Microsoft

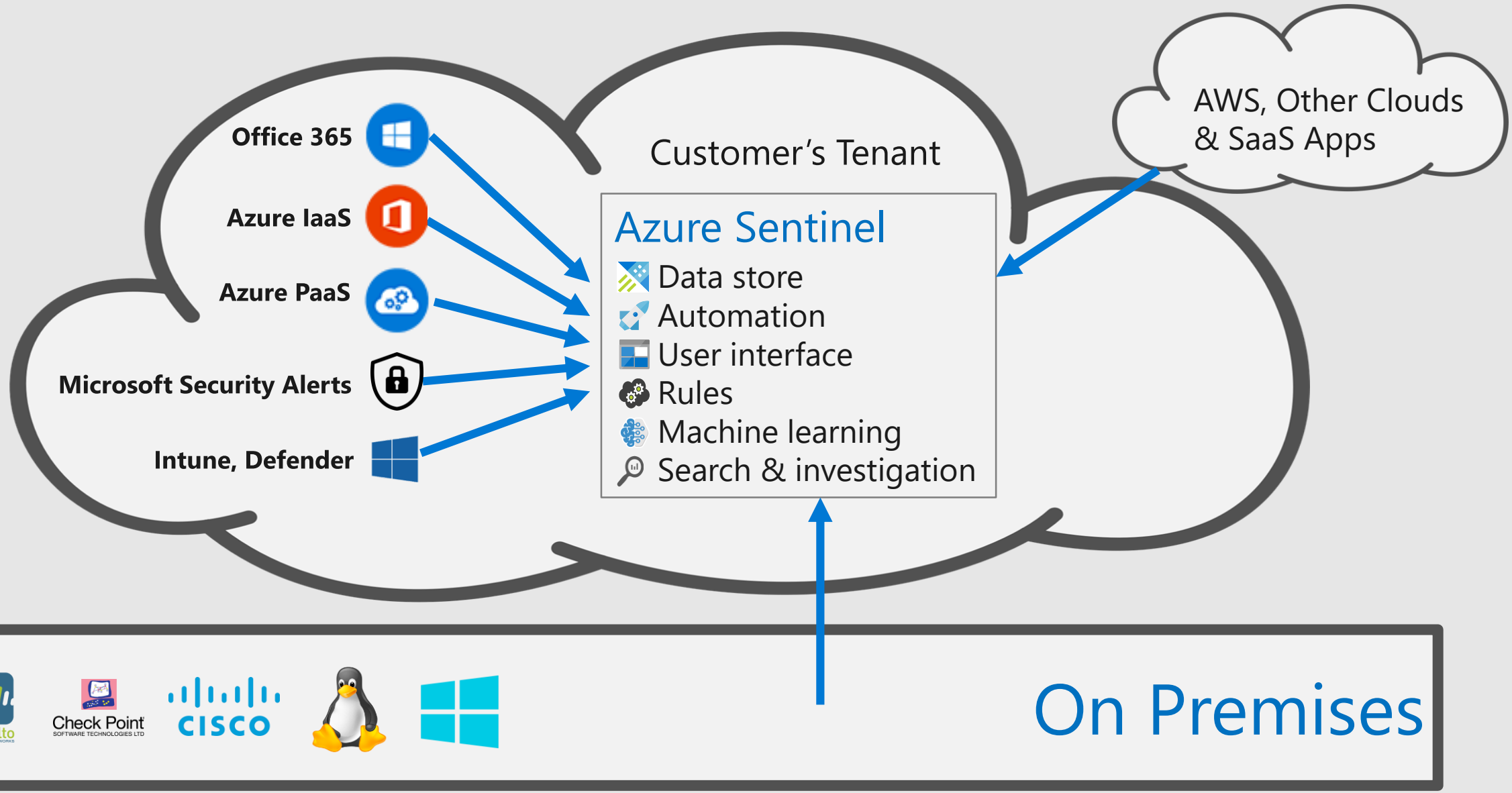
Azure Sentinel Level

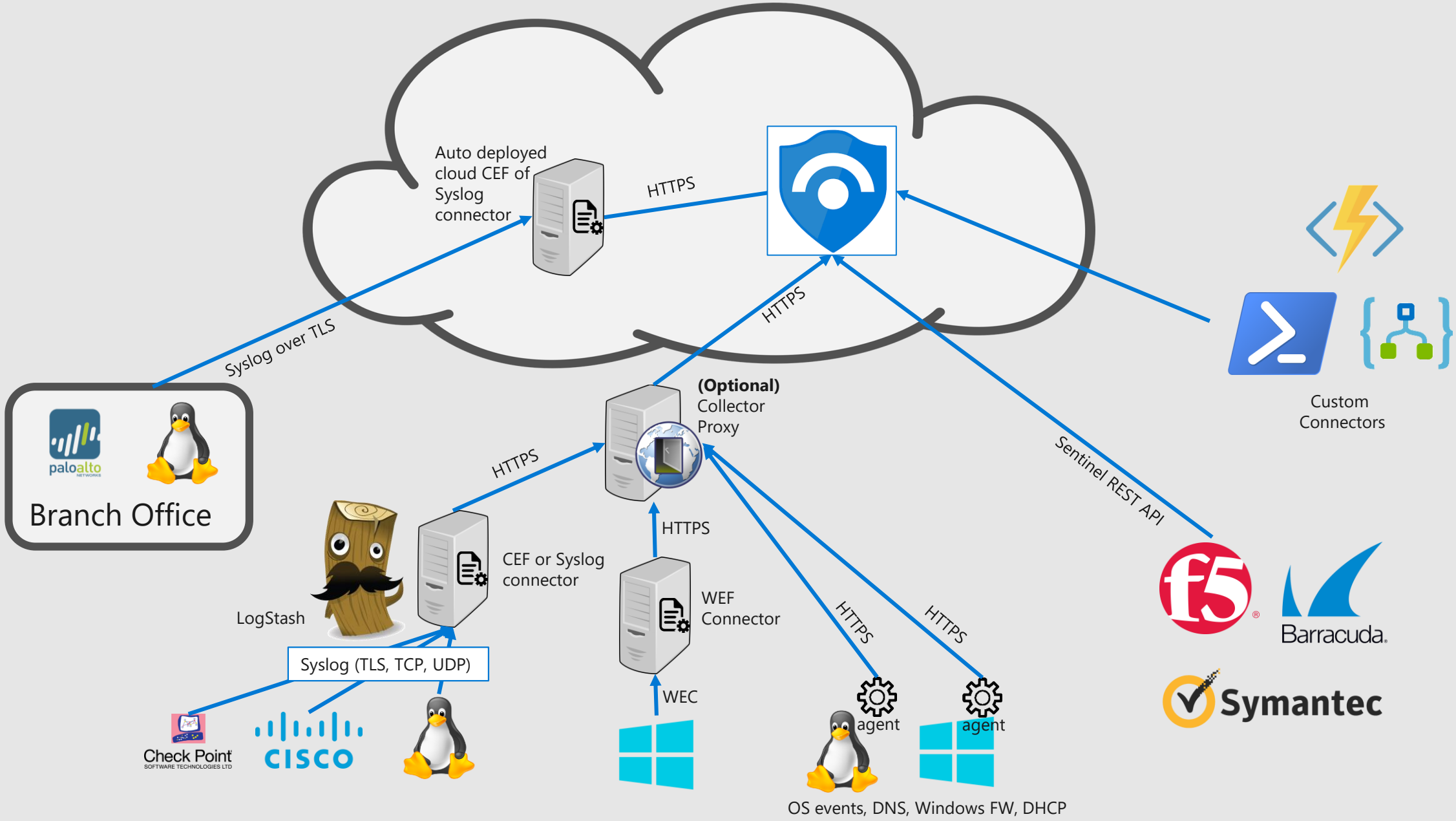
On Prem & IaaS collection Architecture

Agenda

1. Collection overview
2. The Log Analytics Agent (MMA)
3. CEF/Syslog collector
4. Parsing
5. WEF collector
6. Logstash
7. Custom connectors

Collect security data at cloud scale from any source

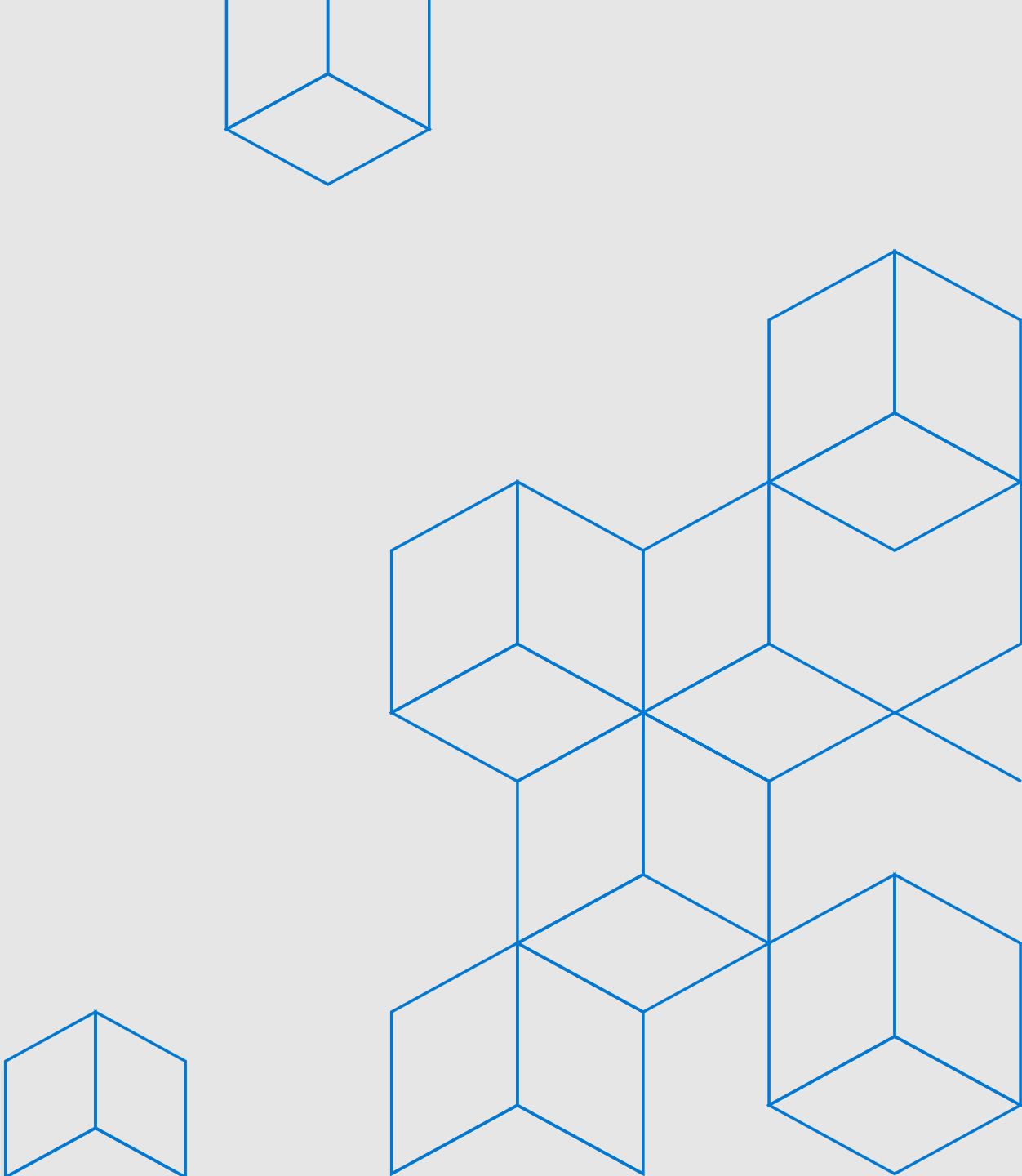



Auto deployed cloud CEF of Syslog connector
HTTPS
Syslog over TLS
HTTPS
Custom Connectors
paloalto
Branch Office
(Optional) Collector Proxy
HTTPS
Sentinel REST API
HTTPS
LogStash
CEF or Syslog connector
WEF Connector
HTTPS
HTTPS
HTTPS
Syslog (TLS, TCP, UDP)
WEC
agent
agent
Check Point
SOFTWARE TECHNOLOGIES LTD
CISCO
Barracuda
Symantec
OS events, DNS, Windows FW, DHCP

The full catalog

- The Syslog and CEF grand list
- Collecting logs from Microsoft Services & Apps
- The Agent: Collecting from on-prem and IaaS server
- Custom Connectors

The Log Analytics Agent



Log Analytics Agent*: collected events

Basics:

- Windows Events, including:
  - AD
  - Sysmon
  - Many others: SQL server for example
- Linux Syslog

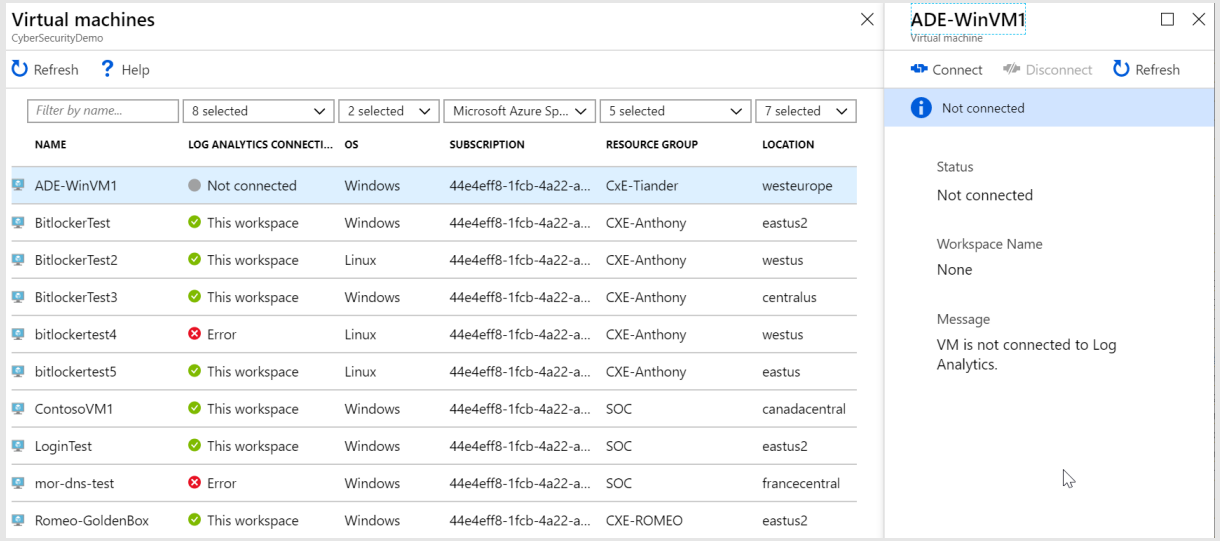
Extras:

- DNS events
- Windows Firewall events
- IIS events
- Files
- FluentD plug-ins

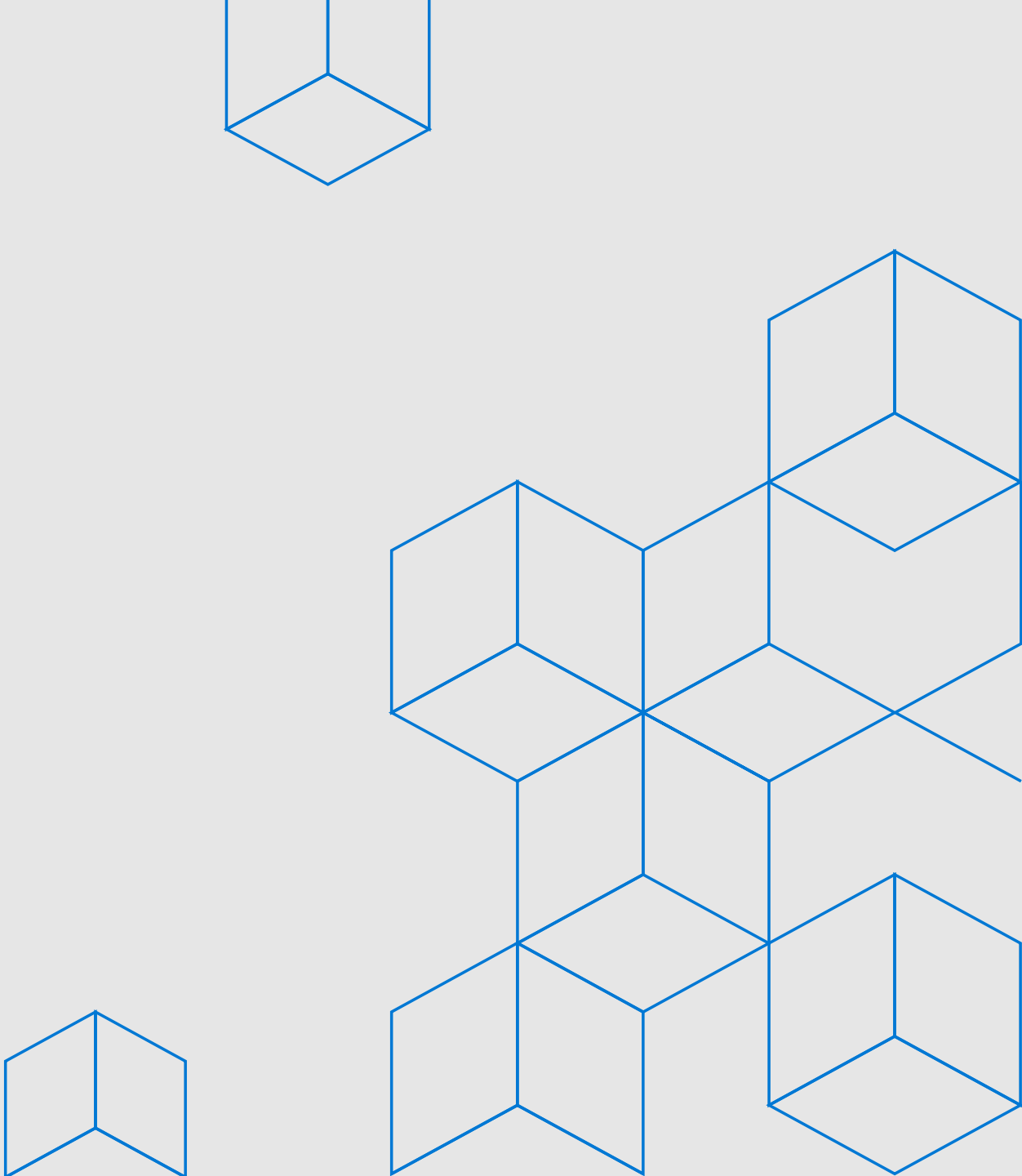
* Also known as the OMS Agent / Microsoft monitoring agent / MMA

Log Analytics Agent: Deployment

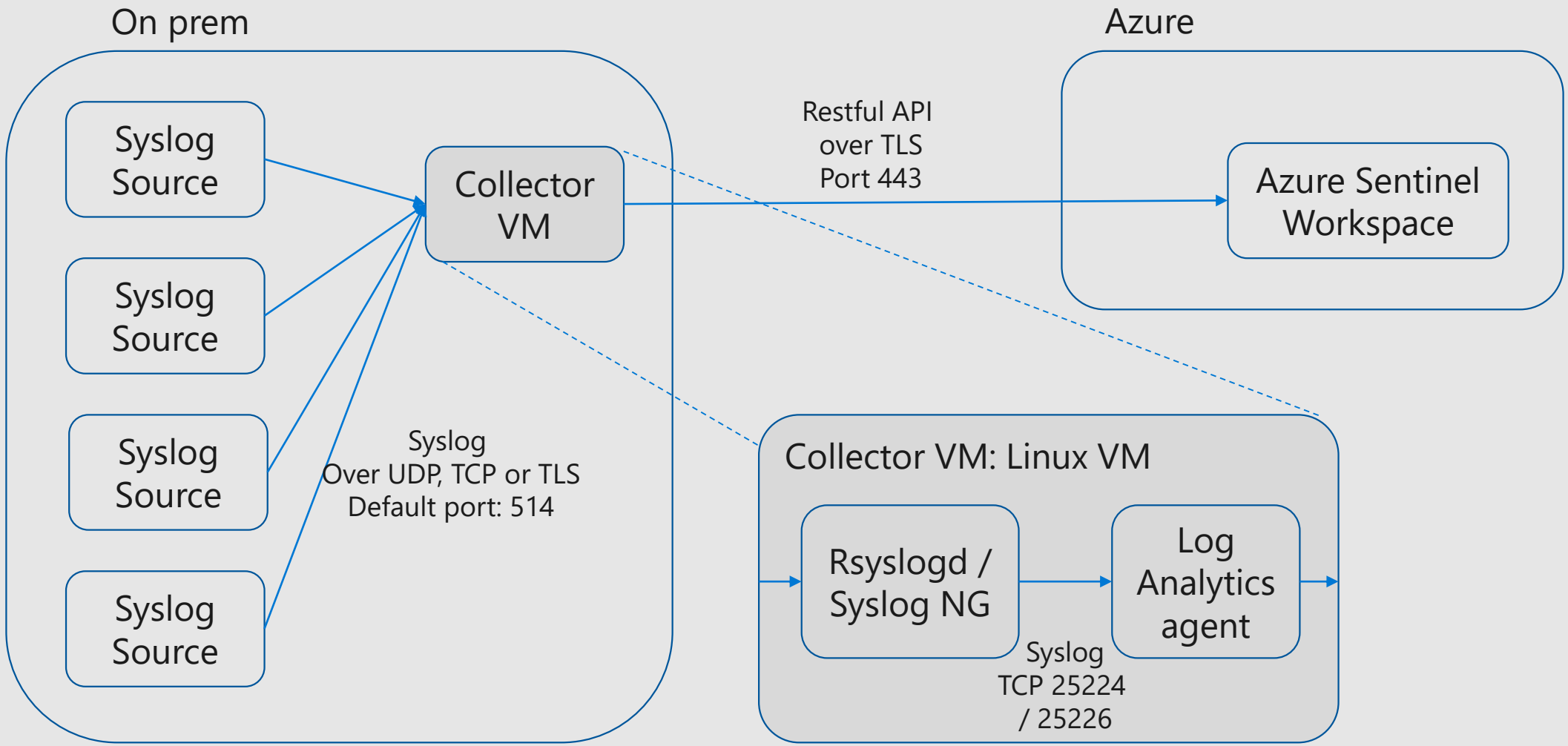
- Windows or Linux
- Automated install in Azure
- Central management
- Proxy support



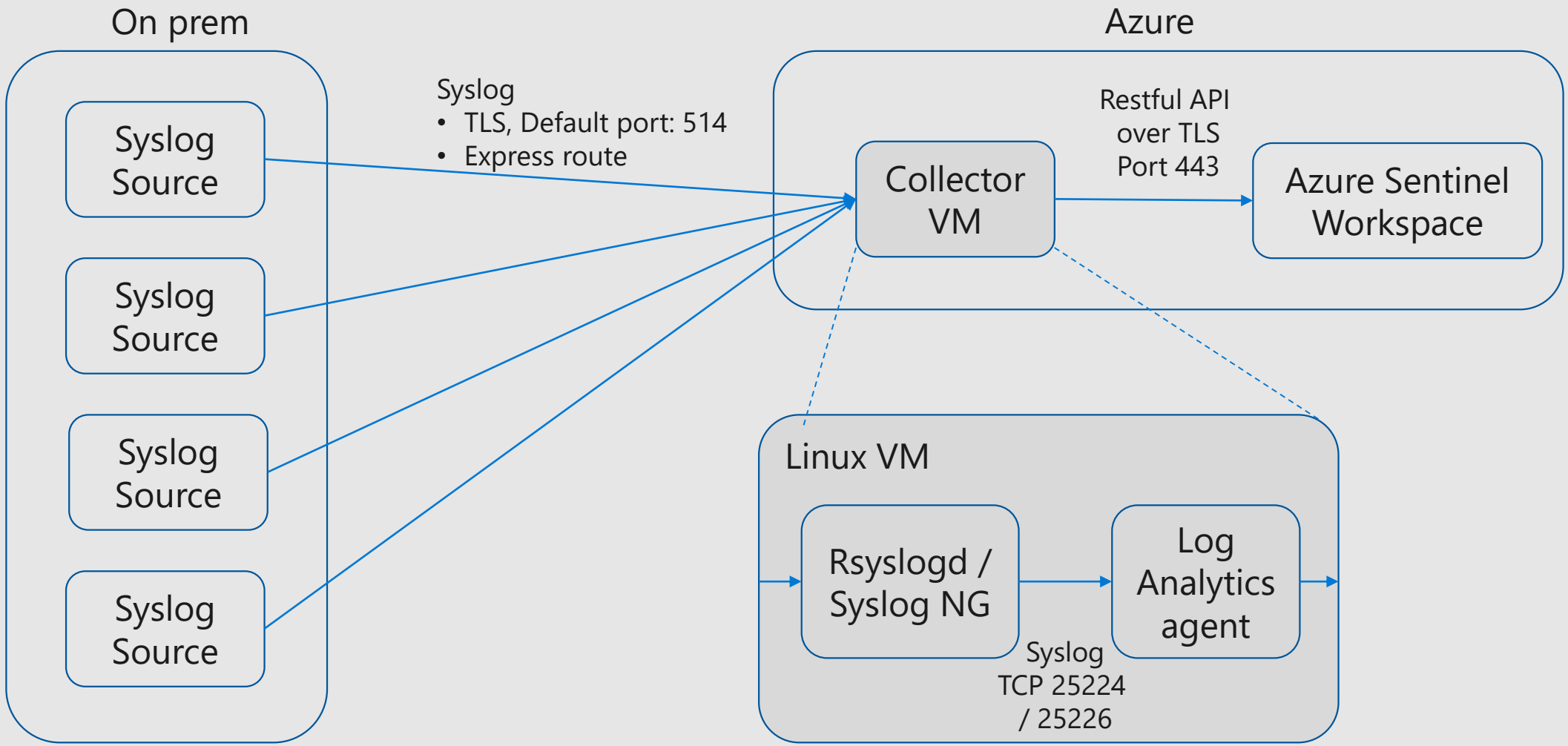
CEF and Syslog collection



CEF/Syslog On-prem collector



CEF/Syslog Azure based collector



Deploying a CEF/Syslog collector

Simple:

- Deploy a Linux VM of your liking
- Run a deployment script:
  - Installs the Log Analytics agent
  - Configured it
  - Configured your Syslog daemon
- Support multiple CEF/Syslog sources with a single collector.
- Make sure CEF is not using facilities configured for Syslog

Advanced, using direct daemon configuration:

- Filter events
- Use TLS

Scaling CEF / Syslog collection

A single collector:

- Scale to 20K EPS
- Supports many CEF or Syslog sources of various types

Clustering:

- Static distribution
- HAProxy:
  - Simple, free, failover
  - No UDP support
- Commercial load balancer

CEF vs. Syslog

- CEF is a structured format and schema over a Syslog transport
- CEF data is parsed. Syslog messages require query time parsing.
- If available, use CEF.

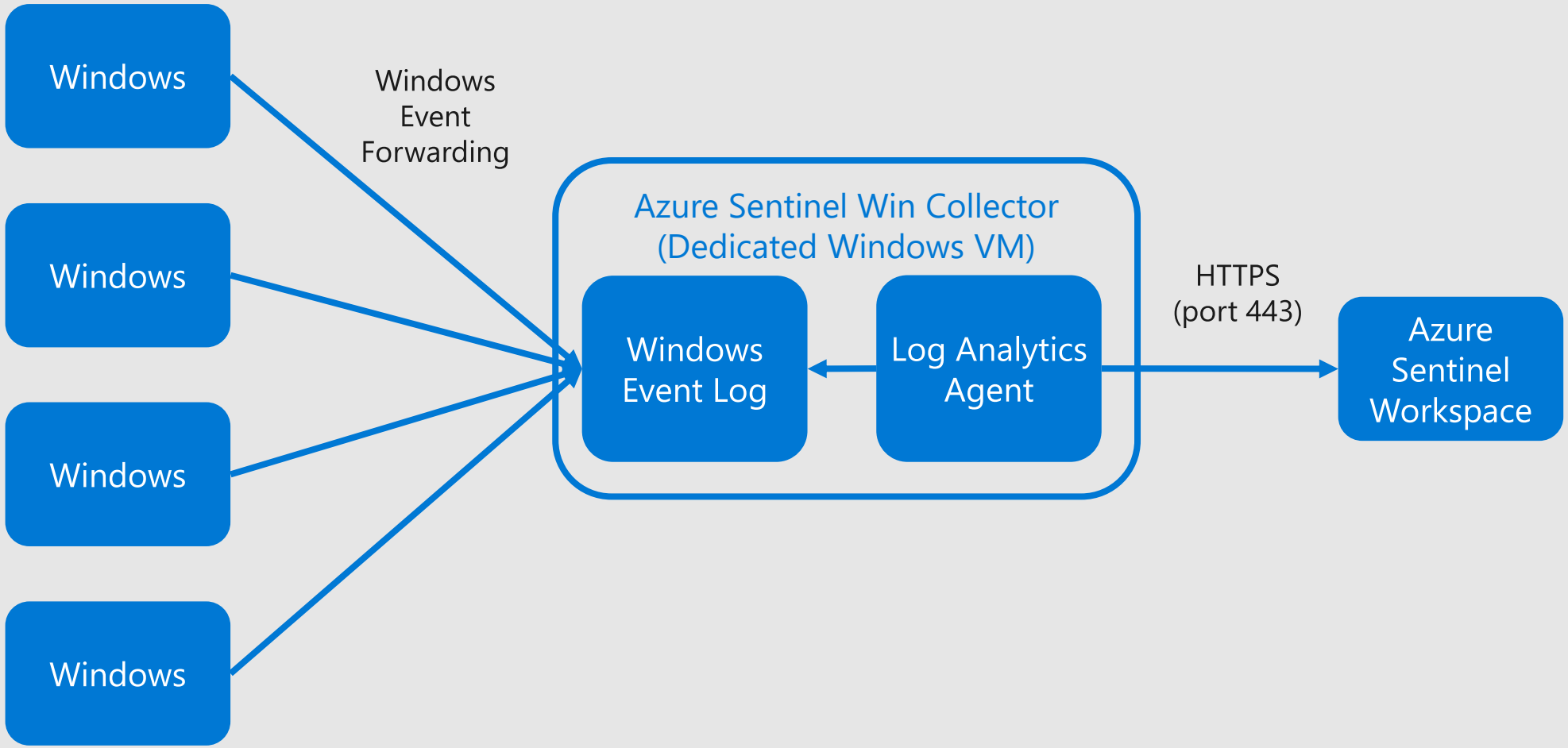
Syslog:

<134> 2018-02-21T16:15:00-04:00 PulseSecure: 2018-02-21 16:15:00 - ive - [127.0.0.1] fakeuser(Admin Users)[] - Primary authentication successful for fakeuser/Administrators from 127.0.0.1

CEF:

<134> Dec 06 16:51:38 hostname CEF:0|JATP|Cortex|3.6.0.1444|email|Phishing|8|externalId=1504 eventId=14067 lastActivityTime=2016-12-06 23:51:38+00 src= dst= src_hostname= dst_hostname= src_username= dst_username=src_email_id=src@abc.comdst_email_id={test@abc.com} startTime=2016-12- 06 23:51:38+00 url=http://greatfilesarey.asia/QA/files_to_pcaps/74280968a4917da52b5555351eeda969.bin fileHash=bce00351cfc559afec5beb90ea387b03788e4af5 fileType=PE32
executable (GUI) Intel 80386, for MS Windows

Windows Event Forwarding



Custom connectors

- For events or enrichment data
- PowerShell
- Logic Apps
  - Scheduled or HTTP triggered
  - Files, Databases, API
  - On-premise gateway
- Direct API use:
  - Ruby, Python, PHP, C#
  - Serverless with Azure Functions