objectives. Continually improve and support the operation of the Information Security Management System complying with ISO 27001 requirements and relevant local and international legal requirements. Fulfill the needs of and contractual obligations to customers and interested parties. Ensure the competence and awareness of all employees, third-party vendors, contractors and other stakeholders in information security. Perform business activities in accordance with the main information security principles – confidentiality, integrity and availability in order to protect information and data of customers, partners or involved parties. Conduct regular internal and external audits (by a certified body).	Assignment of 7-levels of IS responsibilities: CEO, CISO, HR Manager, Process & Quality Manager, Ops Admin, Director of Support Ops and IT Managers. Acceptable use. Access control. Business continuity. Change management. Configuration requirements. Incident management. Information classification. Information security incident management. Password management. Physical security. Problem management. Document. management. Policies are reviewed at least once a year by the CISO and the Information Security Committee (ISC).

Teramind Conforms to the NIST Cybersecurity Framework

In addition to ISMS, Teramind also conforms to the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The framework provides computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber attacks. Originally developed for operators of critical infrastructure in the U.S., the standard is being used by companies like Teramind and governments world-wide for its granular taxonomy and quality.

Identify

Teramind has asset management, business environment, governance and threat assessment strategy to identify cybersecurity risk to our systems, assets and customer data.

Protect

We have implemented strong access controls, database security, employee awareness and training, technical resilience systems and policies and procedures (see our ISMS program above) to ensure delivery of critical services.

Detect

We conduct continuous monitoring and threat assessment to identify occurrence of a cybersecurity event in the shortest possible time (see **Penetration Testing** section above).

Respond

We follow ISMS best practices to be able to ensure timely response to detected cybersecurity incidents. We are fully transparent when it comes to any data breach incident reporting and coordinate with internal and external stakeholders and customers to communicate such events. In addition, our mitigation system ensures we are able to prevent future similar incidents from occurring.

Recover

Teramind conducts recovery planning (RC.RP) after a breach with forensic data to mprove security perimeter (RC.IM) incorporating lessons learned. We communicate and share (RC.CO) threat intelligence with coordinating committee, CSIRTs, security analysts, CSOs, CISOs, auditors and others as established in our ISMS policy (see our **ISMS Program** above).

Teramind uses NIST framework to implement both its internal governance, business environment, asset management and risk management strategies and has designed the same level of safeguards in its platform to ensure delivery of critical infrastructure and data processing services to its customers.

Reliability, Performance and Scalability is Part of the Platform

Whether you choose to deploy Teramind solutions on our Cloud or Private Cloud, you will get the following benefits in addition to solid security and data protection:

Redundancy	Teramind's redundant platform is hosted in a secure, multi-homed data center utilizing multi-node clusters and failover mechanism. Our team constantly monitors server status and your deployment health and responds immediately if they notice any issues.
High availability	To protect your data and app servers from data center outages, Teramind deploys multi-node architecture which ensures 99.982% SLA.
Auto scaling	For both Cloud and Private Cloud deployments, Teramind offers vertical and horizontal scaling with optional auto scaling that adjusts capacity based on demand.
Automated backup	Teramind on Cloud comes with automated daily backup. Teramind Private Cloud and Teramind On-Premise can also be setup for automated backup if the customer chooses to do so.
Fast RTO / RPO	Teramind provides one of the industry's fastest Recovery Time Objective (RTO) and Recovery Point Objective (RPO), both for our systems and customer support.
Premium Support	Teramind Cloud deployments are eligible for telephone and email support. Teramind On-Premise and Private Cloud (AWS, Azure, etc.) deployments are eligible for 24x7 follow-the-sun support with an Enterprise SLA.

Other Security Measures

Network Security

- **Intrusion detection**

  Teramind uses intrusion detection, and threat analytics to monitor communications to/from endpoints, servers and gateway subnets. We also have an internal NOC to deal with cyber attacks, service outage, node failures, and routing black-holes.

- **Port blocking**

  Connection to Teramind servers are only allowed over approved ports and all other ports are blocked minimizing intrusion and hacking. Additionally, Teramind conducts regular penetration testing to ensure all external facing surfaces are tested for vulnerabilities.

- **DDoS attack response**

  Volumetric, application layer and protocol based Distributed Denial of Service (DDoS) attacks are detected and prevented using both software and hardware-based firewalls and other means (i.e. router filters).

- **FTP/SSH sessions**

  All file transfers, even the ones occurring internally are done over SFTP or FTPS. SSH sessions for dashboard administration purposes are only allowed on customer consent and can be disabled by the customer.

Physical Security

- **Secure asset management**

  Teramind keeps an inventory of all its assets including employee laptops, official mobile devices and network resources and has disaster recovery and backup policy in place for these devices.

- **Building access**

  All Teramind corporate buildings have access control systems (i.e. access card, visitor pass, CCTV etc.) and all entries are logged and audited by our security personnel.

- **Disposal of equipment and documents**

  Out of commissioned computers, hard disks, backup drives etc. are securely wiped and destroyed. Documents are shredded and disposed of by certified waste disposal units.

- **Workplace security**

  Server rooms, production and R&D zones and other sensitive areas are protected and access is restricted by various means (i.e. keypad locks, motion detectors etc.).

HR Security

- **Background check**

  Teramind uses multiple assessment methods (including blind tests) to hire all its employees. Additionally, critical employees and system admins that handle our core systems are background checked for security clearance (i.e. Federal Tier 3/ Tier 5 NAC) and only cleared employees are assigned for sensitive/government projects.

- **Access on a need to know basis**

  Teramind follows strict organizational structure and workflow process to decimate sensitive information on a need to know basis. For example: our conformance to PCI DSS compliance means, no Teramind staff are able to see any unprotected PAN/CC number or that the support staff can't access our internal CRM systems.

- **Employee communications**

  All our email, support chat and web communications are encrypted. We also use an end-to-end encrypted messenger for our day to day staff communications. Additionally, Teramind Monitoring Agent and DLP engine continuously monitor, screen and enforce security, harassment and QoS policy on all the corporate communication channels including email, social media and IM.

- **Explicit contract and audit**

  All Teramind staff and contractors have to sign non-disclosure agreements and contracts that explicitly states our data governance, security, confidentiality and integrity policy. They also need to go through periodic reviews, audits and training on how to handle various critical systems and sensitive data as appropriate to their role.

- **Employee activity monitoring**

  We wouldn't be a successful solution provider in our industry if we didn't stand by our products! Teramind uses its UAM and DLP products to monitor its own employees, third party vendors and contractors to prevent insider threats, data leaks, IP theft and sabotage.

- **Product development**

  Teramind uses industry leading tools for its product development, version control, code release, issue tracking, support, update/patch maintenance etc. In most cases, we also use our own proprietary software to ensure code integrity and control. We periodically use third party auditors and code reviews for all our product development activities.

About Teramind

Founded in 2014, Teramind is a leading, global provider of employee and user activity monitoring, user behavior analytics, insider threat detection, forensics and data loss prevention solutions.

Over 4,000 organizations in finance, retail, manufacturing, energy, technology, healthcare and government verticals across the globe trust Teramind's award-winning platform to detect, record, and prevent malicious user behavior in addition to helping teams drive productivity and efficiency.

Teramind is headquartered in Miami, Florida, with sales and support operations around the world.

Teramind is Ranked #1 by:

BEST EMPLOYEE
MONITORING SOFTWARE
2019 (OVERALL)

CAPTERRA
USER REVIEWS
4.5 STARS

BUSINESS.COM
TOP 10 REVIEWS 2017
GOLD AWARD

FINANCES ONLINE
MULTIPLE AWARDS &
TOP 10 RANKING

SERCHEN
EXCELLENT
RANKING

GETAPP
USER REVIEWS
4.65 STARS

BUSINESS.COM
TOP 10 REVIEWS 2017
EXCELLENCE AWARD

CROZDESK
WHAT OUR USERS
THINK - 5 STARS

Live Demo

www.teramind.co/sim

www.teramind.co

hello@teramind.co

+1-212-603-9617