Software Requirements Specification (SRS)

25-26J-076

ForLens – A Lightweight AI-Driven Endpoint Security Solution for Real-Time Threat Detection in SMEs

Sanjula E A Y – IT22340078

M R F Nusfa – IT22908742

M B D Salgado – IT21289934

De Silva H S – IT22887580

Supervisor: Mr. Kanishka Yapa

Bsc (Hons) in Information Technology Specializing in Cyber Security

Department of Information Technology

Sri Lanka Institute of Information Technology

Sri Lanka

02 January 2025

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this document is to specify the functional and non-functional requirements for ForLens, an integrated security platform. It provides a technical roadmap for the development of a lightweight Endpoint Detection and Response (EDR) system, a Security Information and Event Management (SIEM) core, and a Security Orchestration, Automation, and Response (SOAR) engine.

1.2 Scope

The For Lens platform is designed to protect SMEs while providing the same level of protection as enterprise grade solutions. The solution is intended to provide novel ways of protecting devices and full automation capabilities considering the resource constrains that SMEs face. To achieve the objective of the solution the solution comprises of 4 components which are integrated with each other. The scope includes the below 4 components:

- Lightweight Endpoint Agent & Honeypot module – A lightweight background service that gathers telemetry from Linux and windows systems. The agent is integrated with a honeypot module which provides additional security (through deception) and capabilities to monitor attacker behaviors.

- AI-Powered behavioral detection engine – This engine works as the decision-making component of the system. The engine receives telemetry from the agent and monitors for anomalies in the system. Threats are subsequently treated as per the engine training. The AI will be able to identify key users in the organization and create action profiles so that abnormal activities can be detected more accurately. Lightweight unsupervised models like Isolation Forest and LSTM are used to detect anomalies in real time. For better transparency the engine can provide the reasons why a certain decision was made.

- Cryptographically Secure Logging System – This is the core logging storage of the system. It utilizes SHA-256 hashing and Merkle tree chaining to validate the integrity and sequence of log entries. This storage is resilient to network outages and uses a hybrid approach to store logs in a shared model on both endpoint and central servers.

- Security Alert Interface with SOAR-Style Automation – This will be the integrated dashboard & user portal for the entire solution. This dashboard is user friendly and operable by a non-technical user. This dashboard contains essential functionalities similar to already existing SIEM portals. The SIEM is improved by utilizing SOAR style autonomous through AI. An LLM model in the system is capable of providing advice and explanations to non-technical users. It is also able to customize and create playbooks and advice the system to perform certain functions through an AI agent without needing to have any technical knowledge by user.

1.3 Definitions, Acronyms, and Abbreviations

Abbreviations	Definition
AI	Artificial Intelligence
LLM	Large Language Model
SOAR	Security Orchestration, Automation, and Response
SIEM	Security Information and Event Management
LSTM	Long Short-Term Memory
SME	Small and Medium-sized Enterprise
SOC	Security Operations Center
CPU	Central Processing Unit
IT	Information Technology

1.4 Overview

As per comprehensive research conducted by the team we were able to successfully conclude that over 40% of SMEs has faced cyber attacks and around 75% of them failed to properly respond to ransomware attacks [1]. Further research shows that SMEs are resource constrained in all aspects including financial, personal and knowledge to respond to cyber-attacks. This leads them to have degraded and decentralized security measures and are unable to implement enterprise grade security solutions. When cyber-attacks take place in SMEs that impacts them a lot both financially and operationally. Considering the resource constraints cyber security solutions should be financially feasible and operationally efficient for SMEs. Considering the hardships that SMEs are facing the ForLens solutions is created to address all of these challenges.

The goal of this project is to create a light weight fully autonomous endpoint security solution utilizing AI technologies, novelties and enhanced security while creating user trust in autonomous AI (AI SOC analyst), user friendly and light weight.

2 Overall Descriptions

The ForLens solution is a simple and easy-to-use security system powered by AI, made especially for small and medium-sized businesses (SMEs) that have limited money, staff, and technical skills. ForLens is different from regular big business solutions. It makes things simple, automatic, and saves money while also providing strong security features.

The system integrates multiple components to provide comprehensive protection:

- A **cross-platform endpoint agent** that continuously monitors system and user behavior with minimal resource consumption.
- An **embedded honeypot module** for early detection of unauthorized access and lateral movement attempts.
- An **AI-powered behavioral detection engine** that uses unsupervised machine learning models to identify anomalies in real time and provide explainable insights.
- A **tamper-proof cryptographic logging mechanism** based on SHA-256 and Merkle tree chaining to ensure forensic integrity.
- A **centralized dashboard** offering SOAR-style automation for incident response, enabling SMEs to act quickly without requiring specialized security staff.

The design focuses on working without an internet connection, making sure that devices can still spot threats and keep secure records even when the network is down. Automated workflows take care of common security problems, like isolating infected devices or shutting down harmful processes, which means less need for people to get involved. The design focuses on being easy to use. It shows alerts and suggestions in simple words on a clear dashboard.

ForLens helps small and medium-sized businesses get strong security like big companies have. It does this by offering easy-to-use and affordable tools that use AI to find problems, keep data safe with special codes, and automatically respond when there's an issue.

The light weight agent is installed on Windows and Linux servers. This agent gathers telemetry data from the endpoint. This telemetry involves but not limited to network traffic logs & event logs.

2.1 Product perspective

ForLens is a simple and fast security tool for small and medium-sized businesses (SMEs) that uses AI. It is different from big security tools like SIEM, EDR, and SOAR, which are made for larger companies. Unlike these other options that can be expensive, complicated, and need special skills, ForLens aims to be affordable, easy to use, and requires very few resources.

ForLens has better features than regular antivirus software. It can identify threats as they happen by using machine learning, keeps secure logs, and automatically responds to incidents in a quick and organized way. These features usually aren't found in basic antivirus programs, which mostly depend on identifying known threats and don't actively look for new dangers.

Unlike security solutions that rely on the cloud, ForLens focuses on processing data locally and can work offline. This means it stays strong even when the internet is not available and doesn't need a constant connection. This makes it easier for small and medium businesses with less equipment.

Also, ForLens uses honeypots and secure features that you usually find in expensive business software, but not often in products designed for small and medium-sized businesses. ForLens puts together new features in an easy-to-use and affordable way, helping to connect simple security protection with advanced enterprise security systems.

2.1.1 System interfaces

- **Process and Thread Management APIs** – For enumerating processes, monitoring execution, and terminating malicious processes.
- **File System APIs** – To read file attributes, monitor changes, and quarantine suspicious files.
- **Network Stack Interfaces (Socket APIs)** – For monitoring network connections and isolating endpoints when needed.
- **Scheduler/Timer Services** – For periodic scans, heartbeats, and retry mechanisms.
- **Cryptography and Randomness APIs** – For secure key generation and hashing operations.
- **Service/Daemon Control APIs** – To manage agent as a protected service with auto-restart policies.
- **Time and Clock Services** – For accurate timestamping of events and logs.

Windows-Specific Interfaces

- Windows Service Control Manager (SCM)
- Windows Management Instrumentation (WMI)
- Event Tracing for Windows (ETW) / Windows Event Log
- Registry APIs
- Windows Networking (WinSock/WFP)

Linux-Specific Interfaces

- procfs / sysfs for process and system metrics
- inotify / fanotify for file system event monitoring
- Netlink / iptables / nftables for network isolation
- systemd / init scripts for service management
- Auditd for security event collection

Optional Interfaces

- Kernel-level hooks (e.g., eBPF on Linux, ETW advanced providers on Windows)
- Device control notifications (USB monitoring)

2.1.2 User interfaces

- ForLens Portal
- Lightweight endpoint agent

2.1.3 Hardware interfaces

- Network adapters
- Peripheral control.
- End-user devices

2.1.4 Software interfaces

- APIs
- Databases
- Communication protocols
- AI Software

2.1.5 Communication interfaces

- Dashboard Access
- Log Forwarding
- External Feeds

2.1.6 Memory constraints

SIEM/SOAR Server

- **RAM**: Minimum 16 GB for log processing and correlation
- **Disk Storage**: 500 GB for log retention (scalable based on retention policy)
- **Database Cache**: 2 GB reserved for query optimization

Endpoint Agent

- **RAM Usage**: ≤ 200 MB during active scanning
- **Idle RAM Usage**: ≤ 50 MB
- **Disk Usage**: ≤ 500 MB for signatures and temporary files

AI/LLM Component

- **RAM**: 4–8 GB for inference
- **Disk**: Model files up to 5 GB

Log Retention

- **External Storage**: Configurable (e.g., 1 TB for 90-day retention)

2.1.7 Operations

System Administrator (Admin) – Normal Operation

- **Log in to the Central Dashboard** (MFA, RBAC).
- **Configure Global Policies** (scan schedules, device control, exclusions).
- **Manage Integrations** (directory services, notification channels).
- **Set Retention & Storage Policies** for logs (local endpoint log settings; central archival if enabled).
- **Define SOAR-style Playbooks** (automated responses, triage flows).
- **Use AI Agent to get insights, advice and perform actions.**

End User – Normal Operation

- Acknowledge **simple notifications** (e.g., "Restart required after update").
- Report suspicious activity via **one-click "Report Issue"** button.

Incident Response (Admin / AI Analyst) – Special Operation

- **Isolate Endpoint** from the network (containment).
- **Quarantine / Terminate Malicious Process** identified by AI or honeypot triggers.
- **Disable or Lock User Account** (role-aware actions).
- **Trigger Autonomous Playbooks** (enrichment, triage, remediation—SOAR style).

AI Model Maintenance – Special Operation

- Fully automated retraining and updates.
- IT generalist only clicks **"Update AI Model"** when prompted.

2.1.8 Site adaptation requirements

Operating System Compatibility

The endpoint agent must support Windows 10/11 and popular Linux distributions such as Ubuntu and CentOS. The central dashboard and management console should be deployable on Windows Server or Linux servers, with Ubuntu recommended for cost-effectiveness and ease of maintenance.

Hardware Requirements

Endpoints should have a minimum of 4 GB RAM and a dual-core CPU to ensure smooth operation of the lightweight agent without performance degradation. The central dashboard server requires at least 16 GB RAM, a quad-core CPU, and 500 GB of storage to handle logs, AI models, and SOAR-style automation workflows.

Network Requirements

A stable LAN or WAN connection is necessary for communication between endpoints and the central dashboard. The system should operate efficiently with a minimum bandwidth of 1 Mbps per endpoint for telemetry and alert transmission. Secure ports must be open for example HTTPS (443) and Syslog/TLS (6514) to ensure encrypted communication.

Deployment Constraints

The solution must provide a plug-and-play installer for endpoints, requiring minimal technical effort for deployment. The dashboard should be accessible through modern web browsers such as Chrome, Edge, or Firefox. The system should not depend on continuous internet connectivity; it must function offline with local logging and delayed synchronization when connectivity is restored.

Security Adaptation

Local cryptographic logging must remain active even if the central server becomes unreachable, ensuring tamper-proof evidence collection. Role-based access control should be simplified for SMEs, offering predefined roles such as Business Owner and IT Generalist to reduce complexity.

2.2 Product functions

The system continuously monitors endpoint activities such as process execution, file access, and user behavior patterns. By utilizing unsupervised machine learning models like Isolation Forest and LSTM, it detects anomalies in real time, providing explainable insights to help non-technical SME users understand potential threats.

Each endpoint agent includes a honeypot that simulates vulnerable services to attract attackers. This module helps detect lateral movement, privilege escalation attempts, and reconnaissance activities early, improving threat visibility without requiring complex configurations.

The solution implements SHA-256 hashing and Merkle tree chaining to secure logs locally on endpoints. This ensures that all recorded events are tamper-evident and verifiable, supporting forensic investigations and compliance even in environments without centralized servers.

The system provides a lightweight Security Orchestration, Automation, and Response (SOAR) capability tailored for SMEs. It automates key response actions such as isolating compromised endpoints, terminating malicious processes, and notifying stakeholders, reducing reliance on technical expertise and improving response speed.

A user-friendly dashboard aggregates alerts, health status, and recommended actions in plain language. It prioritizes threats based on severity and provides one-click remediation options, enabling business owners and IT generalists to maintain security without specialized knowledge.

2.3 User characteristics

The users will be employees of a SME organization. These employees would be using the ForLens agent. The ForLens portal will be accessed by the administrator or other appointed users. These users can be non-technical people and neither are cyber security or IT specialists or users with limited technical knowledge.

2.4 Constraints

- Must run efficiently on low-resource SME devices.
- Needs to be cost-effective for affordability.
- Should be simple to deploy and manage without expert skills.
- Must provide real-time detection and response (no heavy cloud reliance).
- Logs and data must remain secure and tamper-proof locally.
- Should function during network outages (minimal dependency on connectivity).
- Must support multiple platforms and scale easily without complex infrastructure.

2.5 Assumptions and dependencies

- SMEs have basic IT infrastructure and endpoints capable of running lightweight agents.
- Users will allow installation of the ForLens agent on all relevant devices.
- Behavioral data collected from endpoints is sufficient for anomaly detection.
- Network connectivity is available for periodic updates and alert synchronization, though core functions work offline.
- Cryptographic logging assumes secure local storage and proper key management.
- Machine learning models assume access to representative training data, including simulated attack scenarios.
- Automated response actions depend on appropriate system permissions and administrative privileges.

2.6 Apportioning of requirements

- **Step 1:** Develop the lightweight endpoint agent with embedded honeypot and delete-proof mechanisms.
- **Step 2:** Implement the AI-powered behavioral detection engine for anomaly detection and explainable insights.
- **Step 3:** Set up the cryptographically secured logging system using SHA-256 and Merkle tree chaining.
- **Step 4:** Build the security alert interface with SOAR-style automation for real-time alerts and incident response.

As far as this project is concerned most requirements will be developed at the same time and later integrated together.

3 Specific requirements[1] (for Software Dev. Oriented Projects - SRS)

3.1 External interface requirements

3.1.1 User interfaces

Mainly the user will be interacting with the ForLens portal (dashboard) through the browser and the endpoint agent interface after installation on an endpoint.

ForLens Portal:

The ForLens Portal comprises of multiple modules that are used for individual use cases. This portal is accessed by system administrators and custom accounts created by admins. The portal will be accessible through a web browser using the portal URL.

- Login page / screen – This page will be used to enter usernames, password and MFA. This interface is similar to common login pages used by web applications. All users will have to authenticate themselves through this page. Upon successful authentication only they will be able access other functions in the dashboard.
- Dashboard – This will contain a summary of alerts, events and system health. The user will be able to customize the diagrams and charts based on his / her preference.
- Alerts and Incident panels – This will contain processed telemetry data showing suspected malicious activities that are currently happening and which have happened before. The user can filter out the data as required (based on time ranges, affected hosts, etc.). The incidents and alerts can be interacted by user to drill down and get more information such as artifacts and incident timelines.
- Log Viewer – the user can use this module to browser through all types of logs that the solution stores.
- Settings – This enables the user to change system configurations, user access management and perform custom integration if required.
- Report Section – Across all the portal modules report download features are available where the user is able to download reports with the click of a button.
- AI agent – Chats with user to provide advice to non-technical persons & able to perform actions on behalf of users.

Lightweight endpoint agent:

The agent comprises of an interface which can be accessed upon installation on Windows and Linux systems.

- Status Screen – Shows the current protection status (protected / not protected) and last scan details.
- Scan Options – The user can run on demand scans on the endpoint
- Quarantine Section – shows the quarantine file list to user and comprises with actions that user can perform to either request to release file or delete file.
- Security Alerts – Custom security alerts will be generated on the endpoint which either notifies the user of any threats or provide actions the user should perform in case of a threat.

3.1.2 Hardware interfaces

For the lightweight agent to function properly the following hardware will be required:

- End-user devices: Desktops, laptops or VM running windows and Linux are required for the agent to gather data and provide protection.
- Peripheral control: To effectively deploy device controls features the software should be able to have full control over the ports (USB ports).
- Network adapters: required to communicate with the system backend (servers).

3.1.3 Software interfaces

- APIs: APIs will be used for communications and sharing data across multiple components on the backend of the system. The endpoint agent will interact with underlying OS for file scanning, process monitoring and log collection.
- Databases: The solution will be utilizing databases to store logs, alerts
- Communication protocols: secure communication will be established such as using HTTPS for dashboard access and secure log forwarding protocols.
- AI Software: AI related software such as LLMs and Training Frameworks

3.1.4 Communication interfaces

- Dashboard Access: Secure protocols such as HTTPS are used to securely access the web portal.
- Log Forwarding: To forward logs form the endpoint agent to ForLens backend protocols such as Syslog will be used.
- External Feeds: Threat Intelligence updates are accessed through HTTPS through data formats such as JSON.

3.2 Classes/Objects < For Software Dev. Oriented Projects>

Class: Endpoint

Priority: Essential

Responsibility:
Represents a managed device (workstation or server) on which the endpoint security agent is deployed and actively monitored.

Key Attributes

- **endpointId:** Unique identifier for the endpoint
- **hostname:** Logical name of the device
- **osType:** Operating system category (Windows, Linux, macOS)
- **agentVersion:** Installed agent version
- **status:** Operational and risk status of the endpoint
- **lastSeenAt:** Timestamp of the most recent communication
- **tags:** Logical labels for grouping and policy application

Class: Agent

Priority: Essential

Responsibility:
Logical representation of the software agent installed on an endpoint.

Attributes:

- agentId (UUID)
- capabilities (set: AV, EDR, DEVICE_CONTROL, FIREWALL)
- signatureVersion (string)
- policyId (UUID)

Class: Event

Priority: Essential

Responsibility:
A single normalized record from endpoints or integrated sources (firewall, IDS, AD, applications).

Attributes:

- eventId (UUID)
- source (enum: ENDPOINT, FIREWALL, IDS, AD, APPLICATION)
- timestamp (ISO-8601)
- severity (enum: INFO, LOW, MEDIUM, HIGH, CRITICAL)
- category (enum: AUTH, PROCESS, NETWORK, FILE, POLICY)
- payload (JSON)
-

CorrelationRule

Priority: Desirable

Responsibility:
Defines logic for converting events into alerts.

Attributes:

- ruleId
- name
- version
- conditionDSL
- enabled

Class: Log

Priority: Essential

Responsibility:
Storage-optimized representation of event streams for SIEM and long-term analysis.

Attributes:

- logId
- partitionKey
- eventCount
- sizeBytes
- retentionUntil

Class:Alert

Priority: Essential

Responsibility:
Result of correlation or detection logic indicating an actionable security condition.

Attributes:

- alertId (UUID)
- title (string)
- description (string)
- severity (enum)
- state (enum: NEW, IN_PROGRESS, RESOLVED, SUPPRESSED)
- sourceEvents (list)
- owner (userId)

3.3 Performance requirements

Refer 2.1.8

3.4 Design constraints

The solution must be optimized for SMEs with limited resources. This means the endpoint agent should consume minimal CPU and memory, ensuring it does not affect device performance. Resources in the cloud also should be minimal to reduce cost.

The design must support both Windows and Linux environments for endpoint agents. The dashboard should be accessible from web browsers without the use of third party software.

Since some SMEs lack proper internet connectivity, the system should work well in low bandwidth regions and should continue to operate when connectivity is lost. Local logging and device protection should continue until the connectivity is restored. Upon restoration the data needs to be synced with the cloud.

The agent must be designed in a way to prevent unauthorized tampering, modification and deletion by incorporating self-protecting mechanisms.

Since SMEs lack dedicated security analysts and technical persons, the system must prioritize automation. SOAR-style workflows should handle common incident response actions without requiring technical expertise from users.

The AI-driven detection engine must provide clear, human-readable explanations for alerts. This ensures that non-technical SME users can understand and act on security recommendations.

3.5 Software system attributes

3.5.1 Reliability

The system will keep watching for threats all the time without often breaking down or failing. The endpoint agent needs to keep working all the time, even if there are problems like someone trying to interfere with it or if the network goes down. To ensure reliability, we need to have systems in place that can monitor services and restart them if they stop working. The system should work at least 99. 9% of the time for its main features.

3.5.2 Availability

The solution should be ready for users whenever they need it, with very little time it's not working. The dashboard should be available during regular business hours and should still work for users even if the main server is not accessible. Syncing should happen automatically as soon as the connection is back. You can ensure high availability by using simple designs and backup systems for important parts.

3.5.3 Security

Security is an important part of the system. All records must be safely protected using SHA-256 hashing and Merkle trees to show if they have been changed. The connection between the endpoints and the dashboard needs to be secured with TLS encryption. Access control should be based on specific roles that are appropriate for small and medium-sized enterprises (SMEs). The system should have safety features to stop anyone from deleting or changing the agent without permission.

3.5.4 Maintainability

The design should be easy to update and fix, so that anyone can do it without needing special technical knowledge. The dashboard should have an easy way to update, manage rules, and check alerts. Modular architecture should allow for updates to individual parts (like AI models or agent software) without causing issues for the whole system.

3.6 Other requirements

The system needs to follow security and privacy rules important for small and medium-sized businesses. It should have easy-to-see logs of changes, keep records for checking, and allow settings for how long to keep data. It should focus on being easy to use, with a simple dashboard, clear alerts, and features that help people who aren't tech-savvy. The performance needs to be good for small and medium-sized business (SME) computers, so it should use little CPU and memory on devices and make the dashboard respond quickly. Support for different time zones and basic language options should be included, along with safe backup and restore features for settings and logs. The solution needs to include checking and monitoring important parts, automatic updates and fixes with options to go back if needed, and it should work well with usual directory services and notification systems. We should follow rules that protect privacy and reduce the amount of personal data we collect. This means only collecting what is necessary and making sure that important information is kept safe. Protection systems need to stop anyone from messing with the agent without permission. If the connection is lost, it should still be able to detect problems and keep a record of them. Documentation and setup guides should make it easy to install and configure the system. Licensing and pricing should be affordable for small and medium-sized businesses, without needing costly infrastructure or outside help.

4 Supporting information

References

[1] European Union Agency For Cybersecurity, June 2021, “Cybersecurity for SMEs – Challenges and Recommendations. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

[2] Project Proposals: ForLens – A Lightweight AI-Driven Endpoint Security Solution for Real-Time Threat Detection in SMEs, SLIIT Research Project, September 2025. Available: https://mysliit.sharepoint.com/sites/CDAPSubmissionCloud/2526JCloud/Forms/AllItems.aspx?id=%2Fsites%2FCDAPSubmissionCloud%2F2526JCloud%2F25%2D26J%2D076%2DStudents%2F1%2E%20Project%20Proposal%2FIndividual%20Reports&viewid=b6c5e95e%2Dd054%2D4e72%2Dbb46%2D33a9940141f2