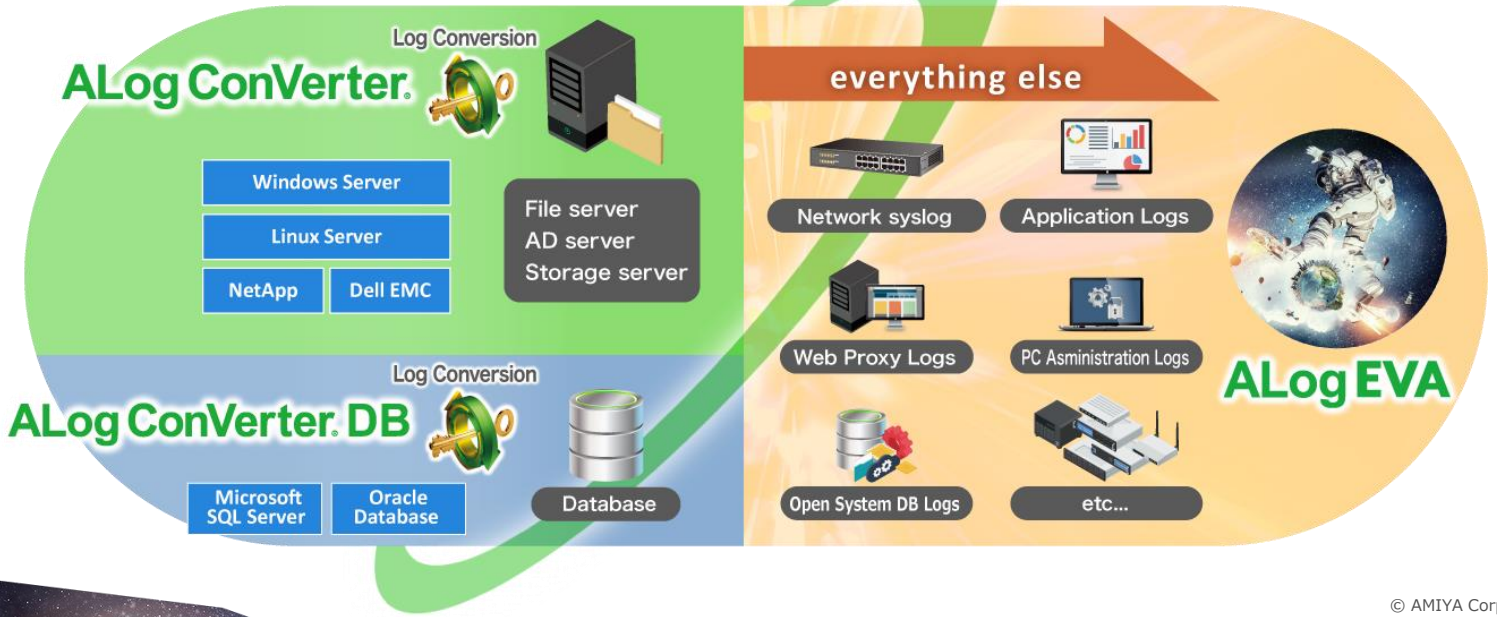
Document Ver. 7.4.0_3_En

Product Outline

ALog EVA

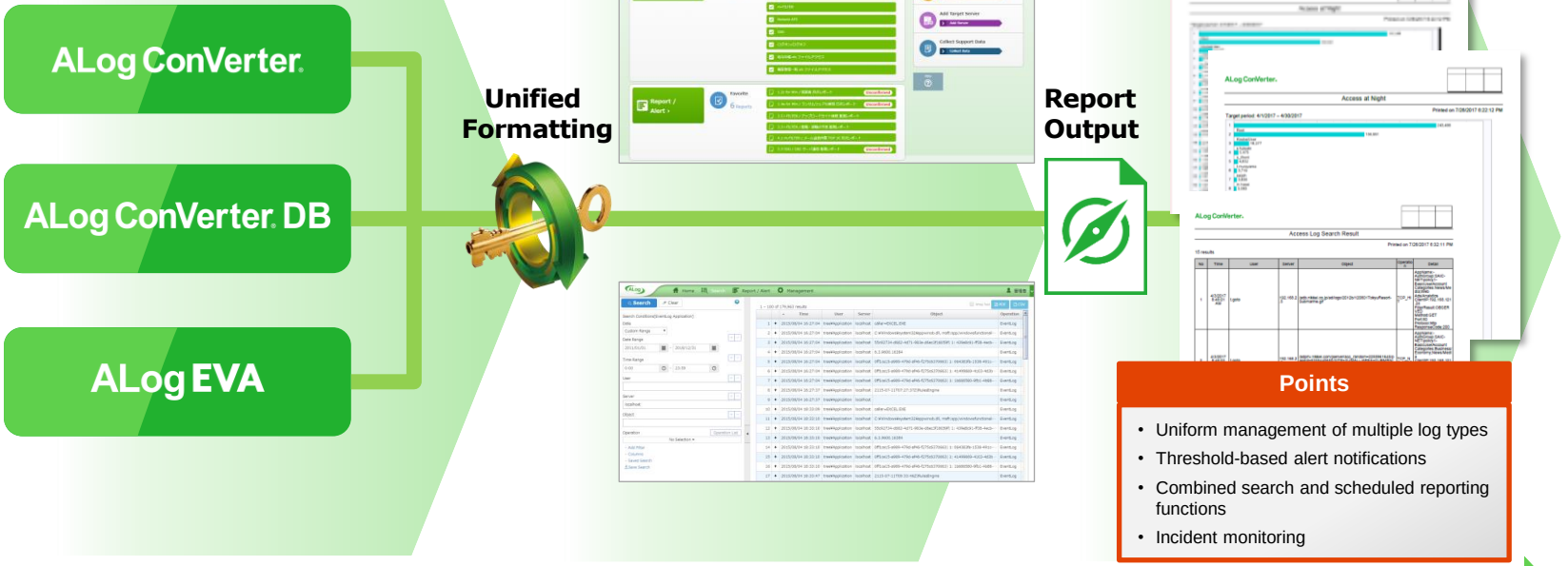
ALog EVA dramatically expands the scope of the ALog series.

This new product allows for integrated security management from all directions, **offering cyber attack detection**, **communication error investigation**, **post-incident data tracking**, and other data management from a variety of devices. ALog EVA also provides visualization of security risks, as well as monitoring and reporting.



All Unified Management

Manage log data using the ALog Series common interface.
The unified GUI performs search and reporting functions, allowing log management from multiple sources.



Points

- Uniform management of multiple log types
- Threshold-based alert notifications
- Combined search and scheduled reporting functions
- Incident monitoring

Downsides of Conventional Products

1 Complex Layouts and Settings

Complicated layouts and difficult-to-understand data mapping settings can lead to a laborious installation process...

2 Too Many Optional Tools

Search and reporting tools are only available in other programs or in add-on options...
Several installations are necessary before the product can actually be used.

3 Useless Log Data

The log data you painstakingly gather is difficult to decipher.
The sheer amount of log data makes it impossible to use during emergencies...

4 High Cost

Licensing fees far exceed expectations...
Moreover, difficult configuration leads to considerable consulting fees.

The ALog EVA Advantage

1 Simple Layout and Settings

Our experience gathering log data from a diverse range of devices has allowed us to provide a multitude of standard mapping templates.

ALog EVA features intuitive GUI and easy settings.

Clear visuals and ease of use

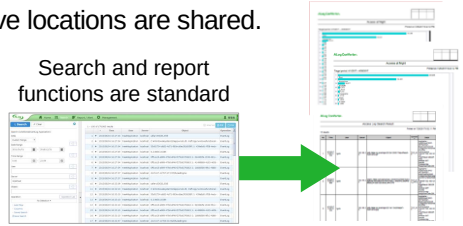
2 Options are Unnecessary

Search and report functions come standard.

The GUI is uniform across the series to ensure ease of administration across programs.

Save locations are shared.

Search and report functions are standard



3 Easy to Understand, Easy to Use

Saves data simply and efficiently.

Our years of expertise have gone into converting stored data into useful logs.

From storage only…

...to useful data.

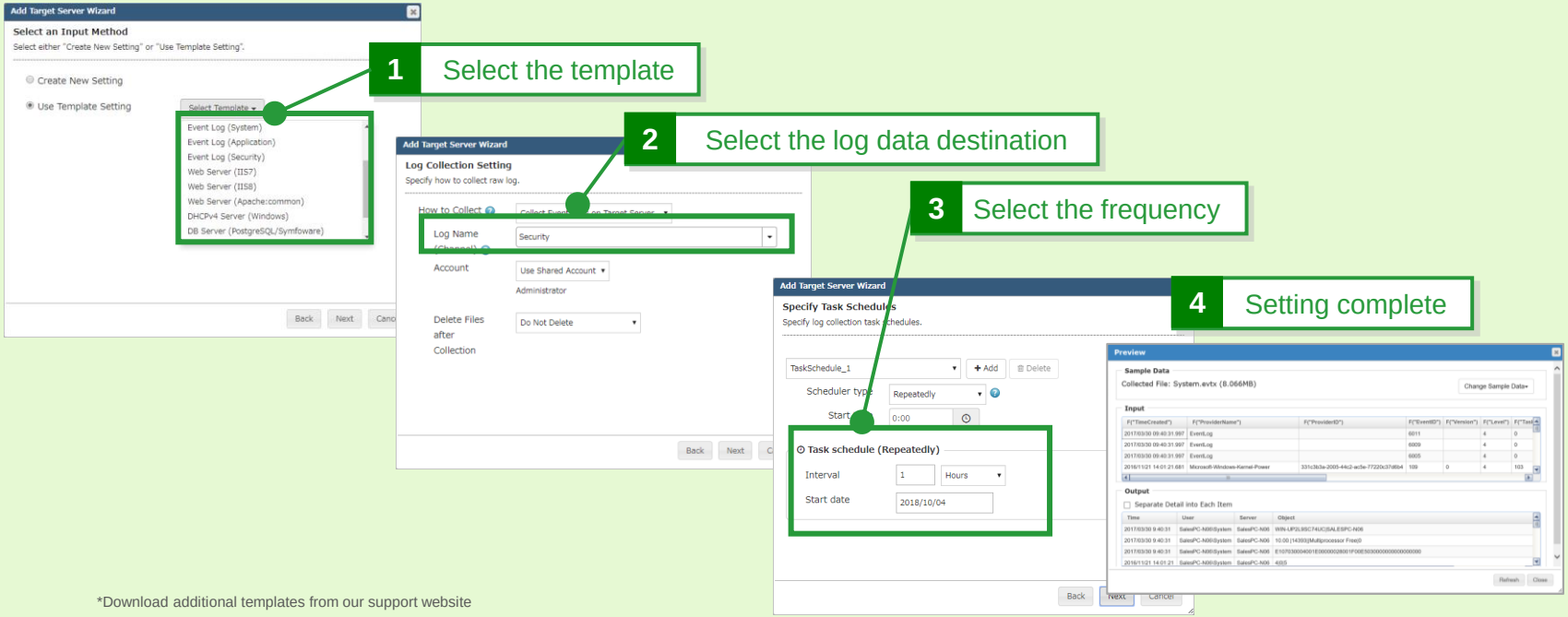
4 Cost Performance

Log recording and data storage shouldn't be so expensive!

We offer long-term use of our programs at prices that are as affordable as possible.

Speedy Log Mapping

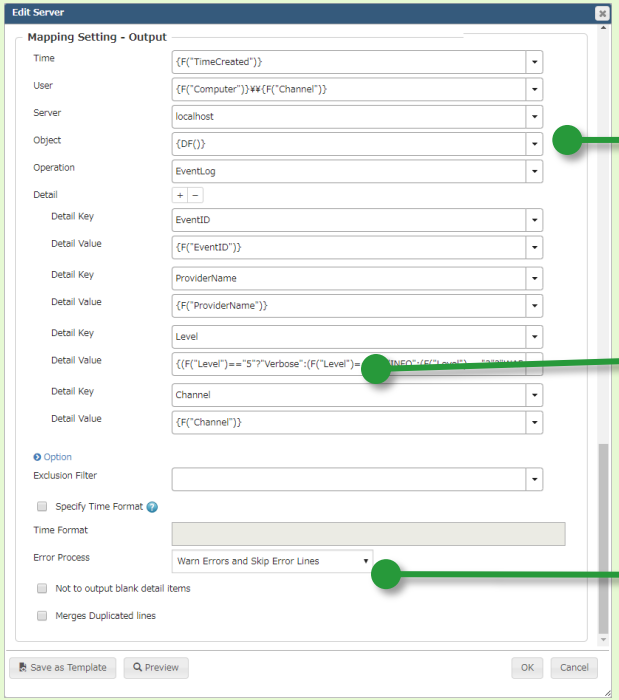
Specialized templates for common log data are already provided with the software.
Simply select the one you want to use.



*Download additional templates from our support website

Flexible Scalability

You can set up the screen with using simple, easy GUI when you are not using template.
There is no need to type a complex definition of scripting languages in order to set up mapping.



Mapping Definition

Besides selecting a prearranged function from pull-down menu, the function of .NET Framework is applicable as well.
You can output from a combination of multiple variables or regular expressions.

Detailed key

You can tag output variable. You can expand search results if you tag application name, port number, event ID, and others beforehand.

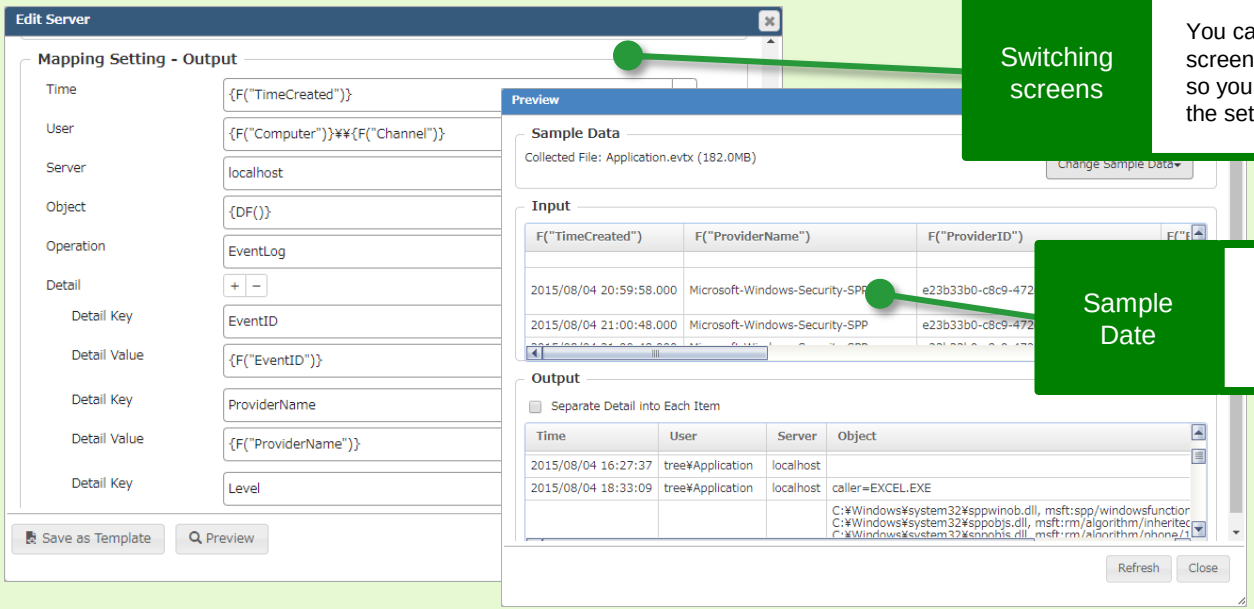
Exclusion Filter

It is possible to set exclusion options like
Ex)

- Exclude the nth line from the top
- Exclude particular lines
- Exclude particular keywords

Smooth Setting with Preview Function

Preview function of mapping setting allows you to adjust setting while viewing the preview screen.
There is no need to go back and forth between screens.



Switching screens

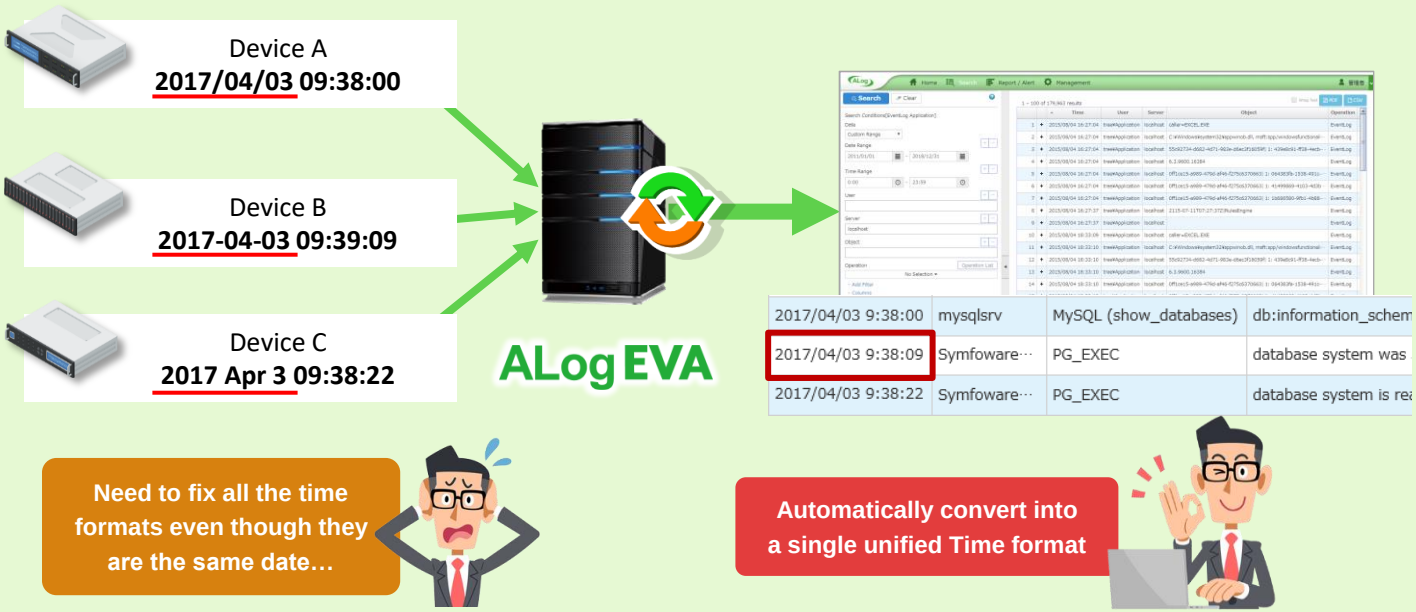
You can view both the mapping setting screen and preview screen at the same time, so you can see adjustments you made in the setting screen.

Sample Date

For sample data, you can specify arbitrary logs or collect data from actual working environment.

Automatic unification of time format

Unify various types of time formats into a single time format automatically.
There is no need to convert each definition, it is easy to collect logs from multiple products.



Automatically recognizable format
yyyy/MM/dd HH:mm:ss.FFFFFFF
yyyy/MM/dd H:mm:ss.FFFFFFF
yyyy-MM-dd HH:mm:ss.FFFFFFF
yyyy-MM-dd H:mm:ss.FFFFFFF
yyyy/MM/dd HH:mm:ss
yyyy/MM/dd H:mm:ss
yyyy-MM-dd HH:mm:ss
yyyy-MM-dd H:mm:ss
yyyyMMdd HHmmssFFFFFFF
yyyyMMdd HHmmss
MMM dd HH:mm:ss.FFFFFFF
MMM d HH:mm:ss.FFFFFFF
MMM dd HH:mm:ss
MMM d HH:mm:ss

ALog EVA Log ingestion List

※as of September 2018 Random order

◆Network System

Cisco ASA series
Cisco Catalyst series
Juniper SSG series
Juniper MAG series
PaloAlto Networks PA series
Blue Coat ProxySG series
Fortigate series
Infoblox DHCP
YAMAHA RTX series
IBM Flex System EN switch
Hitachi Load Balancer EL130
Aruba Networks Mobility Controllers
TrendMicro Deep Discovery Inspector
Soliton Systems NetAttest EPS series
SonicWall series

◆NAS/Cloud Storage/ General-purpose machine

Hitachi Virtual File Platform	(CIFS)
NetApp ONTAP	(NFS audit)
HPE 3PAR StoreServ	
Nutanix AFS	(Nutanix Files)
QNAP	
I-O DATA LAN DISK	
Amazon Web Services CloudTrail	
Box	
FOBAS Cloud Storage Cache	
IBM AS/400	

◆Servers

Apache HTTP Server	(Linux)
IBM HTTP Server	(Linux)
DHCP Server	(Windows)
DNS Server (debug log)	(Windows)
Microsoft Exchange Server	(Windows)
RADIUS Server	(Windows)
WebDAV	(Windows)
Squid common	(Linux proxy server)
Sendmail	(Linux mail server)
Postfix	(Linux mail server)
Samba	(Linux)

◆Application

SAP
NEC Explanner
PCA series
OBIC series
NISSEICOM GrowOne
Microsoft SharePoint (AvePoint)
Cybozu Office series
Cybozu Garoon series
Access Analyzer
Hitachi JP1
FUJITSU Systemwalker
Fuji xerox DocuShare
Fuji xerox ArcSuite

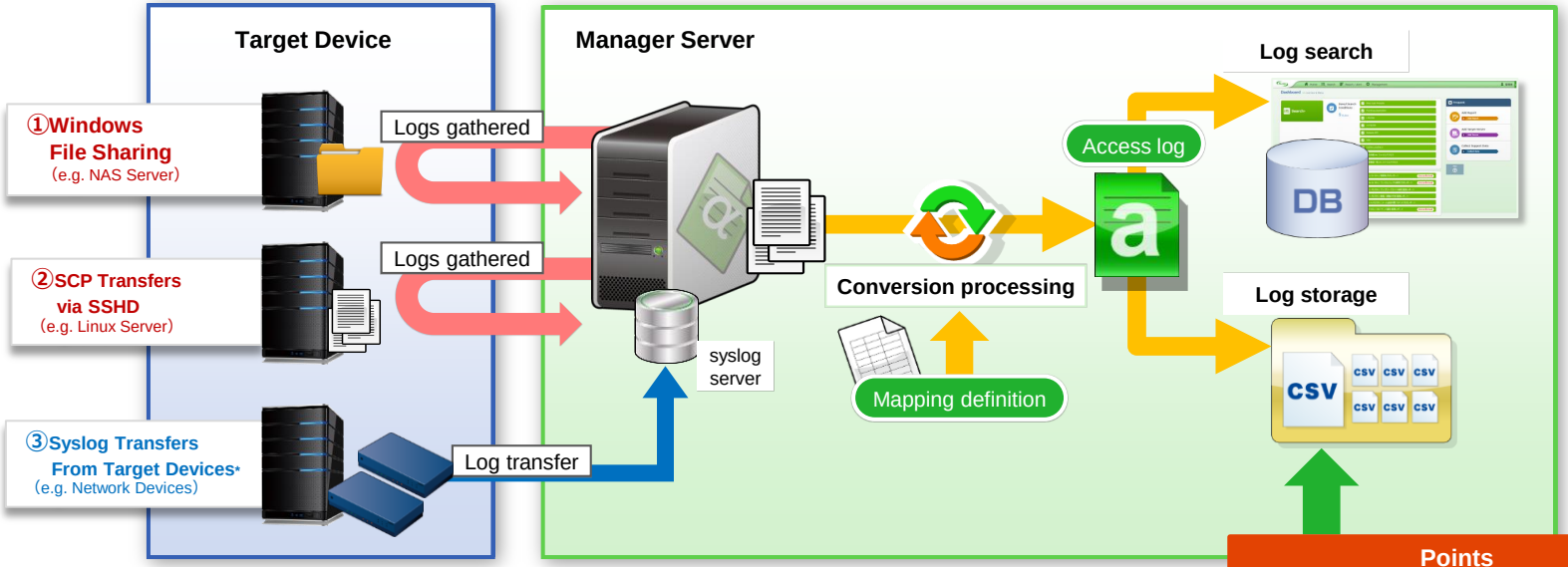
◆Security product

SKYSEA Client View
LanScope Cat
Soliton Systems SmartOn
DOS System Support best1 (SS1)
Quarity soft QND
Digital Arts i-FILTER
Digital Arts m-FILTER
TrendMicro Virus buster
TrendMicro InterScan Messaging Security
ALSI InterSafe ILP
ALSI InterSafe IRM
Symantec Messaging Gateway
Hitachi solutions Hibun
ZenmuTech ZENMU
Cisco cloud Web security
IIJ Secure Web Gateway Service
Pulse Secure series
Logstorage

◆Database

MySQL	(Linux)
PostgreSQL	(Linux)
FUJITSU Symfoware Server	(OPEN)
FUJITSU Symfoware Server	(NATIVE)
Hitachi HiRDB	
IBM DB2	

System Flow



*Logs are transferred from target devices to the ALog manager server, and then received on by the manager server side.
The syslog server (Kiwi Syslog Server, etc.) must be configured as a manager server.

Points

- File compression allows long-term storage
- Data encryption prevents tampering
- DB storage duration can be set to any period
- File output by device
  (Easy coordination with other systems)

Hard ware Requirements - Manager Server

ALog EVA

OS : Windows Server 2008 (x64) / 2008R2 / 2012 / 2012R2 / 2016

*32bit version OS is not supported
*Service pack of each OS(SP)is supported
*Each edition of（Standard / Enterprise / Datacenter）supported
*Virtualized environment (VMWare, Hyper-V, Citrix XenServer)supported.

CPU : Dual Core, or higher (Quad Core or above is recommended)

Memory : 8GB, or higher (16GB, or higher is recommended)

HDD : 500GBor higher disk space.

*There is a case that more disk space is required depending on the number of the target server and access log storing term.

Software : .NET Framework 4.6 or later version

Either of following web browser

- Internet Explorer 10 or later version
- Firefox version 40 or later version
- Google Chrome version 44 or later version

Obtainable log type

ALog EVA is available to obtain log data which is output with Windows Event Log, syslog and text file (with separated value such as csv).
Text file needs to be encoded with UTF-8, UTF16 or the other encoding which is supported by .NET Framework.

The following type of log is not available to obtain with ALog EVA.
- Fixed-length format
- binary file
- Encrypted file

It is also not available in case below.
- In case that the log volume exceeds 100GB per day

In case that syslog server is needed

Syslog server is needed aside ALog EVA when it is not available to share log data with Windows file sharing(CIFS).
*Verified Syslog server software :
Kiwi Syslog server (not free version)