Trustwave WebDefend Enterprise Software Security Target

Version 1.5

June 22, 2012

Trustwave
70 West Madison Street
Suite 1050
Chicago, IL 60602

DOCUMENT INTRODUCTION

Prepared By:

Common Criteria Consulting LLC
15804 Laughlin Lane
Silver Spring, MD 20906
http://www.consulting-cc.com

Prepared For:

Trustwave
70 West Madison Street
Suite 1050
Chicago, IL 60602
http://www.trustwave.com

REVISION HISTORY

Rev	Description
1.0	November 11, 2011, Initial release
1.1	March 2, 2012, Addressed ORs/CRs
1.2	March 6, 2012, Addressed additional ORs/CRs
1.3	April 2, 2012, Addressed certifier issues and FSP consistency
1.4	May 1, 2012, FSP consistency
1.5	June 22, 2012, Updated TOE version to 5.1SP1 and added additional documents to the TOE boundary

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS LIST

ACE	**Advanced Correlation Engine**
CC	**Common Criteria**
DBMS	**DataBase Management System**
DDPA	**Distributed Detect Prevent Architecture**
EAL	**Evaluation Assurance Level**
HTTP	**HyperText Transfer Protocol**
HTTPS	**HTTP Secure**
IDS	**Intrusion Detection System**
IETF	**Internet Engineering Task Force**
IP	**Internet Protocol**
IT	**Information Technology**
I&A	**Identification & Authentication**
LDAP	**Lightweight Directory Access Protocol**
ODBC	**Open DataBase Connectivity**
RFC	**Request For Comments**
SIM	**Security Information Management**
SNMP	**Simple Network Management Protocol**
SOAP	**Simple Object Access Protocol**
ST	**Security Target**
TCP	**Transmission Control Protocol**
TOE	**Target of Evaluation**
TSF	**TOE Security Function**
URL	**Uniform Resource Locator**
VLAN	**Virtual Local Area Network**
XML	**eXtensible Markup Language**

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the Trustwave WebDefend Enterprise Software. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3*. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

Trustwave WebDefend Enterprise Software Security Target, Version 1.5, dated June 22, 2012

1.2 TOE Reference

Trustwave WebDefend Enterprise Software Version 5.1SP1 (7.11.033-3.1).

The WebDefend Enterprise Software version includes versioning information for the overall release (e.g. 5.1SP1) as well as the version of the WebDefend Enterprise Manager (e.g. 7.11.033-3.1) included in the release.

1.3 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) augmented by ALC_FLR.2 from the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 3.

1.4 Keywords

Web application firewall, threats, risk, collection, analysis.

1.5 TOE Overview

1.5.1 Usage and Major Security Features

Trustwave WebDefend Enterprise (hereafter referred to as WebDefend) is a Web application firewall appliance that provides organizations with continuous, real-time Web application-specific security.

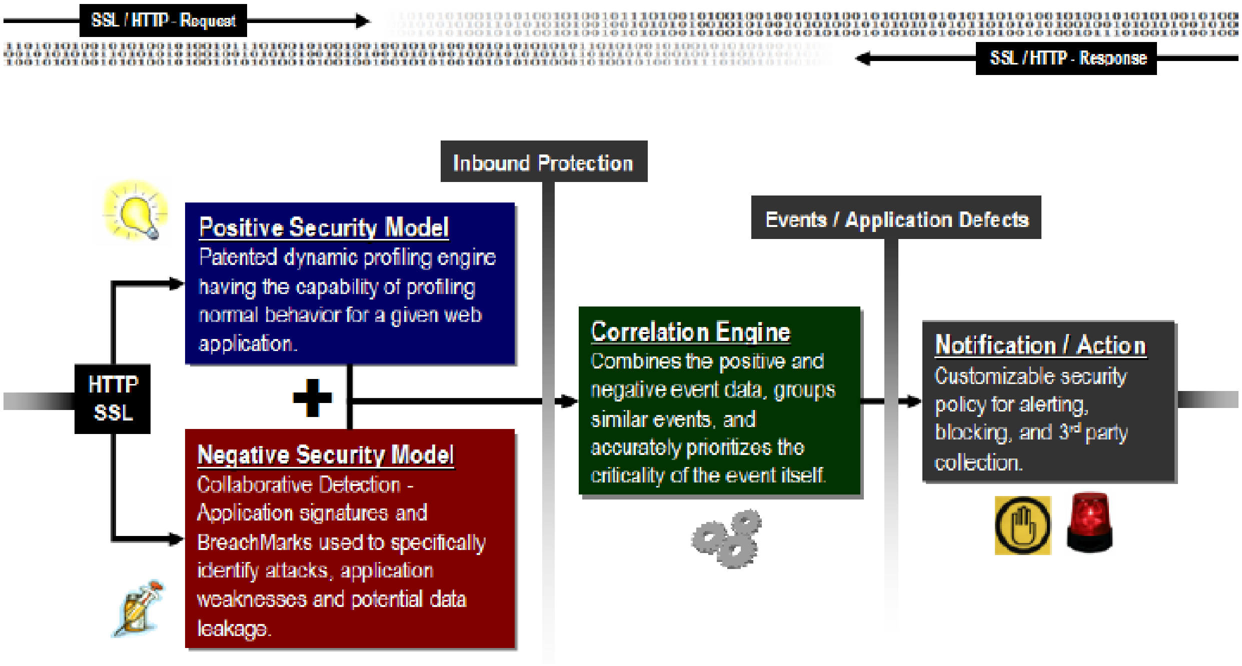
WebDefend is designed to address the unique security needs of Web applications. WebDefend combines a behavioral protection model with a set of collaborative detection engines to provide security analysis within the specific context of the Web application. In addition, WebDefend reduces the manual overhead in configuring its behavioral model, called a security profile, by automating the process of creating and updating this model.

WebDefend is provided with an Application Performance module and an Application Integrity module. These two modules provide information about the application user experience, in terms of application latency and responsiveness, application errors and application health. The Application Performance module functionality is not evaluated.

The WebDefend Console provides a single point of configuration and monitoring. The console helps organizations understand the context of events. For every event or defect detected, a detailed description pinpoints the problem, offers insight into its meaning and explains its resolution. The console offers multiple event views and drill-down capabilities, allowing administrators to identify events easily, examine root causes, view entire transactions and see error messages presented to site visitors. The console supports multiple roles, allowing different users to have different permissions.

WebDefend can be deployed both as an out-of-line appliance connected to a span port or network tap, or as an inline transparent appliance. WebDefend's distributed detect prevent architecture (DDPA) provides a full suite of responsive preventative actions as well as alerts, enabling centralized threat intelligence with flexible, distributed threat control. Actions include TCP resets, integration with firewalls, SIMs and other network devices and interfacing with the protected application to logout users. Integration actions are not evaluated. When deployed inline, WebDefend can also deny requests.

Figure 1 - DDPA


SSL / HTTP - Request
SSL / HTTP - Response
Inbound Protection
Events / Application Defects
Positive Security Model
Patented dynamic profiling engine having the capability of profiling normal behavior for a given web application.
HTTP SSL
Negative Security Model
Collaborative Detection - Application signatures and BreachMarks used to specifically identify attacks, application weaknesses and potential data leakage.
Correlation Engine
Combines the positive and negative event data, groups similar events, and accurately prioritizes the criticality of the event itself.
Notification / Action
Customizable security policy for alerting, blocking, and 3rd party collection.

WebDefend's patented Adaption™ technology automatically builds a positive security model for the Web application called a profile. Application profiles model normal acceptable behavior. This tailored security profile allows WebDefend to analyze the traffic in the context of appropriate behavior for each particular application. If a request does not validate against the application's profile, it is flagged as an anomaly and passed to WebDefend's multiple detection engines, which work collaboratively to determine the nature of the threat. The advanced correlation engine (ACE) uses information from the security policy to determine the appropriate action to take when an anomaly is found.

Features of WebDefend are explained in greater detail in the following sections.

1.5.1.1 Adaption – Automated Security Profile Management

WebDefend creates a custom security profile for each Web application, which is used to model an application’s acceptable behavior and provide a context in which to analyze each request sent to the application and each reply coming from it. This method allows WebDefend to detect whether a user's interaction with the application is legitimate (meaning, is the user using the application as designed?) and whether the output of the application is appropriate. Traffic identified as illegitimate or inappropriate is flagged as an anomaly and passed to the threat detection engines to determine if an actual attack is taking place.

WebDefend eliminates the need to manually create a custom security profile by automatically learning acceptable application behaviour for each site and application. WebDefend creates this profile by monitoring application traffic during a per-site or per-application learning period or continuously (based upon the adaption mode configured for each site and/or application). When specific components are validated as legitimate, they are added to the application's profile. When a site or application is in learning mode, other sites and applications are operating normally. When a site or application is configured for automatic mode (the recommended setting), the traffic is analyzed continuously and updates to the profile are made automatically as the analysis functions determines new or changed properties about the site or application.

When a site or application is in locked mode, the traffic is analyzed against all the configured rules. If any anomalous traffic is identified, the configured actions are taken. The difference from automatic mode is that no traffic analysis is performed for the purpose of updating the site or application profile.

When a site or application is in unprotected mode, no analysis of the traffic is performed and all traffic is passed through without any actions taken.

1.5.1.2 Profile Manager

WebDefend's console includes a Profile Manager for interacting with an application's profile. Each protected application has a profile that includes a site map, which is a full representation of the structure of an application in a tree structure. This tree structure provides a logical hierarchical view of the profile generated for each protected application. Nodes on the tree depict the URLs that represent acceptable application behavior, details of each URL, list types and ranges for parameters, as well as anticipated responses for each combination of parameters for a particular URL.

WebDefend's application profile includes characteristics that are learned and validated at the site level. The Profile Manager provides an interface for viewing and modifying settings to define the application's acceptable behavior for cookies, HTTP protocol, headers, and session identifiers. WebDefend's Profile Manager provides users with the ability to understand the context by which events are generated. When a security event is detected, users are able to directly open the URL related to the event, so they can understand what part of the application is affected and determine the significance of the attack.

1.5.1.3 Multiple Threat Detection Engines

The Behavioral Analysis engine provides positive validation of all application traffic against a profile of acceptable behavior. WebDefend creates and maintains a security profile of acceptable application behavior. The security profile maps all levels of application behavior, including HTTP protocol usage, all URL requests and corresponding responses, session management, and input validation parameters for every point of user interaction. All anomalous traffic is passed to the detection engines to identify any attacks and provide responsive actions.

The Signature Analysis engine provides a database of attack patterns to detect known vulnerabilities in Web applications. These signatures will identify any known attacks against a Web application or any of its components. Signature analysis provides a security context for the anomalies detected by the behavioural engine. Signatures are searched in a sophisticated manner in all traffic. When attacks are identified they are ranked by severity and can be responded to with preventative actions.

The Protocol Violation engine protects against protocol violation attacks to Web applications that exploit the HTTP and HTTPS protocols. WebDefend ensures that all communication with the application is in compliance with the HTTP and HTTPS protocol definitions, as defined by the IETF RFCs.

WebDefend maintains all current user session information and can detect attacks manipulating or hijacking user sessions, including session hijacking, hidden field manipulations, cookie hijacking, cookie poisoning and cookie tampering.

WebDefend provides bi-directional analysis of application communication. While all incoming traffic is checked for attacks, all outgoing traffic is analyzed as well. This outgoing analysis provides insight into sensitive information leaving an organization, the success of incoming attacks, as well as possible Web site defacements when an application's responses do not match what is expected from the profile.

WebDefend provides specific rules, called BreachMarks™, for most forms of privacy data such as social security numbers and credit cards. WebDefend monitors traffic leaving a Web application for patterns to identify information leakage. Organizations may also define their own custom BreachMarks to identify privileged Intellectual Property information that is specific to their organization. The custom BreachMark functionality is not evaluated.

Threats detected by all of the above detection engines are passed to the Advanced Correlation Engine (ACE) where they are analyzed in context of other events to reduce false positives, prioritize successful attacks, and provide indications of security defects detected in the application.

Exceptions may also be defined for each Site. The Exceptions are a prioritized list of conditions that override the associated Policy (which may be associated with multiple Sites). The configured Exception conditions are examined (in priority order) prior to the Policy conditions. For the first set of conditions that match, the configured action is performed. The actions that may be configured are the same as may be configured for Policies. Exception processing is terminated with the first matching Exception. If no Exception conditions match, the Event is processed according to the configured Policy.

1.5.1.4 Policy Manager

Within WebDefend, a policy describes the configuration options for the detection engines, as well as the responsive action to take if an event is detected. A policy lists the security events that WebDefend will look for in the application traffic and the responsive action to be taken for each event.

WebDefend's console includes a Policy Manager to enable users to view and configure their own security policies for WebDefend. The Policy Manager provides a list of events organized into categories within a tree structure. Each event may be enabled or disabled and responsive actions for each event can be configured, such as logging the event, denying a request, sending a TCP Reset or firewall blocking command (this functionality is not evaluated) or setting an SNMP trap.

WebDefend comes with standard policies that can be used out-of-the-box to provide different levels of protection. Users can modify these standard policies in the Policy Manager to create policies that are specific to their environment and applications.

1.5.1.5 Security Event Viewer

WebDefend's console includes a real-time event analysis module called the Security Event Viewer. As security events are detected for a protected application, they are listed in the Security Event Viewer.

WebDefend provides detailed, in-context information for every event detected and makes this data available for analysis. Each event detected by WebDefend is described in detail, including a description of the event with a summary, a full description, implications, fix information, and references for more information. In addition, the Security Event Viewer provides users with all the information used to determine that an event has occurred. A listing of the anomalies detected by the Behavioral Engine, as well as any correlated events, are listed for each security event detected, including the actual HTTP request and reply, allowing users to verify the reasoning behind each determination made by the various detection engines.

1.5.1.6 Integrity Issues Viewer

WebDefend’s Integrity Issues (Application Defects) Viewer provides the ability to detect and report on security defects in protected applications. This capability provides visibility into the security of production Web applications in true production environments.

WebDefend provides the ability to monitor all communication to and from a protected Web application. By leveraging application profiles that define normal behavior in both directions, WebDefend identifies and then analyzes abnormal responses from the application to determine and report the underlying application integrity issues. This analysis extends across all parts of the application as it is used, often to sections unreachable by scanners.

Issues identified by WebDefend are displayed in the Integrity Issues view that lists all the identified vulnerabilities within the Web application itself. This view also includes fields, such as (but not limited to) the last date that the issue was discovered, the exact URL affected, the issue description name and severity. Identified issues are listed once and updates are made to indicate the most recently discovered date when it is identified.

By taking a step beyond inbound attacks and leakage, WebDefend can actually detect when an application is misconfigured and/or insecurely coded – and can immediately communicate that issue. Application errors can be identified, logged and analyzed in full detail in the Application Integrity tab – including the full HTTP or HTTPS request and the Web application’s defective response, which contains the actual page view rendered to the end user.

1.5.2 TOE Type

IDS System

1.5.3 Required Non-TOE Hardware/Software/Firmware

The TOE consists of WebDefend software executing on a dedicated appliance along with the Console application executing on a Windows workstation. The dependencies for each of the software components are described in subsequent paragraphs.

Consoles must be installed on Windows PCs meeting the minimum requirements in the following table. The support software is automatically installed with the Console software if it is not already present on the system. Any number of Consoles may be installed.

Table 1 - Console Minimum Hardware/Software Requirements

Item	Requirements
Operating System	Microsoft Windows XP (SP3 or higher) Microsoft Windows 2003 (32 bit or 64 bit) (any SP level) Microsoft Windows 2008 (32 bit or 64 bit) (any SP level) Microsoft Windows Vista (32 bit or 64 bit) (SP2 or higher) Microsoft Windows 2008 (32 bit or 64 bit) (any SP level) Microsoft Windows 7 (32 bit or 64 bit) (SP1 or higher)
Memory	1GB
Hard Disk Free Space	80 MB
Support Software	MySQL Connector/ODBC 5.1

WebDefend Software is installed on hardened rPath Linux servers. The operating system, DBMS, web server and WebDefend Software are pre-installed on appliances supplied by Trustwave. The following table identifies the required software on the appliance.

Table 2 - WebDefend Appliance Minimum Software Requirements

Item	Requirements
Operating System	rPath Linux
DBMS	MySQL
Web Server	Apache

WebDefend Software is available on multiple models; all models have equivalent security functionality. The only differences involve processing power and storage capacity, which facilitate processing differing amounts of web application traffic. The following appliance choices are supported.

Table 3 - WebDefend Appliances

Model HW Item	GX30i	GX60i	GX110i	GX120i
CPU(s)	Quad Core CPU 2.4 GHz	Quad Core CPU 2.0 GHz	2 Quad Core CPU 2.0 GHz	2 Quad Core CPU 2.5 GHz
RAM	4GB	8GB	8GB	8GB
Disk	Single Disk 250GB disk, no RAID	Single Disk 250GB disk, no RAID	250GB RAID - 1	250GB RAID – 1
Throughput	50 Mbps	100 Mbps	450 Mbps	750 Mbps
Transactions/sec	6,000	8,000	12,000	18,000
Max. web sites protected	10	20	60	60

The Consoles and WebDefend software communicate with one another via a segregated management network to prevent disclosure or modification of the data exchanged between TOE components. It is the responsibility of the operational environment to protect the traffic on the management network from other (non-TOE) devices.

Multiple physical Ethernet interfaces are supported on the WebDefend appliances. A dedicated management interface is used for communication with Console instances; this interface is the only interface connected to the management network. Pairs of Ethernet interfaces are used for monitoring the web application traffic and responding to security events. These interfaces are connected to the same network as the web servers.

1.6 TOE Description

The TOE provides functionality to monitor both directions of web application traffic, detect security events, and respond to those events according to configured policies. The TOE consists of software only.

WebDefend Software components are installed on dedicated Linux servers; Consoles are installed on one or more Windows workstations.

WebDefend Software is pre-installed on appliances by Trustwave.

Typical inline and out-of-line deployments for these components are shown in the following diagrams.

Figure 2 - TOE Inline Deployment

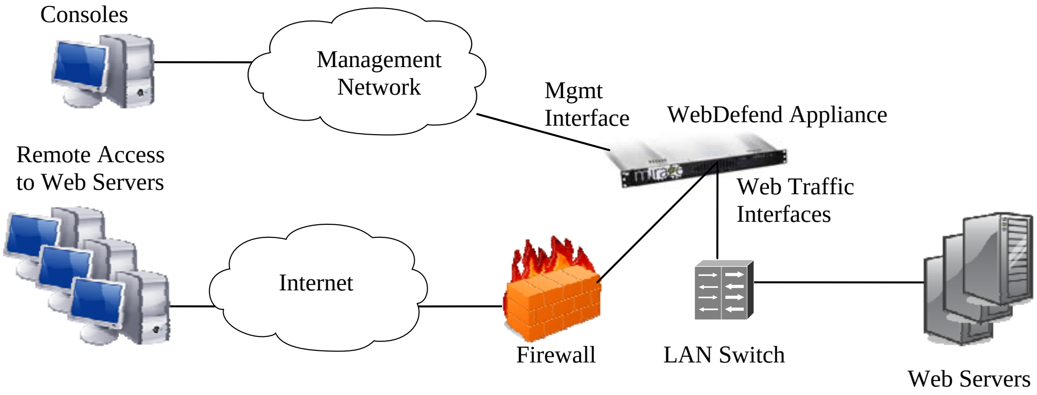
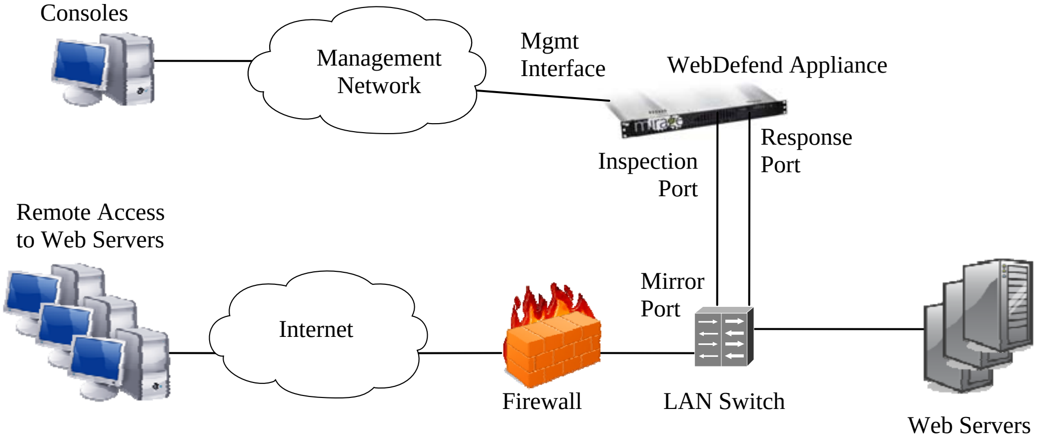


Figure 3 - TOE Out-of-Line Deployment



1.6.1 Physical Boundary

The physical boundary of the TOE is depicted in the following diagram (shaded items are within the TOE boundary).

Figure 4 - Physical Boundary

WebDefend Appliance	Console
WebDefend Applications and Services	Console Application
rPath Linux, MySQL and Apache	Microsoft Windows and MySQL Connector/ODBC
Hardware	Hardware

The physical boundary of the TOE includes the services and applications distributed by Trustwave to perform the WebDefend-specific functions described in this document. The following applications and services are included in the TOE physical boundary:

1. WebDefend Sensor Application – main Sensor function. This application monitors the web applications being protected, analyzes HTTP traffic and generates events, performs the behavioral learning and web application profile building, and executes the configured actions upon event detection.
2. WebDefend Manager – provides communication services with the Windows Console applications and distributes configuration updates to the Sensor application. This service is the interface to the database for insertion and retrieval of audit records, configuration information, System data and reports.

3. WebDefend Watchdog – monitors the WebDefend Sensor Application to ensure it is functioning correctly.
4. WebDefend Reporting Service – responsible for generating the configured WebDefend reports.
5. RPC – for inline deployments, this service is used by the WebDefend Sensor Application to configure the Apache web server.

The hardware and operating system (rPath Linux or Windows) are not included in the TOE boundary.

The physical boundary includes the following guidance documentation:

1. *Trustwave WebDefend Version 5.1 Getting Started Guide*
2. *Trustwave WebDefend Version 5.1 User Guide*
3. *Trustwave WebDefend Version 5.1 Common Criteria Supplement*
4. *Trustwave WebDefend V4.5 to V5.1 Upgrade Instructions*
5. *Trustwave WebDefend V5.0 to V5.1 Upgrade Instructions*
6. *Trustwave WebDefend V5.1 to V5.1SP1 Upgrade Instructions*

1.6.2 Logical Boundary

1.6.2.1 Audit

Audit records are generated for specific actions performed by users. The audit records are stored on the appliance and may be locally saved on the Console system by authorized administrators of the Console for review outside of the TOE. In the unlikely event audit storage space is exhausted, new audit records are discarded (the existing audit records are preserved). Audit records are automatically deleted according to the retention policy configured by authorized administrators.

1.6.2.2 Management

The TOE provides functionality for administrators to configure and monitor the operation of the TOE via the Console. The following administrator roles are supported: Primary Administrators, Organization Administrators, Site Administrators, Primary Viewers, Organization Viewers, and Site Viewers.

The security management functionality provided by the TOE includes:

- User management
- Sensor management
- Organization management
- Site management
- Report management

All TOE data is stored on the WebDefend appliance.

1.6.2.3 Web Application Firewall

The TOE monitors all web traffic going to and from specified web sites. The traffic is collected and analyzed against configured policies to detect security events, and when events are detected the configured reaction is invoked. Users may view the saved information via the Consoles.

The traffic analysis performed by the TOE includes:

- Known attack vector signature matching
- Application integrity checking
- Invalid protocol usage
- Invalid parameter values
- Data leakage

Security events fall into two categories: entry/informative events triggered by a configured policy that detects anomalous content in an application request, and exit events triggered by a configured policy violation in a reply from a web server (e.g. information leakage).

In the unlikely event System data storage space is exhausted, new System data is discarded (the existing System is preserved).

1.6.2.4 I&A

The TOE identifies and authenticates users of Consoles before they are granted access to any TSF functions or data. When valid credentials are presented, security attributes for the user are bound to the session. If incorrect passwords are presented on 3 consecutive login attempts for any user account, the account is automatically locked until unlocked by an authorized administrator.

1.6.3 TOE Data

The following table describes the TOE data.

Table 4 - TOE Data Descriptions

TOE Data	Description
Application Defects	A set of events related to problems detected in the responses of a monitored Application. Attributes of Application Defects include: • Site • Severity • Total Count • Sensor • Date/Time of first and most recent occurrence • Issue Name • Referrer • URL • Associated HTTP message(s)

TOE Data	Description
Applications	Specify a group of URLs within a Site that collectively represent a single Application for monitoring and reporting purposes. Attributes include: • Associated Site • Associated directories • Adaption Mode (unprotected, learning, locked, automatic)
BreachMarks	Predefined definitions for strings to be searched for in HTTP responses as possible data leakage indicators.
Exceptions	Site-specific conditions that override the action performed per the configured Policy. Attributes include: • Priority (relative to other Site Exceptions) • Unique ID • Associated URL(s) • Associated Entry Event(s) • Associated Exit Event(s) • Associated parameter(s) • Associated source address(es) • Associated Result(s) • Action to be performed • Status (enabled/disabled)
Organizations	Specify a list of organizational units for the purpose of administrative delegation and/or group policy application. Attributes include: • Associated Sites • Associated User Accounts • Associated Policies
Policies	Specify a set of Security Rules and BreachMarks to be applied to Sites. Attributes include: • Assigned Security Rules • Security Rule Status (active, inactive) • Associated BreachMarks
Report Templates	Specify parameters and scheduling information for a Report.
Reports	Generated Reports available for review.
Security Events	A set of events related to Policy violations detected for the Sites. Attributes of Security Events include: • Site • Severity • Host • Sensor • Date/Time • Description • Result • Entry/Informative Event • Exit Event • URL • Associated HTTP request and/or response messages • Status (ignored, updated as set by a user)

TOE Data	Description
Security Rule	Specify the analysis to be performed and the actions to be taken upon detection of the conditions specified in the rule. Attributes include: • Condition • Severity • Actions – Log, Alert, TCP Reset, Logout, Deny
Sensor	Specifies a WebDefend appliance acting as a sensor. In the evaluated configuration, a single appliance (sensor) is present. Attributes include: • Name • IP address • Type – only WebDefend is relevant in the evaluated configuration • Deployment mode - in inline (transparent bridge) or out-of-line • VLAN configuration - list of monitored and unmonitored VLANs. Traffic on monitored VLANs is analyzed, while traffic on unmonitored VLANs is ignored. • Associated Sites • Filters – IP addresses or networks for which events are not generated • Static Request Options – parameters in requests that cause profiling and/or inspection to be ignored • Ignore HTTP Parameters – HTTP parameters that are ignored • Enabled Modules – which analysis functions within WebDefend are enabled • Alert configuration – what System Events are enabled and what types of messages are sent when an Event occurs
Site Profiles	Specify properties for a Site. Profiles are generated automatically when the TOE monitors a Site. Attributes include: • HTTP constraints • Cookie configuration • Associated URL profiles • Username Tracking configuration • Excessive Access Rate Detection configuration

TOE Data	Description
Sites	Specifies one or more Sites and their properties. Site properties include: • Domain name • IP address and port • Associated Sensor • Associated Organization • Protocol used for access (HTTP/HTTPS) • Web server technology (e.g. Apache) • Encoding configuration • Assigned Policy • Session ID configuration • Adaption mode – unprotected, learning, locked, or automatic • Case sensitivity configuration • SSL certificate (for HTTPS sites) • Protection status • Prevention configuration • XML Schema properties • Alert Properties – specify the SNMP, Email or Syslog destination and message contents when an Alert occurs • Alerts Status (enabled, disabled) • Customized Page Not Found properties • Forbidden Character Group properties • Restricted Countries properties • Exceptions - URLs that do not generate a Security Event or Application Issue when they otherwise would
URL Profiles	Specify properties for a URL that define acceptable user behavior. Profiles are generated automatically when the TOE monitors a Site. Attributes include: • Associated Site • HTTP Methods configuration • Forceful Browsing Protection configuration • HTTP Request configuration • XML and SOAP configuration • Accessibility configuration • Parameters configuration • Fingerprint configuration • BreachMarks configuration
User Accounts	Specify a list of user accounts with the following attributes: • Account name • Password • Role • Assigned Organization(s) • Assigned Site(s) • Status (locked or unlocked)

1.7 Evaluated Configuration

The evaluated configuration of the TOE includes one instance of WebDefend Enterprise Software installed on an approved appliance and one or more instances of Console installed on Windows systems.

The following configuration restrictions apply to the evaluated configuration:

1. The following System Events are enabled and configured to send an email on each occurrence:
    a. Report Repository has reached its maximum size
    b. Report Repository has reached maximum number of reports
    c. Audit log is full
    d. Disk partition is full
2. Web Server Agents are not used.
3. External Sensors are not used.
4. Only local users are defined. Remote user authentication (via LDAP) is not used.
5. Custom BreachMarks are not configured.
6. Virtual Patching is not configured. This functionality is dependent on Scanner Integration, which is functionality that is not included in the evaluation.
7. The Command Line Interface (CLI) on the WebDefend appliance (Maintenance Tool) is used during installation only. The Console is the only user interface used operationally.
8. All modules in the Sensor are enabled (this is the default configuration).

2. Conformance Claims

2.1 Common Criteria Conformance

Common Criteria version: Common Criteria (CC) for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009

Common Criteria conformance: Part 2 extended and Part 3 conformant

2.2 Security Requirement Package Conformance

EAL2 augmented by ALC_FLR.2

The TOE does not claim conformance to any security functional requirement packages.

2.3 Protection Profile Conformance

The TOE does not claim conformance to any Protection profiles.

3. Security Problem Definition

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies:

A) assumptions about the environment,

B) threats to the assets and

C) organisational security policies.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the Operational Environment.

Table 5 - Assumptions

A.Type	Description
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.MGMTNETWORK	The TOE components will be interconnected by a segregated management network that protects the intra-TOE traffic from disclosure to or modification by untrusted systems or users.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	The TOE can only be accessed by authorized users.
A.PROTCT	The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical modification.

3.3 Threats

The threats identified in the following table are addressed by the TOE and the Operational Environment.

Table 6 - Threats

T.Type	Description
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

T.Type	Description
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data
T.SCNVUL	Users may take advantage of vulnerabilities in the IT System the TOE monitors to access unauthorized information from the IT system.

3.4 Organisational Security Policies

The Organisational Security Policies identified in the following table are addressed by the TOE and the Operational Environment.

Table 7 - Organisational Security Policies

P.Type	Description
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.ANALYZ	Analytical processes and information to derive conclusions about vulnerabilities must be applied to System data and appropriate response actions taken.
P.DETECT	Events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected and analyzed.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P.MANAGE	The TOE shall only be managed by authorized users.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

4. Security Objectives

This section identifies the security objectives of the TOE and the TOE's Operational Environment. The security objectives identify the responsibilities of the TOE and the TOE's Operational Environment in meeting the security needs. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the operational environment are designated as *OE.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 8 - Security Objectives for the TOE

O.Type	Description
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDANLZ	The TOE must apply analytical processes and information to the collected information to derive conclusions about vulnerabilities on the IT System it monitors.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.IDSENS	The TOE must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets.
O.INTEGR	The TOE must ensure the integrity of all audit and System data.
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows.
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.RESPON	The TOE must respond appropriately to analytical conclusions.

4.2 Security Objectives for the Operational Environment

The TOE's operational environment must satisfy the following objectives.

Table 9 - Security Objectives of the Operational Environment

OE.Type	Description
OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information.
OE.AUDIT_SORT	The IT Environment will provide the capability to sort the audit information.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.
OE.INTROP	The TOE is interoperable with the IT System it monitors

OE.Type	Description
OE.MGMTNETWORK	The operational environment will provide a segregated management network interconnecting the TOE components that protects the intra-TOE traffic from disclosure to or modification by untrusted systems or users.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.PROTECT	The IT environment will protect itself and the TOE from external interference or tampering.
OE.SD_PROTECTION	The IT Environment will provide the capability to protect system data.
OE.TIME	The IT Environment will provide reliable timestamps to the TOE

5. Extended Components Definition

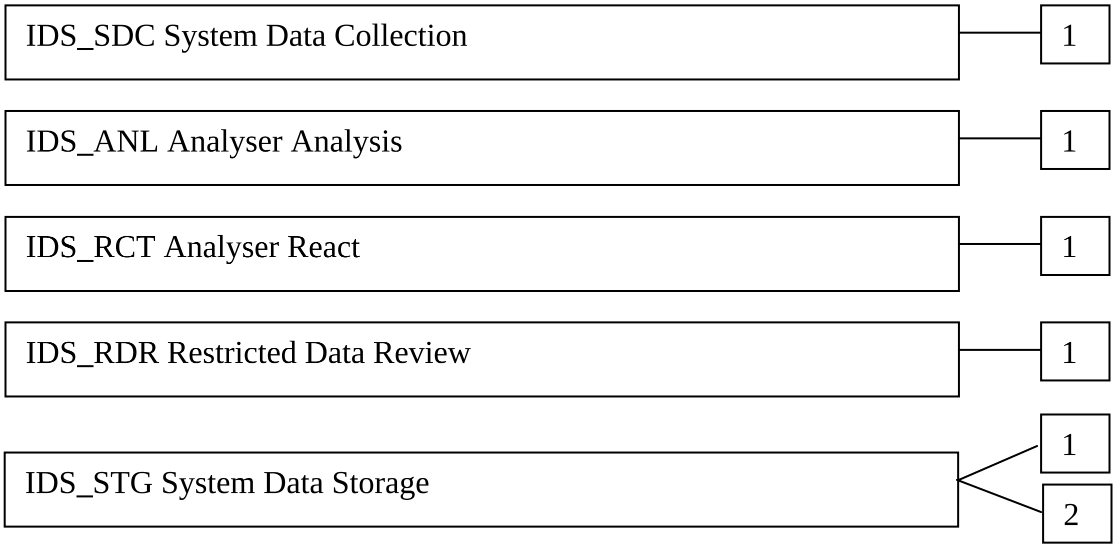
5.1 Extended Security Functional Components

5.1.1 Class IDS: Intrusion Detection

All of the components in this section are based on the class specified in the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments.

This class of requirements is taken from the IDS System PP to specifically address the data analysed by an IDS analyzer. The audit class of the CC (FAU) was used as a model for creating these requirements. The purpose of this class of requirements is to address the unique nature of analyser data and provide for requirements about analyzing, reviewing and managing the data.

Application Note: The PP does not provide hierarchy and dependency information for the extended SFRs defined in the PP. This information has been derived from the model SFRs referenced by the PP.


IDS_SDC System Data Collection
1
IDS_ANL Analyser Analysis
1
IDS_RCT Analyser React
1
IDS_RDR Restricted Data Review
1
IDS_STG System Data Storage
1
2

5.1.1.1 IDS_SDC.1 System Data Collection

Family Behaviour:

This family defines the requirements for the TOE regarding collection of information related to security events.

Component Levelling:

IDS_SDC System Data Collection
1

IDS_SDC.1 System Data Collection provides for the functionality to require TSF collection of data that may be related to security events.

Management:

The following actions could be considered for the management functions in FMT:

a) Configuration of the events to be collected.

Audit:

There are no auditable events foreseen.

IDS_SDC.1 System Data Collection

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

IDS_SDC.1.1 **The System shall be able to collect the following information from the targeted IT System resource(s):**

a) **[selection: *Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, data introduction, detected malicious code, access control configuration, service configuration, authentication configuration., accountability policy configuration, detected known vulnerabilities*]; and**

b) **[assignment: *other specifically defined events*].**

IDS_SDC.1.2 **At a minimum, the System shall collect and record the following information:**

a) **Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and**

b) **The additional information specified in the Details column of the table below.**

Table 10 - System Data Collection Events and Details

Component	Event	Details
IDS_SDC.1	Start-up and shutdown	none
IDS_SDC.1	Identification and authentication events	User identity, location, source address, destination address
IDS_SDC.1	Data accesses	Object IDs, requested access, source address, destination address
IDS_SDC.1	Service Requests	Specific service, source address, destination address
IDS_SDC.1	Network traffic	Protocol, source address, destination address
IDS_SDC.1	Security configuration changes	Source address, destination address
IDS_SDC.1	Data introduction	Object IDs, location of object, source address, destination address
IDS_SDC.1	Detected malicious code	Location, identification of code
IDS_SDC.1	Access control configuration	Location, access settings
IDS_SDC.1	Service configuration	Service identification (name or port), interface, protocols
IDS_SDC.1	Authentication configuration	Account names for cracked passwords, account policy parameters
IDS_SDC.1	Accountability policy configuration	Accountability policy configuration parameters
IDS_SDC.1	Detected known vulnerabilities	Identification of the known vulnerability

Application Note: The rows in this table must be retained that correspond to the selections in IDS_SDC.1.1 when that operation is completed. If additional events are defined in the assignment in IDS_SDC.1.1, then corresponding rows should be added to the table for this element.

5.1.1.2 IDS_ANL Analyser Analysis

Family Behaviour:

This family defines the requirements for the TOE regarding analysis of information related to security events.

Component Levelling:

IDS_ANL.1 Analyser Analysis provides for the functionality to require TSF controlled analysis of data collected that is related to security events.

Management:

The following actions could be considered for the management functions in FMT:

a) Configuration of the analysis to be performed.

Audit:

There are no auditable events foreseen.

IDS_ANL.1 Analyser Analysis

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System Data Collection

IDS_ANL.1.1 **The TSF shall perform the following analysis function(s) on all System data received:**

a) **[selection: *statistical, signature, integrity*]; and**

b) **[assignment: *other analytical functions*].**

Application Note: Statistical analysis involves identifying deviations from normal patterns of behaviour. For example, it may involve mean frequencies and measures of variability to identify abnormal usage. Signature analysis involves the use of patterns corresponding to known attacks or misuses of a system. For example, patterns of system settings and user activity can be compared against a database of known attacks. Integrity analysis involves comparing system settings or user activity at some point in time with those of another point in time to detect differences.

IDS_ANL.1.2 **The TSF shall record within each analytical result at least the following information:**

a) **Date and time of the result, type of result, identification of data source; and**

b) **[assignment: *other security relevant information about the result*].**

Application Note: The analytical conclusions drawn by the analyser should both describe the conclusion and identify the information used to reach the conclusion.

5.1.1.3 IDS_RCT Analyser React

Family Behaviour:

This family defines the requirements for the TOE regarding reactions to the analysis of information related to security events received from remote IT systems when a vulnerability is detected.

Component Levelling:

IDS_RCT.1 Analyser React provides for the functionality to require TSF controlled reaction to the analysis of data received from remote IT systems regarding information related to security events when an intrusion is detected.

Management:

The following actions could be considered for the management functions in FMT:

a) the management (addition, removal, or modification) of actions.

Audit:

There are no auditable events foreseen.

IDS_RCT.1 Analyser React

Hierarchical to: No other components.

Dependencies: IDS_ANL.1 Analyser Analysis

IDS_RCT.1.1 **The System shall send an alarm to [assignment: *alarm destination*] and take [assignment: *appropriate actions*] when a vulnerability is detected.**

Application Note: There must be an alarm, though the ST should refine the nature of the alarm and define its target (e.g., administrator console, audit log). The TSF may optionally perform other actions when vulnerabilities are detected; these actions should be defined in the ST.

5.1.1.4 IDS_RDR Restricted Data Review

Family Behaviour:

This family defines the requirements for the TOE regarding review of the System data collected or generated by the TOE.

Component Levelling:

IDS_RDR.1 Restricted Data Review provides for the functionality to require TSF controlled review of the System data collected or generated by the TOE.

Management:

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the group of users with read access right to the System data records.

Audit:

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Basic: Attempts to read System data that are denied.

b) Detailed: Reading of information from the System data records.

IDS_RDR.1 Restricted Data Review

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System Data Collection
IDS_ANL.1 Analyser Analysis

IDS_RDR.1.1 The System shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of System data*] from the System data.

Application Note: This requirement applies to authorised users of the System. The requirement is left open for the writers of the ST to define which authorised users may access what System data.

IDS_RDR.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information.

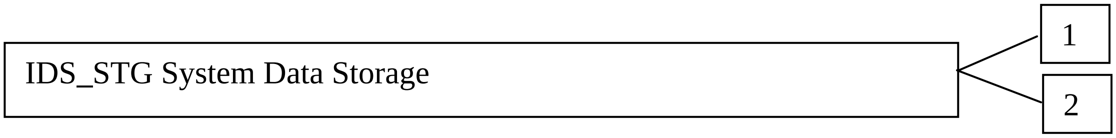
IDS_RDR.1.3 The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

5.1.1.5 IDS_STG System Data Storage

Family Behaviour:

This family defines the requirements for the TOE to be able to create and maintain a secure System data trail.

Component Levelling:



IDS_STG.1 Guarantee of System Data Availability requires that the System data be protected from unauthorised deletion and/or modification and defines the behaviour when specific conditions occur.

IDS_STG.2 Prevention of System Data Loss defines the actions to be taken if the System data storage capacity has been reached.

Management: IDS_STG.1

The following actions could be considered for the management functions in FMT:

a) maintenance of the parameters that control the System data storage capability.

Management: IDS_STG.2

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of actions to be taken in case System data storage capacity has been reached.

Audit: IDS_STG.1

There are no auditable events foreseen.

Audit: IDS_STG.2

There are no auditable events foreseen.

IDS_STG.1 Guarantee of System Data Availability

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System Data Collection
IDS_ANL.1 Analyser Analysis

IDS_STG.1.1 **The System shall protect the stored System data from unauthorised deletion.**

IDS_ STG.1.2 **The System shall protect the stored System data from modification.**

Application Note: Authorised deletion of data is not considered a modification of System data in this context. This requirement applies to the actual content of the System data, which should be protected from any modifications.

IDS_ STG.1.3 **The System shall ensure that [assignment: *metric for saving System data*] System data will be maintained when the following conditions occur: [selection: *System data storage exhaustion, failure, attack*].**

Application Note: The ST needs to define the amount of System data that could be lost under the identified scenarios.

IDS_STG.2 Prevention of System data loss

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System Data Collection
IDS_ANL.1 Analyser Analysis

IDS_STG.2.1 **The System shall [selection: *'ignore System data', 'prevent System data, except those taken by the authorised user with special rights', 'overwrite the oldest stored System data'*] and send an alarm if the storage capacity has been reached.**

Application Note: The ST must define what actions the System takes if the result log becomes full. Anything that causes the System to stop analysing events may not be the best solution, as this will only affect the System and not the system on which it is analysing data (e.g., shutting down the System).

5.2 Extended Security Assurance Components

None

6. Security Requirements

This section contains the security requirements that are provided by the TOE.

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in italics

Selection: indicated in underlined text

Assignments within selections: indicated in italics and underlined text

Refinement: indicated with bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by numbers in parentheses following the component or element (e.g., FAU_ARP.1(1)).

6.1 TOE Security Functional Requirements

The functional requirements are described in detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation* and/or the previous chapter of this document with the exception of completed operations.

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified level of audit; and

c) *The events in the following table*.

Table 11 - Auditable Events

SFR	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
	Access to System	IP address of the remote system
	Access to the TOE System data	
FIA_UAU.2	Use of the authentication mechanism	User identity, location
FIA_UID.2	Use of the identification mechanism	User identity, location
FMT_MTD.1	Modifications to the values of TSF data	
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *the User IP address, User TCP port, Sensor name, and Sensor IP address*.

6.1.1.2 FAU_STG.2 Guarantees of Audit Data Availability

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to <u>prevent</u> unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that *the oldest* stored audit records will be maintained when the following conditions occur: <u>audit storage exhaustion</u>.

Application Note: In the unlikely event audit storage space is exhausted, new audit records are discarded (the existing audit records are preserved).

6.1.1.3 FAU_STG.4 Prevention of Audit Data Loss

FAU_STG.4.1 The TSF shall <u>ignore audited events</u> and *send an Alert* if the audit trail is full.

Application Note: In the unlikely event audit storage space is exhausted, new audit records are discarded (the existing audit records are preserved).

6.1.2 Identification and Authentication (FIA)

6.1.2.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when <u>*3*</u> unsuccessful authentication attempts occur related to *consecutive login failure attempts of an individual User Account*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been <u>met</u>, the TSF shall *lock the User Account*.

6.1.2.2 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) User identity;

b) Password;

c) Role;

d) Organization;

e) Assigned Sites; and

f) Status (locked or unlocked).

6.1.2.3 FIA_UAU.2 User Authentication Before Any Action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.2.4 FIA_UID.2 User Identification Before Any Action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.3 Security Management (FMT)

6.1.3.1 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, delete, *create* the *data identified in the following table* to *the authorised identified roles identified in the following table*.

Table 12 - TSF Data Access Details

TSF Data	Primary Admin	Org. Admin	Site Admin	Primary Viewer	Org. Viewer	Site Viewer
Application Defects	Query and Delete all	Query and Delete any within the Organization	Query and Delete any within the Assigned Sites	Query all	Query any within the Organization	Query any within the Assigned Sites
Applications	Create, Query, Modify and Delete all	Create, Query, Modify and Delete any within the Organization	Create, Query, Modify and Delete any within the Assigned Sites	Query all	Query any within the Organization	Query any within the Assigned Sites
Exceptions	Create, Query, Modify and Delete all	Create, Query, Modify and Delete any within the Organization	Create, Query, Modify and Delete any within the Assigned Sites	None	None	None
Organizations	Create, Query, Modify and Delete all	None	None	Query all	None	None

TSF Data	Primary Admin	Org. Admin	Site Admin	Primary Viewer	Org. Viewer	Site Viewer
Policies	Create, Query, Modify and Delete all	Create, Query, Modify and Delete any within the Organization Query all default Policies	Create, Query, Modify and Delete any within the Organization Query all default Policies	Query all	Query any within the Organization Query all default Policies	Query any within the Organization Query all default Policies
Report Templates	Create, Query, Modify and Delete all	Create, Query, Modify and Delete any within the Organization	Create, Query, Modify and Delete any created by the same user	Create and Query all Modify and Delete any created by the same user	Create and Query any within the Organization Modify and Delete any created by the same user	Create, Query, Modify and Delete any created by the same user
Reports	Create, Query and Delete all	Create all Query and Delete any within the Organization	Create all Query and Delete any created by the same user	Create and Query all Delete any created by the same user	Create all Query any within the Organization Delete any created by the same user	Create all Query and Delete any created by the same user
Security Events	Query and Delete all	Query and Delete any within the Organization	Query and Delete any within the Assigned Sites	Query all	Query any within the Organization	Query any within the Assigned Sites
Security Rule	Query, Modify and Delete all	Query, Modify and Delete any within the Organization	Query, Modify and Delete any within the Assigned Sites	Query all	Query any within the Organization	Query any within the Assigned Sites
Sensor	Query, Modify and Delete all	None	None	Query all	None	None
Site Profiles	Query, Modify and Delete all	Query, Modify and Delete any within the Organization	Query, Modify any within the Assigned Sites	Query all	Query any within the Organization	Query any within the Assigned Sites

TSF Data	Primary Admin	Org. Admin	Site Admin	Primary Viewer	Org. Viewer	Site Viewer
Sites	Create, Query, Modify and Delete all	Create, Query, Modify and Delete any within the Organization	Query any within the Assigned Sites	Query all	Query any within the Organization	Query any within the Assigned Sites
URL Profiles	Query, Modify and Delete all	Query, Modify and Delete any within the Organization	Query, Modify and Delete any within the Assigned Sites	Query all	Query any within the Organization	Query any within the Assigned Sites
User Accounts	Create, Query, Modify and Delete all	Create, Query, Modify and Delete within the Organization	None	Query all except Primary Administrators and Primary Viewers	Query within the Organization	None

Application Note: All users are required to change their password upon first successful login..

6.1.3.2 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

a) *User management;*

b) *Sensor management;*

c) *Organization management;*

d) *Site management;*

e) *Report management.*

6.1.3.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles *Primary Administrators, Organization Administrators, Site Administrators, Primary Viewers, Organization Viewers, and Site Viewers*.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.4 Intrusion Detection (IDS)

6.1.4.1 IDS_SDC.1 System Data Collection

IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

a) <u>network traffic,</u>; and

b) *no other events*.

IDS_SDC.1.2 At a minimum, the System shall collect and record the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) The additional information specified in the Details column of the table below.

Table 13 - System Data Collection Events and Details

Component	Event	Details
IDS_SDC.1	Network traffic	Protocol, source address, destination address

6.1.4.2 IDS_ANL.1 Analyser Analysis

IDS_ANL.1.1 The TSF shall perform the following analysis function(s) on all System data received:

a) signature, integrity and

b) *invalid protocol usage, invalid parameter values, and data leakage*.

IDS_ANL.1.2 The TSF shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and

b) *associated HTTP messages*.

6.1.4.3 IDS_RCT.1 Analyser React

IDS_RCT.1.1 The System shall send an alarm to *the configured notification destinations for an Alert* and take *the configured actions* when a vulnerability is detected.

6.1.4.4 IDS_RDR.1 Restricted Data Review

IDS_RDR.1.1 The System shall provide *authorised users* with the capability to read *Security Events and Application Defects for the Organizations and Sites they are authorized to view* from the System data.

IDS_RDR.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information.

IDS_RDR.1.3 The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

6.1.4.5 IDS_STG.1 Guarantee of System Data Availability

IDS_STG.1.1 The System shall protect the stored System data from unauthorised deletion.

IDS_ STG.1.2 The System shall protect the stored System data from modification.

IDS_ STG.1.3 The System shall ensure that *the oldest* System data will be maintained when the following conditions occur: System data storage exhaustion.

Application Note: In the unlikely event System data storage space is exhausted, new System data is discarded (the existing System data is preserved).

6.1.4.6 IDS_STG.2 Prevention of System data loss

IDS_STG.2.1 The System shall ignore System data and send an alarm if the storage capacity has been reached.

Application Note: In the unlikely event System data storage space is exhausted, new System data is discarded (the existing System data is preserved).

6.2 TOE Security Assurance Requirements

The assurance requirements are identified in the following table. These requirements reference Part 3 of the *Common Criteria for Information Technology Security Evaluation*.

The TOE meets the assurance requirements for EAL2 augmented by ALC_FLR.2. These requirements are summarised in the following table.

Table 14 - EAL2+ Assurance Requirements

Assurance Class	Component ID	Component Title
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

6.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 15 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No other components.	FPT_STM.1	Satisfied by the operational environment (OE.TIME).
FAU_STG.2	FAU_STG.1	FAU_GEN.1	Satisfied
FAU_STG.4	FAU_STG.3	FAU_STG.1	Satisfied by FAU_STG.2
FIA_AFL.1	No other components.	FIA_UAU.1	Satisfied by FIA_UAU.2
FIA_ATD.1	No other components.	None	n/a
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Satisfied by FIA_UID.2
FIA_UID.2	FIA_UID.1	None	n/a
FMT_MTD.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components.	None	n/a
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied by FIA_UID.2
IDS_SDC.1	No other components.	FPT_STM.1	Satisfied by the operational environment (OE.TIME).
IDS_ANL.1	No other components.	IDS_SDC.1	n/a
IDS_RCT.1	No other components.	IDS_ANL.1	Satisfied
IDS_RDR.1	No other components.	IDS_SDC.1 IDS_ANL.1	Satisfied Satisfied
IDS_STG.1	No other components.	IDS_SDC.1 IDS_ANL.1	Satisfied Satisfied
IDS_STG.2	No other components.	IDS_SDC.1 IDS_ANL.1	Satisfied Satisfied

7. TOE Summary Specification

7.1 FAU_GEN.1

The TOE generates audits for the events specified in the table included with the FAU_GEN.1(1). Startup and shutdown of the audit function is equivalent to startup and shutdown of the WebDefend Software components. The following fields are included in all audit records, although not all fields are populated in all records:

- Record ID
- Date/time
- User Name (subject identity)
- User Source IP address (location)
- User Source TCP Port
- Application
- Sensor Name
- Sensor IP
- Site Name
- Manager IP (in the evaluated configuration, the Manager is the same as the Sensor)
- Result
- Action (Event)

When items with multiple parameters are configured, multiple records may be generated, recording one parameter value per record. The primary audit record indicates the item being configured, while the secondary audit records indicate the specific parameter values. Secondary audit records point to the item being configured by containing the Record ID of the associated primary audit record. Primary audit records either contain 0 or their own Record ID in this field.

The audits records are maintained by the TOE in the database on the WebDefend appliance in plain text and may be exported via the Console by Primary Administrators for review outside the TOE.

7.2 FAU_STG.2, FAU_STG.4

The user access functionality of the TOE does not provide any mechanism to modify or delete audit records. If no space is available in the database when the TOE attempts to insert a new audit record, the existing audit records are retained and the new audit record is discarded. When this occurs, a System Event is generated and a message is sent to the Alert destination configured for the Sensor.

7.3 FIA_AFL.1

The TOE tracks consecutive login failures for each defined user account. If three consecutive failures occur for any user account (for any combination of Console accesses), the user account is automatically locked. The account must be manually unlocked before logins against it are permitted.

7.4 FIA_ATD.1

The TOE maintains the following information for each user account:

- User identity;
- Password;
- Role;
- Organization;
- Assigned Sites; and
- Status (locked or unlocked).

User account information is stored in the database on the WebDefend appliance.

7.5 FIA_UAU.2, FIA_UID.2

The TOE requires all users of the Consoles to successfully identify and authenticate themselves via a username and password before access is granted to any TSF data or functions. Validation of the supplied credentials is performed by the TOE.

7.6 FMT_MTD.1

The TOE grants access to TSF data via Consoles according to the roles and permissions specified in the table included with FMT_MTD.1(1). Consoles may only be used by authorized users. Access to TSF data other than that specified in the table is prevented.

7.7 FMT_SMF.1

The TOE provides functionality for authorized users to manage the following items via the Console:

- User management (User Accounts);
- Sensor management (Sensors);
- Organization management (Organizations, Sites);
- Site management (Application Defects, Applications, Policies, Security Events, Security Rules, Site Profiles, URL Profiles);
- Report management (Report Templates, Reports).

7.8 FMT_SMR.1

All interactive users of the TOE are required to successfully complete I&A, at which time the role configured for the user account is associated with the user session. The role assigned to the user account determines the access permissions for the user per the table with FMT_MTD.1. The roles that may be assigned to a user are: Primary Administrators, Organization Administrators, Site Administrators, Primary Viewers, Organization Viewers, and Site Viewers.

7.9 IDS_SDC.1

The TOE collects network traffic for the configured Sites. The traffic is used for analysis against configured policies and to detect profile changes for sites and/or applications. When a security event is generated, the network traffic associated with the event is stored with the event in the database on the WebDefend appliance.

7.10 IDS_ANL.1, IDS_RCT.1

As network traffic is collected, it is analyzed by the TOE. Analysis is performed for the following functions based upon the Exceptions and Policy associated with the applicable Site:

- Profiles are generated and updated based on the interactions contained in the traffic.
- Comparisons are made to signatures of known attacks (signature analysis).
- Responses from the applications are monitored to detect abnormalities based on the profiles (integrity analysis).
- Comparisons are made to previous message contents to detect anomalous behavior.
- HTTP protocol violations are detected.
- Invalid parameter values are detected.
- Comparisons to BreachMarks are made to detect data leakage in messages sent from the protected web servers.
- Excessive access violations (signature analysis)

The following information is stored for Security Events:

- Site
- Severity
- Host
- Sensor
- Date/Time
- Description
- Result
- Entry/Informative Event
- Exit Event
- URL
- Associated HTTP request and/or response messages
- Status

The following information is stored for Application Defects:

- Site
- Severity
- Total Count
- Sensor

- Date/Time of first and most recent occurrence
- Issue Name
- Referrer
- URL
- Associated HTTP message(s)

Prior to generating an Event and performing the configured action, the configured Exceptions are examined to determine if any overrides of the Policy apply. The configured Exceptions are checked in priority order to determine if any Exception conditions match the conditions associated with the Event. If so, the Exception actions are performed rather than the Policy actions. As soon as one matching Exception is found, Exception checking is halted.

When a configured condition is detected, the associated actions are performed as follows:

- Log – A Security Event or Application Defect is generated and
- Alert - The configured Alert parameters are used to send an SNMP, E-mail or Syslog message
- TCP Reset – TCP Reset messages are sent to the web server and client.
- Logout – An HTTP Logout message is sent to the web server.
- Deny – The message being analyzed is dropped. This action is only available with the inline deployment mode.

7.11 IDS_RDR.1

The TOE provides authorized users with the ability to read Security Events, Application Defects, and captured traffic in a human readable form via the Consoles. The information is presented through views, dashboards, and reports. Access to information is limited to the Organizations and Sites each user is authorized to access.

7.12 IDS_STG.1, IDS_STG.2

The user access functionality of the TOE does not provide any mechanism to modify System data. System data may be deleted by authorized users. If no space is available in the database when the TOE attempts to insert new System data, the existing information is retained and the new information is discarded. When this occurs, a System Event is generated and a message is sent to the Alert destination configured for the Sensor.

8. Protection Profile Claims

Conformance to a Protection Profile is not claimed.

9. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions and threats. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functional.

9.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective.

The following table identifies for each organizational security policy, threat and assumption, the security objective(s) that address it.

Table 16 - Security Objectives Mapping

	O.ACCESS	O.AUDITS	O.EADMIN	O.IDANLZ	O.IDAUTH	O.IDSENS	O.INTEGR	O.OFLOWS	O.PROTCT	O.RESPON	OE.AUDIT_PROTECTION	OE.AUDIT_SORT	OE.CREDEN	OE.INSTAL	OE.INTROP	OE.MGMTNETWORK	OE.PERSON	OE.PHYCAL	OE.PROTECT	OE.SD_PROTECTION	OE.TIME
A.ACCESS															X						
A.ASCOPE															X						
A.DYNMIC															X		X				
A.LOCATE																		X			
A.MANAGE																	X				
A.MGMTNETWORK																X					
A.NOEVIL													X	X				X			
A.NOTRUST													X					X			
A.PROTCT																		X			
P.ACCACT		X			X							X									X
P.ACCESS	X				X				X		X									X	
P.ANALYZ				X						X											
P.DETECT				X		X															X
P.INTGTY							X				X									X	
P.MANAGE	X		X		X				X				X	X			X				
P.PROTCT								X										X	X		
T.COMDIS	X				X				X										X		
T.COMINT	X				X		X		X										X		
T.IMPCON	X		X		X									X							
T.LOSSOF	X				X		X		X												
T.MISACT						X															
T.MISUSE						X															
T.PRIVIL	X				X				X												
T.SCNVUL				X		X															

The following table describes the rationale for the security objectives mappings.

Table 17 - Rationale For Security Objectives Mappings

Item	Security Objectives Rationale
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions. The OE.INTROP objective ensures the TOE has the needed access.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors. The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors. The OE.INTROP objective ensures the TOE has the proper access to the IT System. The OE.PERSON objective ensures that the TOE will be managed appropriately.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. The OE.PHYCAL provides for the physical protection of the TOE.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
A.MGMTNETWORK	The OE.MGMTNETWORK objective ensures that the TOE components will be interconnected by a segregated management network that protects the intra-TOE traffic from disclosure to or modification by untrusted systems or users.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.NOTRUST	The TOE can only be accessed by authorized users. The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.PROTCT	The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical modification. The OE.PHYCAL provides for the physical protection of the TOE software and the hardware on which it is installed.
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE. The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The OE.TIME objective supports this policy by providing a time stamp for insertion into the audit records. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. The OE.AUDIT_SORT objective supports this policy by providing a mechanism for administrators to sort the audit logs for effective review.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.AUDIT_PROTECTION and OE.SD_PROTECTION objectives counter this threat via IT Environment protections of the audit trail. The O.PROTCT objective addresses this policy by providing TOE self-protection.

Item	Security Objectives Rationale
P.ANALYZ	Analytical processes and information to derive conclusions about vulnerabilities must be applied to System data and appropriate response actions taken. The O.IDANLZ objective requires analytical processes be applied to data collected. The O.RESPON objective requires the TOE to respond appropriately to the detected vulnerabilities.
P.DETECT	Events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected and analyzed. The O.IDSENS and O.IDANLZ and objectives address this policy by requiring collection and analysis of network traffic for the monitored IT Systems. The OE.TIME objective supports this policy by providing a time stamp for insertion into the System data records.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification. The O.INTEGR objective ensures the protection of data from modification. The OE.AUDIT_PROTECTION and OE.SD_PROTECTION objectives ensure the protection of audit and System data from outside the TSF.
P.MANAGE	The TOE shall only be managed by authorized users. The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self-protection.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions. The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions (overflows) of audit and System data storage (these are the only TOE data items that are dynamically created without human interaction). The OE.PHYCAL objective protects the TOE from unauthorized physical modifications. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.PROTCT objective addresses this threat by providing TOE self-protection. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures the integrity of all audit and System data. The O.PROTCT objective addresses this threat by providing TOE self-protection. The OE.PROTECT objective supports the TOE protection from the IT Environment.

Item	Security Objectives Rationale
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected. The OE.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors. The O.IDSENS objective addresses this threat by requiring a TOE to collect Sensor data.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors. The O.IDSENS objective addresses this threat by requiring a TOE to collect Sensor data.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.SCNVUL	Users may take advantage of vulnerabilities in the IT System the TOE monitors to access unauthorized information from the IT system. The O.IDSENS and O.IDANLZ objectives counter this threat by requiring a TOE to collect and analyze traffic involving the IT System to detect indications of a vulnerability.

9.2 Security Requirements Rationale

9.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each TOE security objective, the SFR(s) that address it.

Table 18 - SFRs to Security Objectives Mapping

	O.ACCESS	O.AUDITS	O.EADMIN	O.IDAUTH	O.IDANLZ	O.IDSENS	O.INTEGR	O.OFLOWS	O.PROTCT	O.RESPON
FAU_GEN.1		X								
FAU_STG.2	X	X		X			X	X	X	
FAU_STG.4		X						X		
FIA_AFL.1				X						
FIA_ATD.1				X						
FIA_UAU.2	X			X						
FIA_UID.2	X			X						
FMT_MTD.1	X			X			X		X	
FMT_SMF.1	X		X				X			
FMT_SMR.1				X						
IDS_ANL.1					X					
IDS_RCT.1										X
IDS_RDR.1	X			X						
IDS_SDC.1						X				
IDS_STG.1	X			X			X	X	X	
IDS_STG.2								X		

The following table provides the detail of TOE security objective(s).

Table 19 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.2, FIA_UAU.2]. Authorized users are granted access to data based upon their configured security attributes [FMT_MTD.1]. The System is required to protect the audit trail and System data from any modification and unauthorized deletion [FAU_STG.2, IDS_STG.1]. The appropriate TOE management functions are identified [FMT_SMF.1].
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions. Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must prevent unauthorized modification and deletion of audit data as well as the loss of collected data in the event the audit trail is full [FAU_STG.2, FAU_STG.4].
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data. The management functions provided by the TOE are specified [FMT_SMF.1].

Security Objective	SFR and Rationale
O.IDANLZ	The TOE must apply analytical processes and information to the collected information to derive conclusions about vulnerabilities on the IT System it monitors. The Analyzer is required to perform vulnerability analysis and generate conclusions [IDS_ANL.1].
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.2, FIA_UAU.2]. The TOE mitigates against brute force login attempts by automatically locking accounts upon repeated login failures [FIA_AFL.1]. Authorized users are granted access to data based upon their configured security attributes [FMT_MTD.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1]. The System is required to protect the audit trail and System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion [FAU_STG.2, IDS_STG.1].
O.IDSENS	The TOE must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets. The TOE is required to collect events indicative of vulnerabilities on IT System being monitored [IDS_SDC.1].
O.INTEGR	The TOE must ensure the integrity of all audit and System data. Only authorized administrators of the System may query or add audit and System data [FMT_MTD.1]. The System is required to protect the audit trail and System data from any modification and unauthorized deletion [FAU_STG.1, IDS_STG.1]. The functions made available to users for management of the TOE are limited [FMT_SMF.1].
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows. The TOE must prevent unauthorized modifications and deletions and the loss of audit data in the event the audit trail is full [FAU_STG.2, FAU_STG.4]. The System must prevent the loss of audit data in the event the audit trail is full [IDS_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion [IDS_STG.1].
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The System is required to protect the audit trail and System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion [FAU_STG.2, IDS_STG.1].
O.RESPON	The TOE must respond appropriately to analytical conclusions. The TOE is required to respond as configured in the event a vulnerability is detected [IDS_RCT.1].

9.2.2 Security Assurance Requirements Rationale

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 augmented by ALC_FLR.2 from part 3 of the Common Criteria.