ManageEngine
DataSecurity Plus

Architecture

About DataSecurity Plus

ManageEngine DataSecurity Plus is a web-based, real-time data visibility and security platform. It comprises of five modules:

- **File Audit**

  The File Audit module tracks file modifications and movement across file servers, failover clusters, and workstations, triggers real-time alerts in the event of suspicious or critical file activities, and executes scripted responses to halt the spread of ransomware.

- **File Analysis**

  With File Analysis, users can take back control over enterprise file storage by tracking storage growth, locating junk, stale, and non-business files, managing duplicate files, and identifying permission hygiene issues like broken permissions and files allowing open access.

- **Data Risk Assessment**

  The Data Risk Assessment module streamlines compliance with multiple regulatory mandates by locating files containing sensitive personal data (PII, PCI, and ePHI). It helps analyze the vulnerability and risk associated with those files, classify them accordingly, and thereby enable the secure usage of critical files.

- **Data Leak Prevention (DLP)**

  The software deploys a lightweight agent in every monitored file server, failover cluster, and workgroup server. The agent uses a Windows minifilter driver to audit file activities, and a Windows API to analyze file properties.

- **Cloud Protection**

  With the Cloud Protection module, users can track enterprise web traffic, analyze the use of shadow applications, view web reputations, and enforce policies to safeguard employees against inappropriate or malicious web content.

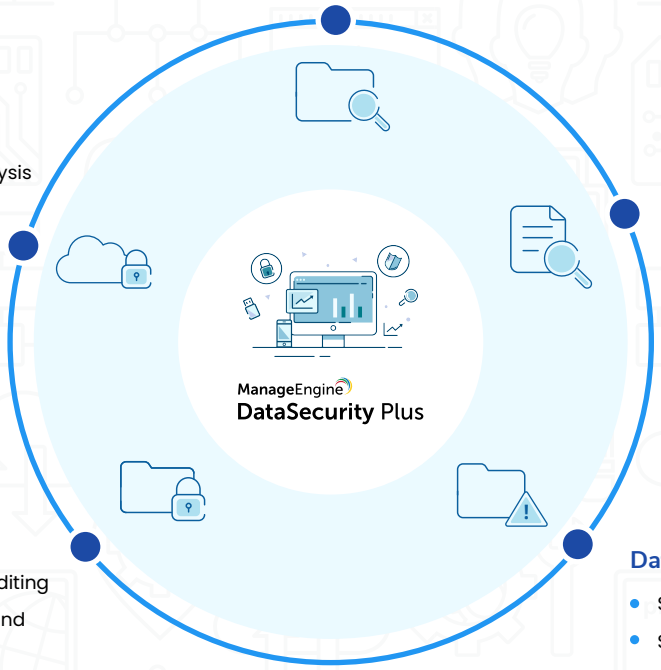
Architecture of the data visibility and security platform

File Audit

- Real-time file auditing and FIM
- Ransomware detection and response
- Compliance auditing and reporting

Cloud Protection

- Cloud app usage tracking
- Shadow IT discovery and analysis
- Application whitelisting and blacklisting



File Analysis

- Disk usage and permission analysis
- Permission vulnerability detection
- Junk file detection and deduplication

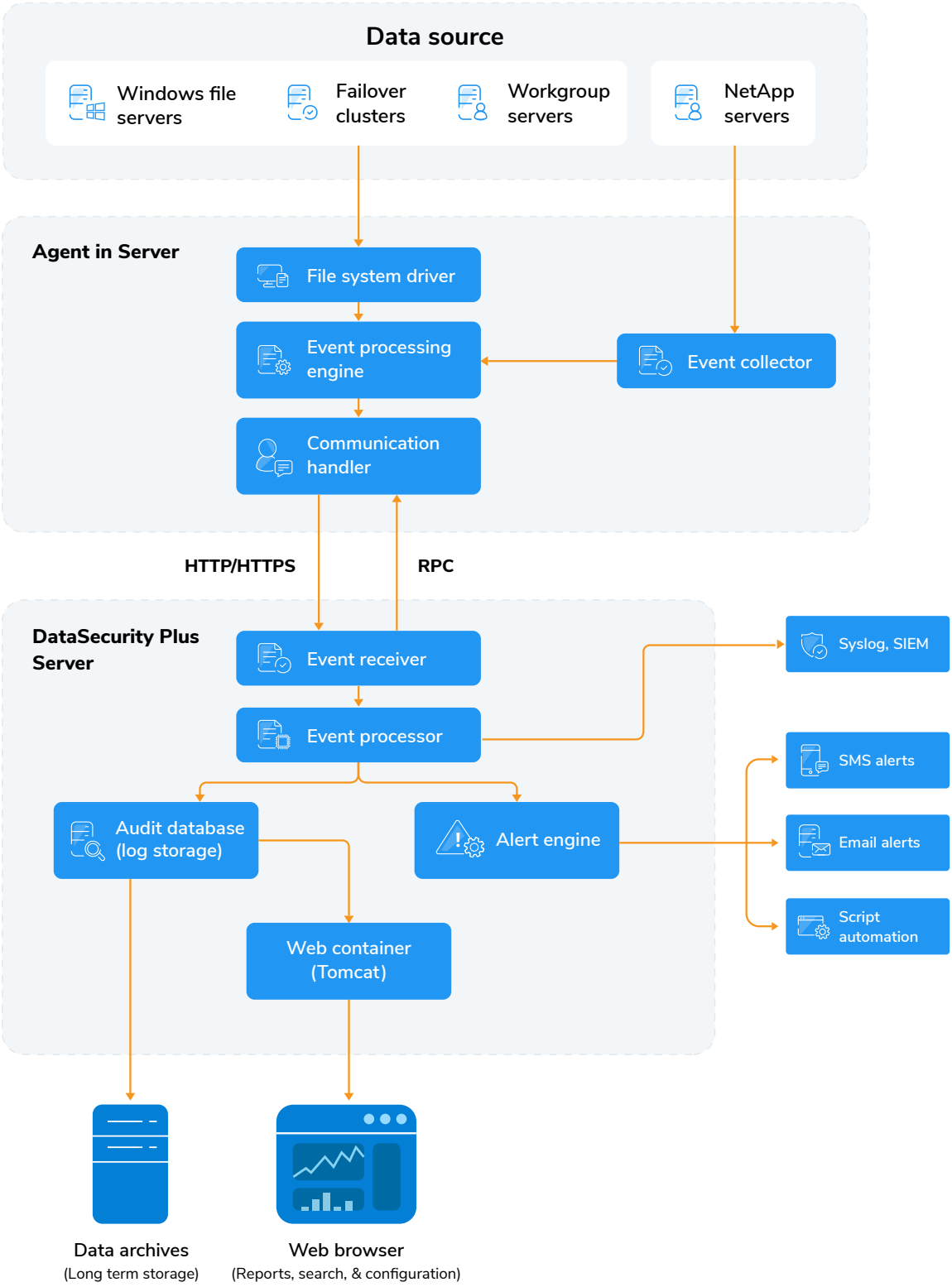
Data Leak Prevention

- Workstation and USB file auditing
- Data exfiltration detection and disruption
- Built-in DLP policies and strategies

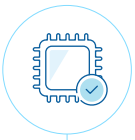
Data Risk Assessment

- Sensitive data discovery
- Security analysis of sensitive files
- Dynamic risk scoring

File Audit module



Components of the File Audit module:



Event Processor

All events that are fetched from the network are processed here before they are stored in the database or a corresponding alert is triggered. It filters unneeded logs—as configured by the administrator—and normalizes raw logs to standard formats.

Alert Engine

Based on configured rules, the Alert Engine automates passive responses such as sending email notifications and executing batch files.

Audit database

DataSecurity Plus is bundled with a PostgreSQL database that stores both raw and normalized event information from configured data sources.

DataSecurity Plus agent

The software deploys a lightweight agent in every monitored file server, failover cluster, and workgroup server. The agent uses a Windows minifilter driver to audit file activities, and Windows API to analyze file properties. For NetApp, the agent receives file events from the NetApp server and forwards them to DataSecurity Plus.

External components

Console

DataSecurity Plus' web interface can be accessed via a browser (Mozilla Firefox, Google Chrome (recommended), and Microsoft Edge), and connects to the web server component of Tomcat which listens on port number 8800 by default.

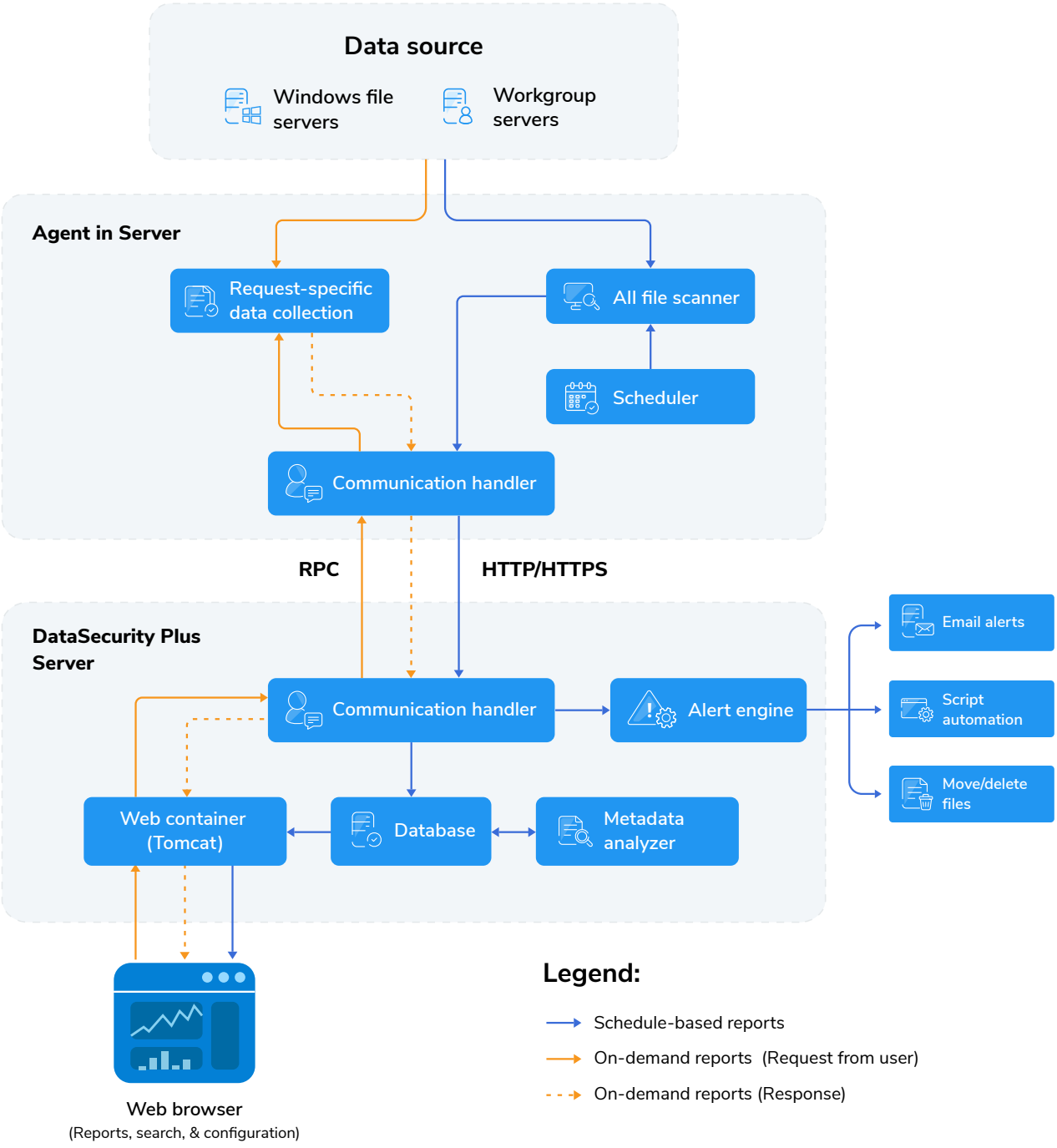
SIEM forwarding

DataSecurity Plus allows you to forward all file server audit data to your syslog server or Splunk for further analysis.

Email alerting

A Simple Mail Transfer Protocol (SMTP) server configuration is used for sending alert emails to recipients.

File Analysis module



The File Analysis module offers two types of reports:

Schedule-based File Analysis reports

The File Analysis module collects the data for these reports by running periodic metadata, security, and disk space scans at time intervals specified by the user.

On-demand File Analysis reports

The data for these reports is collected from the file server upon request, according to the inputs provided by the user.

Components of the File Analysis module:

Alert engine

Based on configured rules, the alert engine automates passive responses such as sending email notifications, executing batch files, deleting files, or moving them to a specified location.

Database

DataSecurity Plus is bundled with a PostgreSQL database that stores both raw and normalized event information from configured data sources.

Metadata analyzer

DataSecurity Plus's File Analysis module uses a metadata analyzer to detect instances of permission inconsistencies, permission hygiene issues, unused files, duplicate files, and more.

External components

Console

DataSecurity Plus' web interface can be accessed via a browser (Mozilla Firefox, Google Chrome (recommended), and Microsoft Edge), and connects to the web server component of Tomcat which listens on port number 8800 by default.

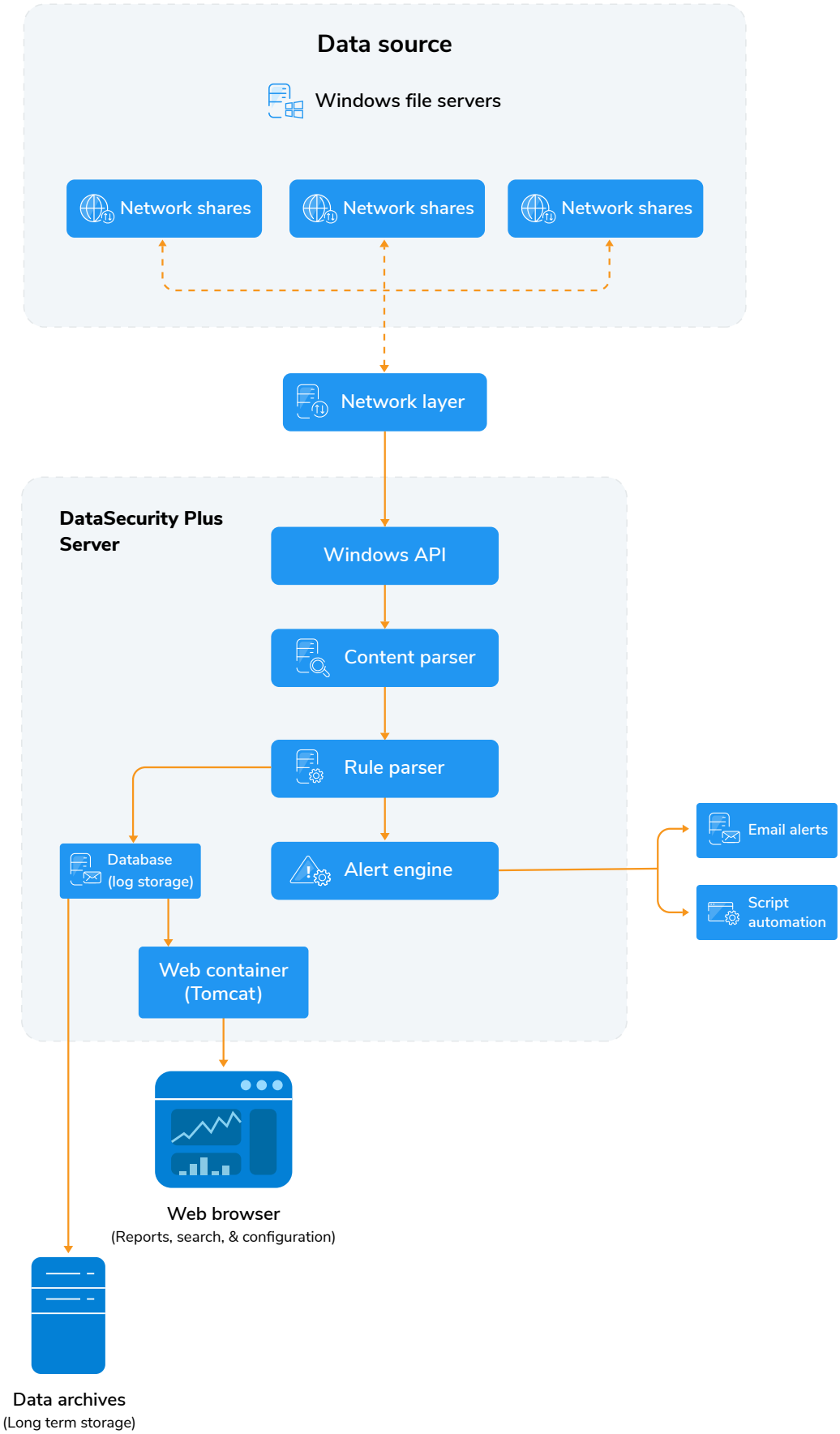
Security incident and event management (SIEM) forwarding

DataSecurity Plus allows you to forward all file server audit data to your syslog server or Splunk for further analysis.

Email alerting

A Simple Mail Transfer Protocol (SMTP) server configuration is used for sending alert emails to recipients.

Data Risk Assessment module



Components of the Data Risk Assessment module:

Content parser

The content parser extracts and processes content from the files being analyzed by the Data Risk Assessment module.

Rule parser

The rule parser compares the processed data against data discovery rules and policies to find data strings that match the regular expressions and keyword phrases in those rules, and execute the actions defined in the policies.

Alert engine

Based on configured rules, the alert engine automates passive responses such as sending email notifications and executing batch files.

Database

DataSecurity Plus is bundled with a PostgresQL database that stores sensitive and business-critical data discovered in configured data sources.

External components

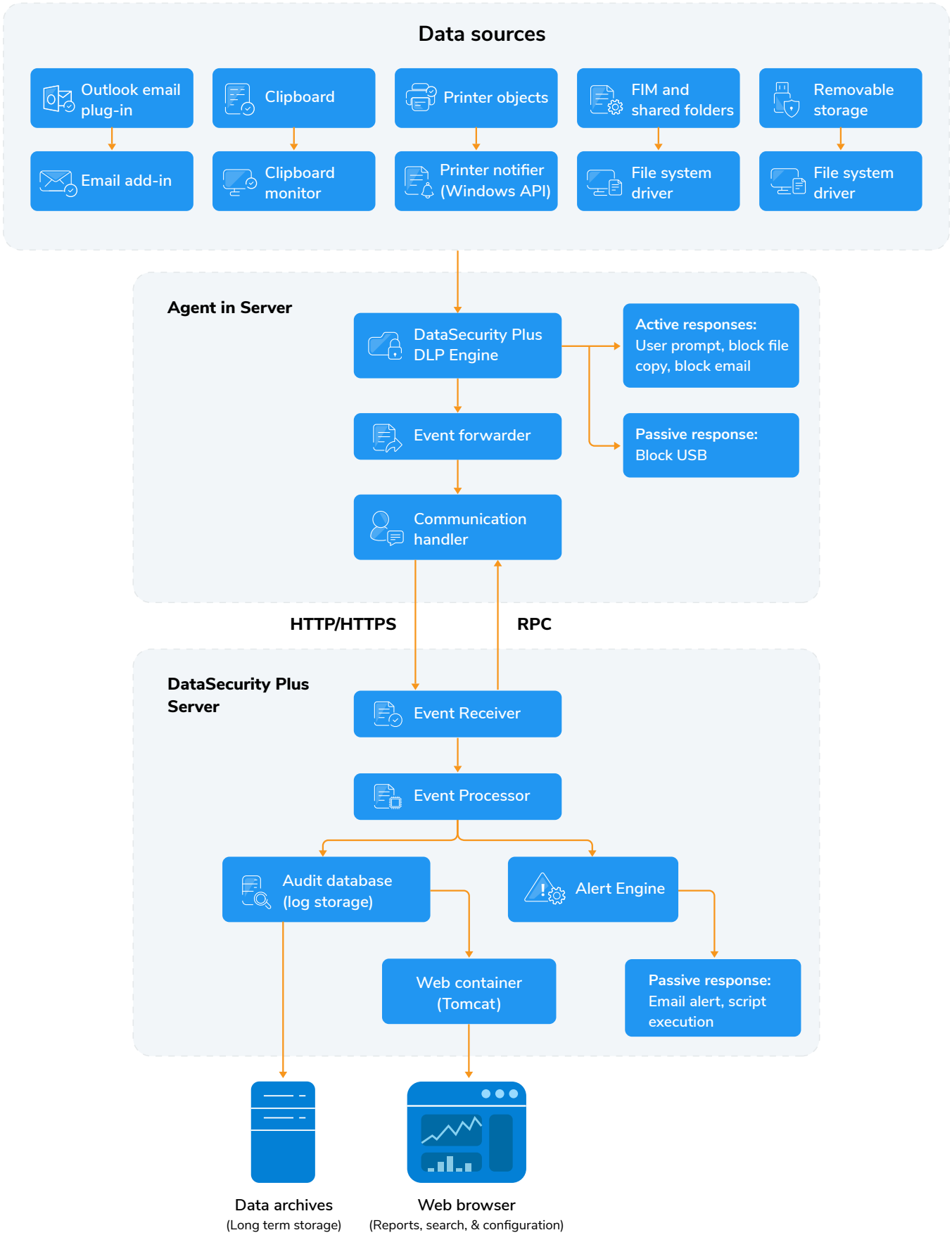
Console

DataSecurity Plus' web interface can be accessed via a browser (Mozilla Firefox, Google Chrome (recommended), and Microsoft Edge), and connects to the web server component of Tomcat which listens on port number 8800 by default.

Email alerting

An SMTP server configuration is used for sending alert emails to recipients.

Data Leak Prevention module



Components of the Data Leak Prevention module:

Alert Engine

Based on configured rules, the Alert Engine automates active responses such as displaying user prompts and blocking USB devices, as well as passive responses such as sending email notifications, executing batch files, deleting files, or moving them to a specified location.

Audit database

DataSecurity Plus is bundled with a PostgreSQL database that stores both raw and normalized event information from configured data sources.

DataSecurity Plus agent

The software deploys a lightweight agent in every monitored workstation. The agent uses a Windows minifilter driver to audit file activities, and Windows API to analyze file properties. It also allows end users to manually classify files in workstations.

DataSecurity Plus DLP Engine

The DLP Engine processes all incoming data from configured data sources, and compares it with a repository of both built-in and user-defined DLP policies.

External components

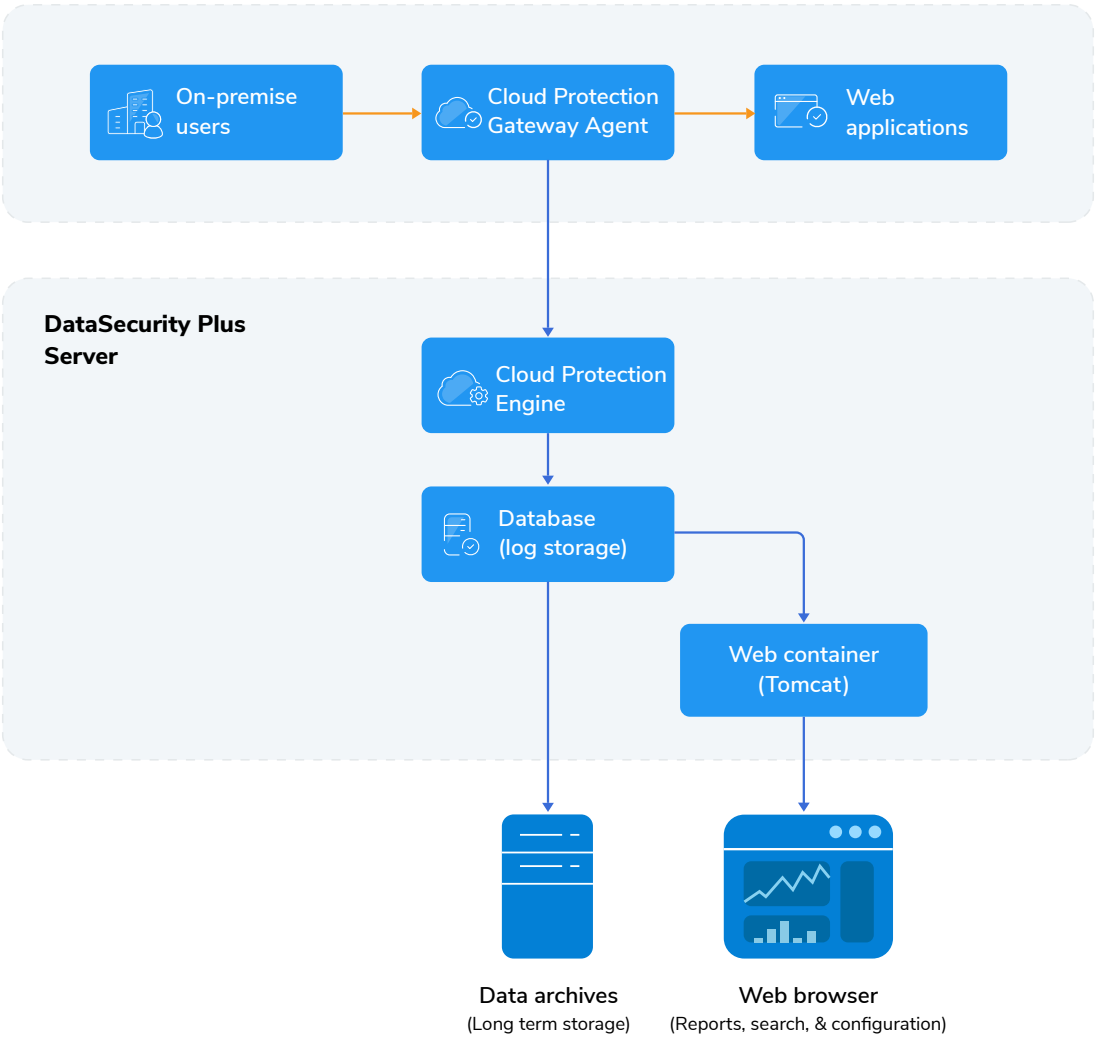
Console

DataSecurity Plus' web interface can be accessed via a browser (Mozilla Firefox, Google Chrome (recommended), and Microsoft Edge), and connects to the web server component of Tomcat which listens on port number 8800 by default.

Email alerting

An SMTP server configuration is used for sending alert emails to recipients.

Cloud Protection module



Components of the Cloud Protection module:

Cloud Protection Gateway Agent

The Cloud Protection Gateway Agent acts as a proxy between users and cloud applications. It monitors access requests, helps admins enforce organizational policies over cloud application usage by employees, and forwards audit data to the Cloud Protection Engine.

Cloud Protection Engine

The Cloud Protection Engine manages gateway servers, syncs configurations between the console and the gateway agent, processes users' web usage and activity logs, and provides a snapshot of enterprise cloud application use.

Database

DataSecurity Plus is bundled with a PostgreSQL database that stores both raw and normalized event information from configured gateway servers.

External components

Console

DataSecurity Plus' web interface can be accessed via a browser (Mozilla Firefox, Google Chrome (recommended), and Microsoft Edge), and connects to the web server component of Tomcat which listens on port number 8800 by default.

DataSecurity Plus

ManageEngine DataSecurity Plus is a unified data visibility and security platform. It audits file changes in real time, triggers instant responses to critical events, shuts down ransomware intrusions, and helps organizations comply with numerous IT regulations. It analyzes file storage and security permissions, deletes junk files, and detects security vulnerabilities. Users can assess the risks associated with sensitive data storage by locating and classifying files containing personally identifiable information (PII), payment card information (PCI), and electronic protected health information (ePHI). It also prevents data leaks via USBs, email, printers, and web applications; monitors file integrity; and audits cloud application usage. Together, these capabilities ensure the all-round protection of data at rest, data in use, and data in motion.

To explore these features and see DataSecurity Plus in action, check out the online demo.
To learn more about DataSecurity Plus, visit www.datasecurityplus.com.

Download free trial $ Get a quote

Explore DataSecurity Plus' capabilities

File server auditing

Audit and report on file accesses and modifications, with real-time alerts and automated responses for critical file activities.

Learn more

File analysis

Analyze file security and storage, manage junk files, optimize disk space usage, and identify permission vulnerabilities.

Learn more

Data risk assessment

Discover and classify files containing sensitive data such as PII, PCI, and ePHI by combining content inspection and contextual analysis.

Learn more

Data leak prevention

Detect and disrupt data leaks via USBs, email, web applications, and printers; monitor endpoint file activity; and more.

Learn more

Cloud protection

Track enterprise web traffic and enforce policies to block the use of inappropriate, risky, or malicious web applications.

Learn more

Our Products

AD360 | Log360 | ADAudit Plus | EventLog Analyzer

Exchange Reporter Plus | SharePoint Manager Plus