Security Whitepaper

March 2022

1. Overview

Netreo is a full-stack IT performance monitoring platform which provides customers deep visibility and insight into the performance, availability, and utilization of their IT infrastructure. Netreo monitors servers, network devices, and applications deployed as on-premise, cloud, or hybrid resources. Netreo also supports on-premises, hybrid and SaaS deployment models.

Given the nature of our offerings, we are acutely aware of our responsibility with respect to security. Hence, through our 21-year history of serving customers in sensitive industries like government, aerospace, financial services, and healthcare, we have developed a holistic governance, risk, and compliance (GRC) program that has served as a foundation for meeting security and compliance objectives.

Netreo's GRC program continuously monitors the 3 key dimensions of cybersecurity—people, processes, and technology, with security architecture, engineering, and operations. Our approach includes continuous technology and process improvements, continuous compliance monitoring and audit, secure systems, a responsible workforce, a resilient organization, and risk-informed decision making.

This multi-action, multi-dimensional, and multi-layered mindset to security proactively secures our people, processes, and technology. It also minimizes the need for reactive incident response. While maintaining our need for discretion, this paper outlines key elements of our security framework:

- Product Security
- Operational Security
- Data Security
- Platform Security
- Organizational Security

Netreo's offering is SOC 2 certified, and undergoes continuous compliance monitoring, including certification under the Veracode Verified program at the Team level for ongoing continuous third-party security validation, including recurring security validation of all open-source and third-party libraries.

2. Product Security

2.1. Product Updates

Updates and patches are generally released every two weeks (or more often, if needed for urgent security issues). Patching is designed to be applied without disrupting the production use of the system. Patches include all required OS, database, and application updates in a single consolidated update.

These updates are digitally signed to prevent tampering, and all build systems use multi-factor authentication including certificate-based authentication to strictly limit access to only the designated development personnel.

Netreo Cloud systems are updated regularly and automatically as soon as updates are available.

For on-premise appliance-based systems, these updates may be scheduled to be applied automatically, or manually applied on demand if the system has Internet access. If the system is in an air-gapped environment with no external network access, the updates can be downloaded as a cryptographically-secure binary package that can be uploaded directly to the system. These updates are verified with digital signatures before they are decrypted, decompressed, or any code is executed on the appliance.

2.2. Remote Support Access

Netreo product updates and remote support can be delivered via a secure VPN system. Customers have full control over this VPN connection and can enable or disable it through the administrative web interface of the product. All VPN communications are sent outbound. Depending on version and configuration, this usually uses UDP port 1194, but may optionally use TCP port 443 or TCP port 5000.

VPN communications are initiated from the Netreo server to Netreo's VPN concentrator and are authenticated and encrypted with 256-bit AES encryption using 2048-bit HMAC authentication. This ensures the highest possible level of data security. VPN tunnels may be administratively activated or deactivated by the customer to further restrict access.

VPN tunnels terminate in an isolated, secured network with strictly regulated access. Each end of the tunnels uses separate packet-level filters, application-level firewalls and packet analysis, and stateful inspection to limit the type, origin, and destination of the traffic. Access is controlled through multiple separate passwords with required two-factor authentication and public/private key authentications. Netreo systems are configured to not forward traffic between interfaces to prevent any data leakage between networks.

2.3. Attack Prevention

Onboard Intrusion Detection and Prevention systems monitor Appliances for signs of attempted intrusion and actively respond to block traffic from potential intruders.

Network-level security such as TCP SYN-Cookies are used to prevent TCP SYN floods from being used to create Denial-of-Service (DoS) attacks. Reverse-path verification is used to ensure that inbound packets cannot spoof the IP addresses of the Netreo server to bypass IP-level security. Evasive HTTP techniques with automatic blacklists are used to further mitigate DoS attacks and prevent brute-force password scanning.

Listening services are configured wherever possible to obscure version numbers or software information, in order to make reconnaissance more difficult.

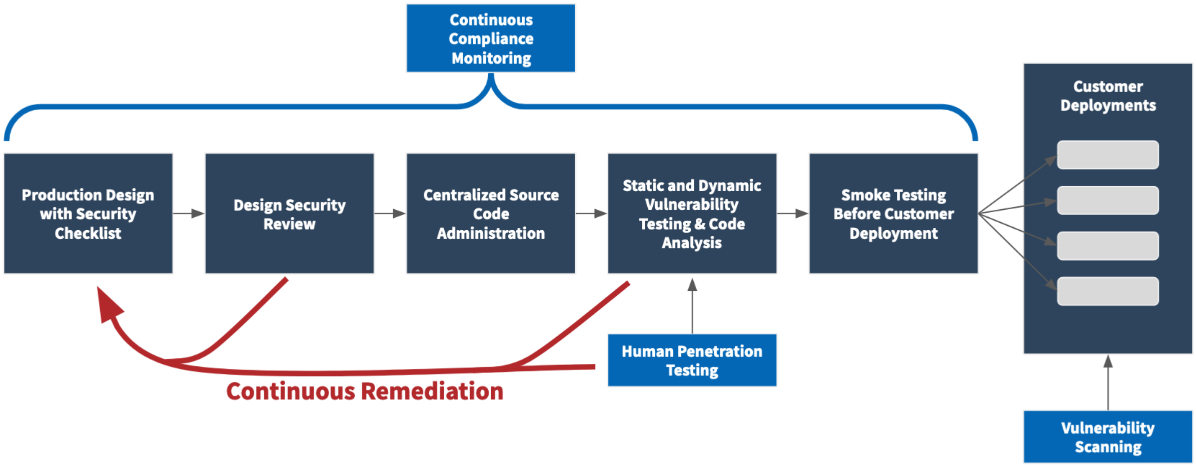
Customer access to the OS shell is never permitted. Netreo employees only have access to an Appliance's OS shell if granted by the customer, and is restricted to engineering employees, who are given access (via certificate-based authentication) only after they have completed security training and background checks.

2.4. Monitoring and Event Management

Netreo's offerings monitor themselves and their components for performance, reliability, and security. The system supports both auto-remediation and alerting. Netreo can also forward events to a customer's central log repository or Security Management (SEIM) platform if desired.

3. Operational Security

Netreo adopts software industry best practices to provide a security-first approach in delivering software to customers. Figure 1 below illustrates the company's secure development workflow:


Continuous Compliance Monitoring
Production Design with Security Checklist
Design Security Review
Centralized Source Code Administration
Static and Dynamic Vulnerability Testing & Code Analysis
Smoke Testing Before Customer Deployment
Customer Deployments
Human Penetration Testing
Continuous Remediation
Vulnerability Scanning

3.1. Product Design

Each feature design of Netreo's offering complies with a defined security checklist, including industry best practices such as Open Web Application Security Project (OWASP). The Open Web Application Security Project is an online community that produces articles, methodologies, documentation, tools, and technologies in the field of web application security.

Netreo has adhered to leading practices that have been accumulated in Netreo's 21 years of experience serving customers in every industry.

3.2. Security Architecture Review

For key features or major releases, there is a dedicated security architecture review conducted by architects and lead engineers who have extensive experience with product, software, and network security to ensure compliance with all relevant industry security best practices.

3.3. Centralized Source Code Administration

Netreo's product source code is managed in different repositories depending on the security exposure, with proper authentication applied. Access to these repositories is through a principle of least-privilege. Each code check-in undergoes a security review procedure to guarantee that no hidden security issues are present.

3.4. Security Smoke Testing

Each Netreo Product release is first deployed in Netreo's lab environment, where it undergoes rigorous testing that simulates real-world scenarios.

3.5. Vulnerability Scanning

Static and dynamic vulnerability scanning is an integral part of the Netreo Software Development Lifecycle (SDLC) process. These tests are run and reviewed for all builds. Passing stringent vulnerability scanning standards is required for all smoke and regression runs. Netreo developers are required to take monthly security training update courses. Most vulnerabilities are not exploitable in the wild, due to our security-in-depth architecture and limited access to the appliance.

Netreo has also achieved certification under the Veracode Verified program, and is listed in the Veracode Verified Directory, which assures ongoing, continuous vulnerability assessment and remediation and third-party validation. Veracode is the leading AppSec partner for creating secure software, reducing the risk of a security breach and increasing security and development teams' productivity.

Detected vulnerabilities are tracked and resolved promptly. Our policy is that vulnerabilities must be resolved within 30 days for high priority, 60 for medium priority, and 120 for low priority issues. In practice, vulnerabilities are generally corrected much faster. Critical vulnerabilities are identified during development or QA testing, and must be resolved before the software is released.

3.6. Third-Party Vendor Selection

Netreo follows a strict process in selecting 3rd party tools or libraries. Tools that are Vericode Verified, maintain SOC 2 certifications, or other security-related third-party certifications will be considered first, and be fully tested, including a security analysis, before being incorporated into production. Any open-source libraries will be scanned at the source code level and a copy of the library will be managed in Netreo private repositories for our production usage. No third-party compilation of open source code is allowed. Any changes or modifications to the open source code will be re-evaluated before being added into the Netreo repository for deployment on customer systems.

4. Data Security

4.1. Key-controlled Console Access

All console and serial access to the appliance is password (or public/private key) protected and user accounts are strictly limited to only those required for functionality.

4.2. Data Encryption

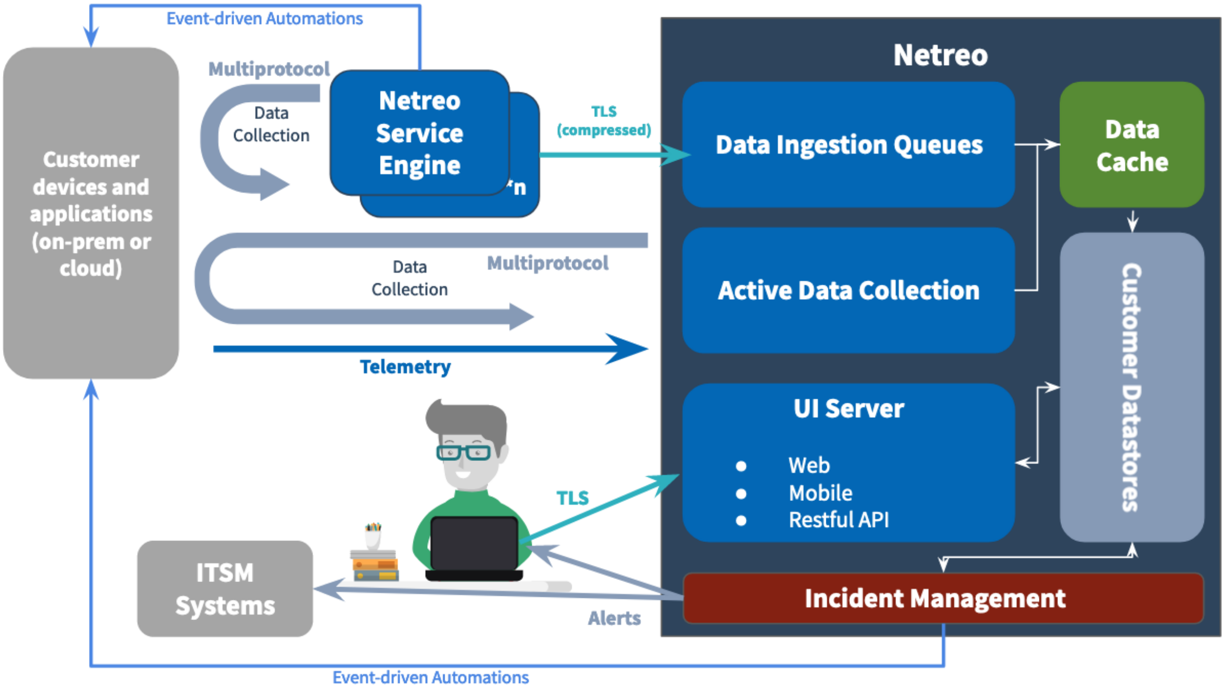
Netreo application users may be authenticated locally or using Security Assertion Markup Language version 2 (SAML2) or Lightweight Directory Access Protocol (LDAP). When locally authenticated, user passwords are encrypted using one-way hash functions with a minimum complexity of 256 bits and randomly generated salts. Local users can be forced to change their passwords at an administrator-defined interval. When using LDAP/Active Directory or SAML, user passwords are never stored or cached on the server.

Authentication credentials used to access customer systems are kept encrypted at rest, using a customer-unique key, so that data exfiltrated from a server cannot be decrypted or read even on another Netreo appliance. Backups of this data are encrypted with a minimum of AES256 encryption and digitally signed to prevent tampering.

In high-availability clusters and multi-server configurations, Netreo encrypts all data in transit between our systems using the latest TLS protocols. All inter-system database communications and clustering traffic are encrypted and source-authenticated.

5. Appliance Platform Security

Figure 2 illustrates the high-level architecture of the Netreo Appliance platform:



5.1. Operating System Security

Netreo's Appliance offerings run on a customized and hardened version of the Linux Operating System. To secure the operating system from network attacks, all unnecessary network services have been removed from the operating system. As a result, the only listening (open) TCP or UDP ports on the server are the services in use:

- HTTP (may be disabled by the customer, and is not recommended for use)
- HTTPS
- SSH (may be disabled by customer)
- Log collection (for Syslog and SNMP traps)
- Flow collection (for NetFlow, sFlow, and IPFIX)

Network access to any other ports from any interface is forbidden.

5.2. Web Interface Security

Netreo's appliance offering uses a 100% HTML5-based user interface, with no dependencies on Java libraries, Java Runtime Environments, or external client-side executable code ("thick clients"). This ensures that end-user browser and system security is maintained as no code is executed locally outside the browser. Browsers are required to use TLS 1.2 or higher and secure encryption protocols for access.

5.3. Remote Access Control

Remote Secure Shell (SSH) access is used on the Netreo appliance as a back-up method for low-level networking configuration. Access is strictly controlled and limited to specific administrative users, who are given limited access via a menu system and no direct access to shell commands. In addition, SSH authentication is done primarily using public-key cryptography instead of passwords. SSH access is not required during normal customer operations and can be completely disabled by the customer.

5.4. Independent Security Audit

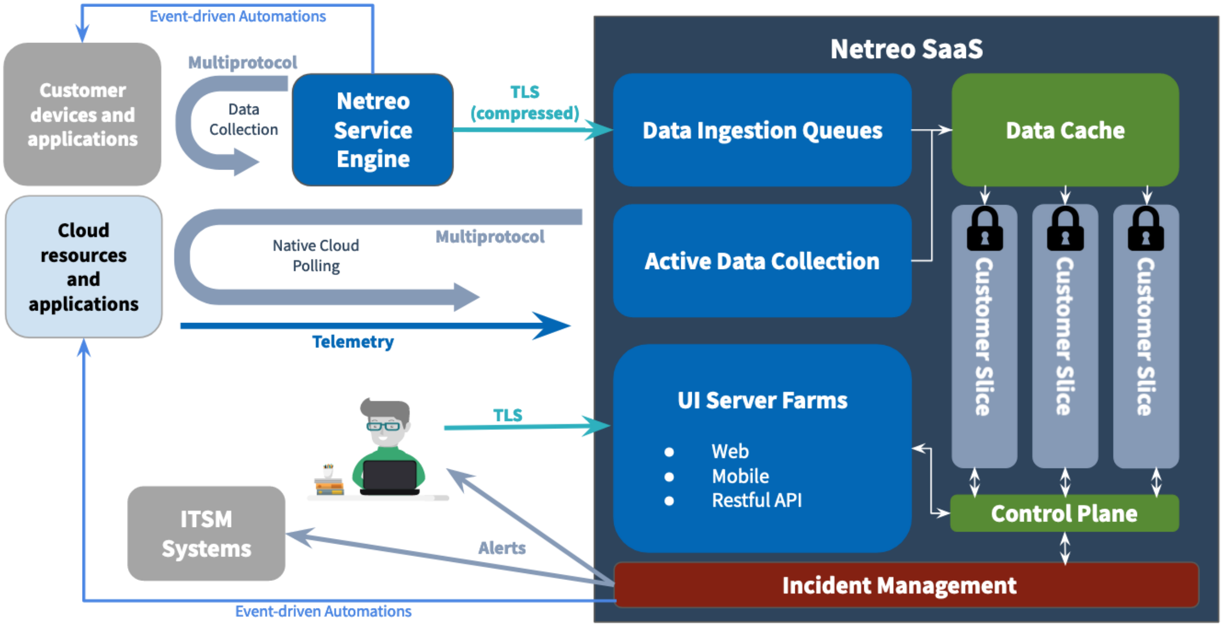
Netreo's appliance security is independently and continuously audited by Veracode and is certified under the Veracode Verified program. This audit includes both static and dynamic code testing, as well as regular human penetration testing using a known administrative password, and the system has been proven to be extremely resistant to intrusion.

5.5. Security Incident Response

Security incidents are handled based on severity. Netreo will respond to severity 1 issues within 4 hours on a 24x7x365 basis and provide continuous efforts to resolve the issue until it can be mitigated or resolved, or until the incident can be downgraded to a lower severity level. By policy, severity level 1 security issues must be resolved within 5 days. Note that policies and response times for non-security related support are detailed in the customer's support agreement.

6. Cloud/Hosted Platform (SaaS) Security

As with Netreo's other offerings, Netreo adopts a rigorous approach to the security of its SaaS offering - Netreo Cloud - particularly through continuous monitoring and improvement. Figure 3 below illustrates Netreo SaaS' product architecture:



6.1. Web Interface Security

Netreo's SaaS offering is 100% HTML5-based, with no dependencies on Java libraries, Java Runtime Environments, or Flash. This ensures that end-user browser and system security is maintained as no code is executed locally outside the browser. Browsers are required to use TLS 1.2 or higher and secure encryption protocols for access. Network DDOS and intrusion detection and prevention technologies are used to further heighten security.

6.2. Data Sovereignty and Availability

Netreo Cloud keeps all customer data within the United States, primarily in Amazon Web Services' west-coast data centers. Customer data is stored in Amazon S3 which provides 99.999999999% durability and 99.99% availability and is designed to sustain multiple data center failures without loss of data.

6.3. Service Levels and Incident Response

Netreo's standard SLA for SaaS services is 99.9% with a Recovery Point Objective (RPO) of < 24 hours, and a Recovery Time Objective (RTO) of < 2 hours. Our customer success team proactively contacts customers to address any incidents that cause service level misses.

Security incidents are handled based on severity. Netreo will respond to severity 1 issues within 4 hours on a 24x7x365 basis and provide continuous efforts to resolve the issue until it can be mitigated or resolved, or until the incident can be downgraded to a lower severity level. By policy, severity level 1 security issues must be resolved within 5 days.

6.4. Tenancy

All customer data is stored in separated customer-specific databases that are cryptographically isolated (using a minimum encryption level of AES256) with customer-unique keys. This ensures that even if data were to be somehow accessed from another Netreo customer portal, from an external system, or exfiltrated, the data can not be decrypted or accessed.

6.5. Network Defenses

Netreo uses Intrusion Detection Systems (IDS) and Intrusion Protection Systems (IPS) on all our networked systems. We also use anti-virus systems and have a central log for all events which is audited periodically.

6.6. Independent Security Auditing

Netreo's security is independently and continuously audited by Veracode, and is certified under the Veracode Verified program. This audit includes both static and dynamic code testing, as well as regular human penetration testing using a known administrative password, and the system has been proven to be extremely resistant to intrusion.

7. Organizational Security

7.1. Personnel

Netreo performs thorough background checks on all employees. These checks, subject to local labor laws and regulations, verify previous employment, criminal and financial history, and validate references provided by the candidate. Upon acceptance of employment at Netreo, all employees are required to execute a confidentiality agreement and must acknowledge receipt of and compliance with policies described in the Netreo Employee Handbook.

Netreo believes in creating a responsible workforce and resilient organization. Netreo employees undergo security training (with development personnel doing monthly training) to keep abreast of key developments, as well as governance, risk, and compliance requirements. Netreo also conducts internal security tests, such as phishing simulations to increase security awareness.

Employees also practice personal data/laptop security management. They are required to update their laptop passwords periodically, and to encrypt all storage devices at the operating system level. Netreo employees are also required to maintain the latest version of their laptop operating systems, as well as ensure the latest OS security patches and anti-virus updates have been applied.

7.2. Authentication and Authorization to Resources

Netreo provides each employee a unique User ID through our human resources process, which is used to identify their activity on the corporate network. All Netreo business systems are configured to be accessible by this User ID. Access to any systems that contain customer data requires authentication via a centrally-managed system.

This system enforces the use of two-factor authentication and strong password policies, including password expiration, restrictions on password reuse, and minimum password strength, which protect against unauthorized access. At the end of an individual’s employment with Netreo, a policy-based workflow ensures that account access is immediately disabled.

Netreo employees are granted a limited set of default permissions to access common corporate resources based on an employee’s job function and role based on a principle of least privilege. Where additional access is required, employees may follow a process that includes both automated steps and approval from a manager or other executive. All approvals are tracked and auditable where necessary.