DATASHEET

WATCHGUARD SIEMFEEDER

Monitor, detect, and alert for security events occurring on your network

Security Information and Event Management: Overview

System Information and Event Management (SIEM) solutions have become a necessity to manage the security of the great majority of modern enterprise infrastructures. Their capabilities to collect and correlate the status of IT systems allow companies to turn the ever-increasing volume of events into helpful information for decision making.

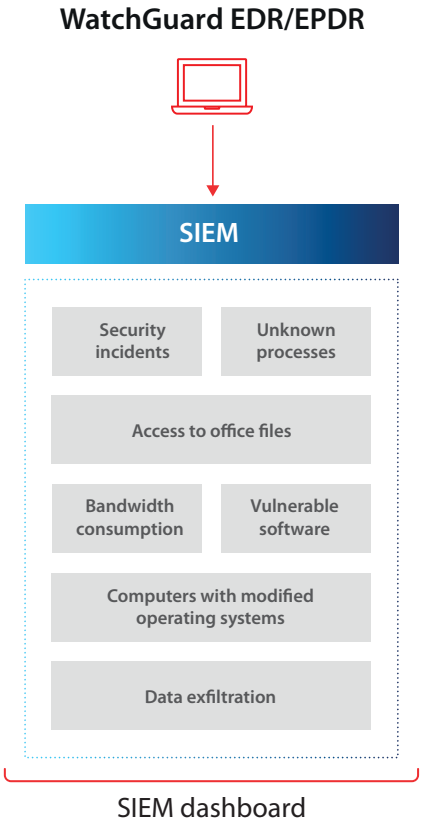
Integrating a new source of critical information into your security intelligence can solve many cybersecurity challenges and free up time for security professionals to identify and protect against state-of-the-art cyberattacks within massive events logged, sophisticated threats, and complex infrastructures.

Comprehensive Visibility of Security Events from Your SIEM Console

As a security professional, you need to have great visibility into the processes running on your workstations and servers. WatchGuard SIEMFeeder centralizes the events received from all your endpoints in your SIEM tool, helping you monitor security incidents and anticipate the problems caused by advanced threats on your corporate networks.

Main challenges faced by security administrators:

- **Anticipating potential security problems by finding run programs that have not yet been classified as goodware or malware and getting information about how they reached computers.**
- **Gaining visibility into IOA (indicators of attack) and detecting suspicious activity, such as Windows registry modifications or driver installations.**
- **Monitoring the execution of legitimate software often exploited by attackers that go unnoticed on your network, such as scripting or remote access tools.**
- **Operational efficiency of IT infrastructures:**
  1. **Monitoring inbound and outbound communications to avoid unwanted connections**
  2. **Reducing bandwidth consumption**
  3. **Designing policies for preventing massive download of unproductive content**
- **Detecting data exfiltration incidents, identifying which processes and users are accessing files with sensitive information.**



Benefits:

✓ **Comprehensive visibility of everything that runs on your devices**

Monitor and manage security. Detect anomalies continuously in each customer's execution environment.

✓ **Centralized configuration**

Configure WatchGuard SIEMFeeder settings for all your endpoints simultaneously using the centralized management console (WatchGuard Cloud).

✓ **Simple to install, secure, and easily scalable**

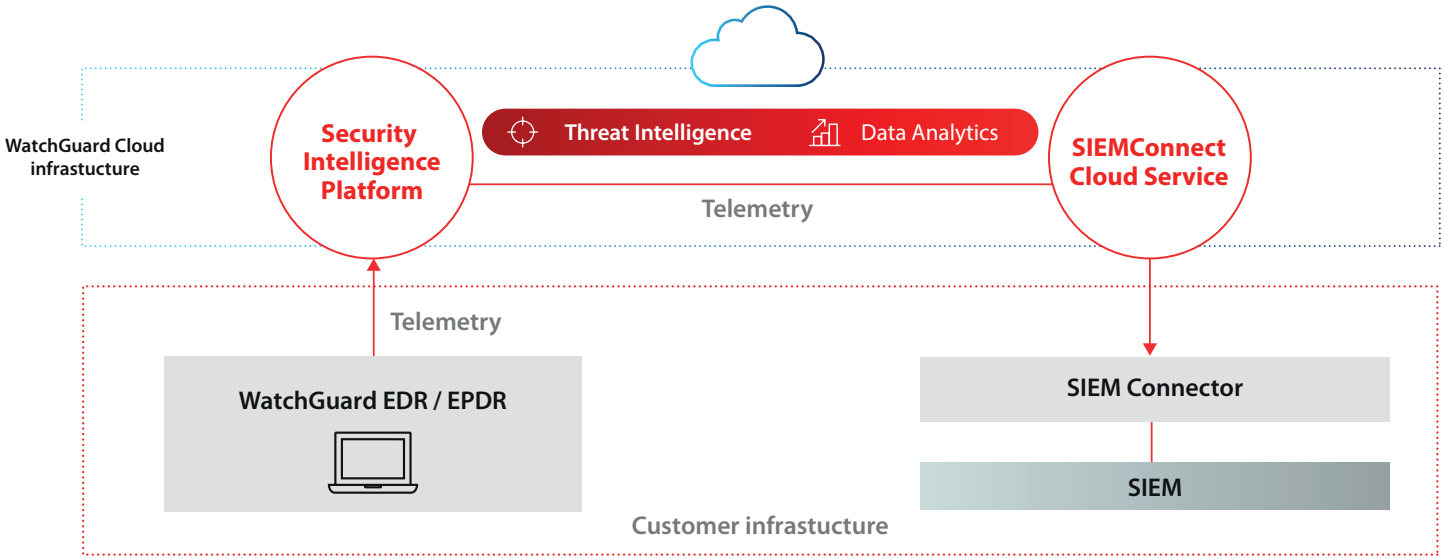
Configure the telemetry download service only once and add new endpoints without having to deploy or install any additional components. Safe downloads through secure TLS (Transport Layer Security) connections from the WatchGuard Cloud.

✓ **Reduced SIEM storage costs**

Filter required events before they reach your infrastructure, minimizing storage costs.

✓ **Compatible with most SIEM solutions on the market**

Download telemetry in CEF or LEEF format, compatible with the leading SIEM solutions on the market such as QRadar, AlienVault, Splunk, Devo, etc., and natively with ArcSight.



Compatible with:

ALIEN VAULT · ArcSight An HP Company · QRadar · splunk> · elasticsearch · DEVO

Key Features:

- Centralized endpoint management through WatchGuard Cloud
- Easy to install and configure
- Event filtering prior to integration into the SIEM tool
- Configurable format: LEEF or CEF
- Safe event download through TLS connections

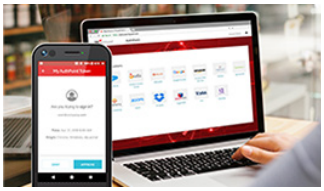
WatchGuard SIEMFeeder System Requirements and Supported Platforms

See https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Endpoint-Security/installation/install-requirements.html

This module is available with:
WatchGuard EPDR | WatchGuard EDR

THE WATCHGUARD PORTFOLIO

Network Security



Multi-Factor Authentication

Secure Cloud Wi-Fi

Endpoint Security