TrueNAS
OPEN STORAGE

Secure Your Storage: The 2025 Guide to TrueNAS Security Features

TrueNAS
OPEN STORAGE

Why TrueNAS Security Matters More as We Head into 2025

TrueNAS has established itself as a leader in secure, enterprise-grade storage, providing the reliability and protection organizations need. As we look ahead to 2025, cybersecurity threats continue to grow in both scale and sophistication. Organizations need robust, adaptive solutions to safeguard their critical data against evolving risks like ransomware, data breaches, and insider threats.

This guide explores how TrueNAS' open standards, advanced features, and community-driven approach offer a strong, future-proof foundation to help organizations meet federal and enterprise security requirements while staying ahead of the latest threats.

TrueNAS
OPEN STORAGE

Open Standards — The Foundation of TrueNAS Security

How Open Standards Lead to Higher Security

Open standards are at the heart of what makes TrueNAS secure. By embracing transparency and collaboration, TrueNAS ensures that its security mechanisms benefit from continuous scrutiny and improvement by the community. This philosophy of "sunlight as the best disinfectant" allows potential vulnerabilities to be quickly identified and mitigated.

TrueNAS' source code is publicly available, enabling developers, security experts, and users to audit and contribute to its integrity. This collective insight leads to proactive threat identification and quicker resolutions, providing organizations with confidence in the security of their storage environment.

Building on these open foundations, TrueNAS includes a suite of built-in security tools such as encryption, access control, auditing, and logging. These features work together to deliver a secure storage solution and provide a strong foundation for data integrity and privacy.

Admin & Vendor Security

Admin Security
- Active Directory, Kerberos
- LDAP, Google Oauth
- KMIP Key Management
- SSH with FIPS 140-3
- Rootless Administration
- Separate Management Network

Vendor Security
- Security Notices
- Software Bill of Materials (BoM)
- Pen Testing
- Open Source Code
- Community Testing

TrueNAS
OPEN STORAGE

Advanced Security Features in TrueNAS Enterprise

TrueNAS Enterprise — Secure by Design

TrueNAS is crafted with security as a core design principle. Unlike many consumer-oriented storage solutions that may prioritize convenience at the cost of security, TrueNAS puts protection first. This commitment ensures that TrueNAS integrates seamlessly into secure network environments while minimizing potential attack vectors.

TrueNAS Enterprise stands as a reliable solution for the demanding security needs of enterprises, offering features that resist both internal and external threats. This secure-by-design approach helps organizations maintain the integrity of their critical data, regardless of the challenges they face.

The TrueSecure™ Feature Set

The TrueSecure package, exclusive to TrueNAS Enterprise, delivers a robust solution that meets the stringent security requirements of modern organizations. TrueSecure™ includes:

- **FIPS 140 Validated Cryptographic Modules:** Ensuring SSL-based encryption of data both in transit and at rest, complying with and certified against the rigorous security standards for sensitive information.
- **KMIP Support:** Simplifying security management by allowing centralized encryption key control across multiple systems.
- **Restricted Administration Roles:** Limiting access to sensitive functions, ensuring that only authorized individuals can perform critical actions.
- **Immutable ZFS Snapshots:** Providing advanced ransomware protection by preventing unauthorized deletions or modifications of data.

These features are designed to give enterprises confidence in their storage security, helping them meet compliance needs while mitigating the risk of cyber threats.

Role-Based Access with Restricted Admins

TrueNAS Enterprise introduces multi-level administrative roles to enhance security through separation of duties. System Admins, Storage Admins, and Monitor-Only Admins each have specific roles, ensuring that access is precisely controlled. This role-based approach minimizes the risk of unauthorized data manipulation and bolsters the overall security posture.

For organizations that handle sensitive information, separation of duties is vital. By restricting access based on role, TrueNAS makes it easier to enforce security policies and reduce the impact of insider threats.

TrueNAS
OPEN STORAGE

Rootless Administration and Snapshot Retention

To further strengthen security, TrueNAS has implemented rootless administration, moving away from the commonly known "root" username. Instead, administrators can create custom, unique accounts, which reduces the risk associated with default credentials.

Additionally, immutable snapshot retention tags ensure that restore points are safeguarded against premature deletion. This feature is especially crucial for ransomware protection, allowing administrators to make informed decisions about when it is safe to remove or modify snapshots.

Two-Factor Authentication (2FA)

Adding an extra layer of security, TrueNAS supports Two-Factor Authentication (2FA) for administrative access. By utilizing tools such as Google Authenticator or other TOTP-compliant applications, TrueNAS ensures that only verified individuals can access system controls. This feature is essential in protecting against unauthorized logins and enhancing the overall security posture.

TrueSecure

True Secure
- FIPS validation
- FIPS 140-3 Software Encryption
- FIPS, NIST 800-171
- STIG Support
- NIST CSF orientation

Data Share Security
- SMBv3 Encryption
- NFSv4 ACLs
- Snapshot Retention
- Immutable S3 Buckets
- SMB Auditing

TrueNAS
OPEN STORAGE

Best Practices for Maximum Storage Security

Network and Endpoint Security Best Practices

For optimal security, storage solutions need to be part of a broader, well-defended network environment. Organizations using TrueNAS should implement strong firewalls, network segmentation, and intrusion detection systems to prevent unauthorized access.

Integrating a directory service such as Active Directory or LDAP is also key to centralizing identity management, making it easier to enforce secure access policies. Regular audits and compliance checks further enhance security, ensuring that the entire system remains fortified against emerging threats.

Recommended Setup and Usage Tips for TrueNAS

Configuring TrueNAS for maximum security is crucial. Follow the Security Recommendations made available on the TrueNAS Documentation Hub to secure your active services, and disable any services that are not in use. Always enable encryption for sensitive data, and be selective in assigning administrative roles to limit access to critical functions. Keeping TrueNAS updated with the latest software patches is also a vital practice, ensuring your system benefits from recent security advancements.

Leveraging the TrueSecure™ package can significantly elevate the protection of critical data, making TrueNAS a resilient choice in the face of evolving cybersecurity challenges.

Management & Client options

Clients
- SMB
- NHS
- iSCSI
- S3

Management
- TrueCommand
- SNMP
- Syslog
- WebUI
- SSH

TrueNAS
OPEN STORAGE

Security Enhancements in TrueNAS Electric Eel

TrueSecure™ — Enhanced Capabilities in Electric Eel

The v24.10 ("Electric Eel") release introduces further enhancements to the TrueSecure™ package, specifically designed to meet the security challenges of 2025 and beyond. This includes FIPS 140 validated cryptographic modules, which provide even stronger encryption for data in transit and at rest, ensuring that your data remains safe under the most rigorous compliance standards.

Electric Eel also brings advanced auditing capabilities, delivering complete transparency regarding system changes and configurations. These improvements make TrueNAS an even more formidable partner in the fight against cyber threats.

iX-Storj: Globally Distributed Storage for Zero-Trust Protection

Electric Eel features iX-Storj, TrueNAS's new approach to globally distributed cloud storage. With zero-trust encryption for security and erasure coding for protecting data integrity, this highly-redundant and highly-available solution ensures that your data stays safe from prying eyes. iX-Storj's distributed model enhances data integrity, providing organizations with a reliable option for securing sensitive information in the cloud.

New to Electric Eel, the TrueCloud Backup functionality enables access to the same versioned backups and easy rollback that administrators have leveraged locally through TrueNAS for years. With the ability to retain multiple previous copies of uploaded files and perform granular restores, TrueCloud Backup gives you control and flexibility even for your offsite storage.

Additionally, TrueNAS integrates a cloud sync feature for seamless data synchronization between on-premises storage and cloud providers, ensuring data availability and protection. With comprehensive cloud backup capabilities, TrueNAS enhances data resilience for disaster recovery and business continuity.

The zero-trust encryption guarantees that your data remains safe—encrypted and inaccessible without proper credentials. This is particularly valuable for enterprises handling highly confidential data.

Enhanced Logging and Auditing Features

Electric Eel also enhances logging and auditing capabilities, offering detailed insights into configuration changes, command executions, and access attempts. These logs provide valuable visibility, enabling proactive monitoring and rapid response to potential security incidents.

With these features, TrueNAS makes it easier for administrators to track and manage system activities, ultimately ensuring a more secure storage environment.

Compliance with General Purpose Operating System STIG

TrueNAS is advancing its security capabilities to meet the rigorous requirements outlined in the General Purpose Operating System STIG. Developed by the U.S. Defense Information Systems Agency (DISA), this STIG provides essential guidelines to secure systems by minimizing vulnerabilities and adhering to best practices for system protection.

TrueNAS SCALE 24.10 Electric Eel has integrated GPOS STIG support and there is ongoing work to improve and maintain compliance. This demonstrates TrueNAS's commitment to helping organizations align with stringent government and military standards, ensuring their data is safeguarded against sophisticated cybersecurity threats.

Encryption & Data Security

Data-in-Transit Encryption
- ZFS replication
- FIPS 140-3 Validated SSH
- AES-256 grade
- Wireguard VPNs

Data-at-Rest Encryption
- Per ZFS dataset or pool
- AES-256 grade
- Self-encrypting Drives
- FIPS 140-2 HDDs & SSDs

TrueNAS
OPEN STORAGE

Defend Against Ransomware and Prepare for Growing Security Threats

TrueNAS is a comprehensive solution for secure, compliant, and resilient storage, designed to meet the evolving needs of modern enterprises. As security threats continue to grow and evolve in 2025 and beyond, it is essential to partner with a solution that prioritizes both innovation and proven security practices.

TrueNAS Enterprise is built to provide long-term peace of mind, with the scalability and security features necessary to face the challenges of tomorrow. In an era where data is both an asset and a target, TrueNAS is committed to being your trusted partner, safeguarding your data with cutting-edge technology and a community-driven approach.

Explore TrueNAS's full feature set or contact us to discuss how TrueNAS can help protect your organization's future.