



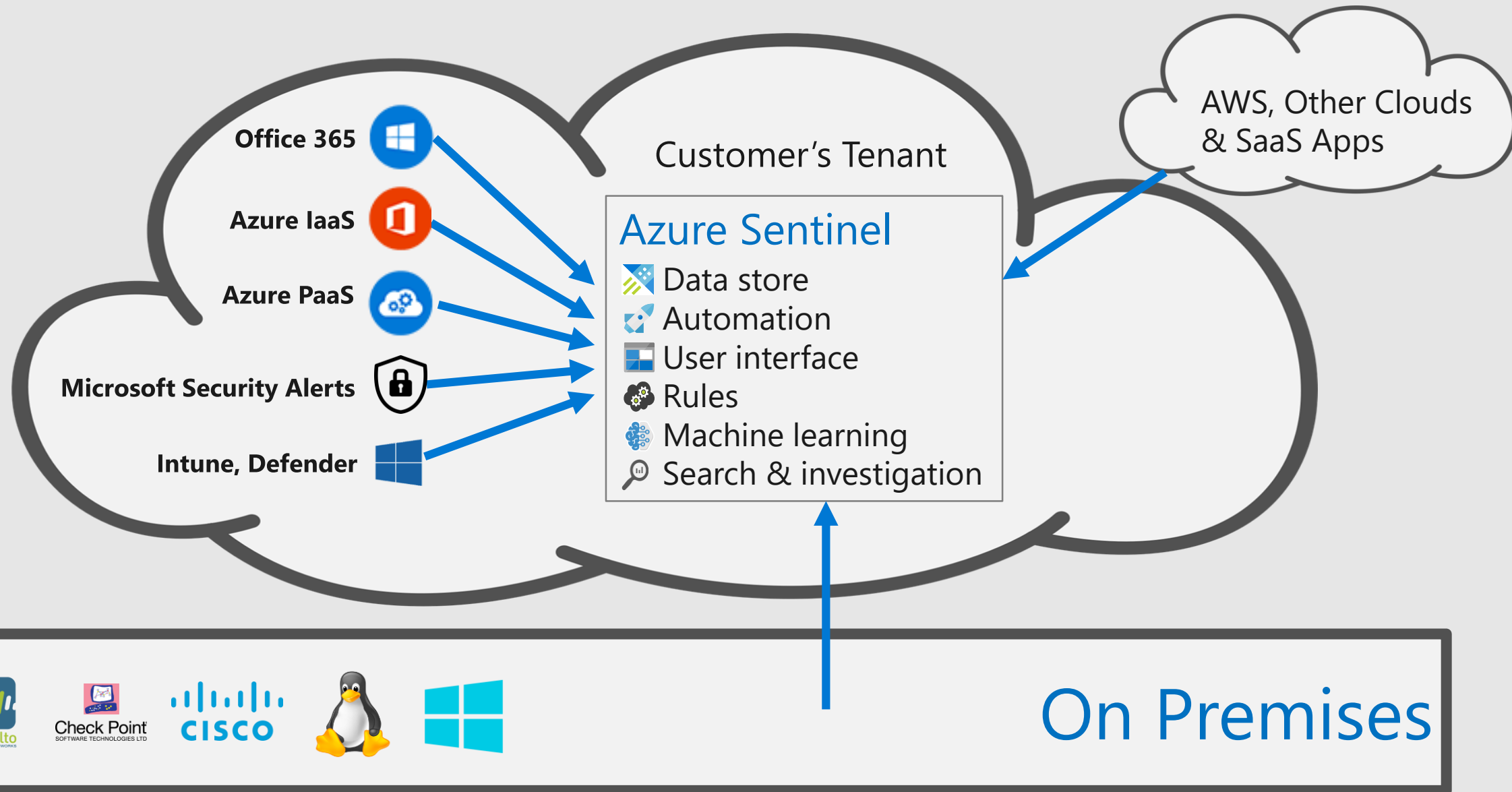
Azure Sentinel Level On Prem & IaaS collection Architecture

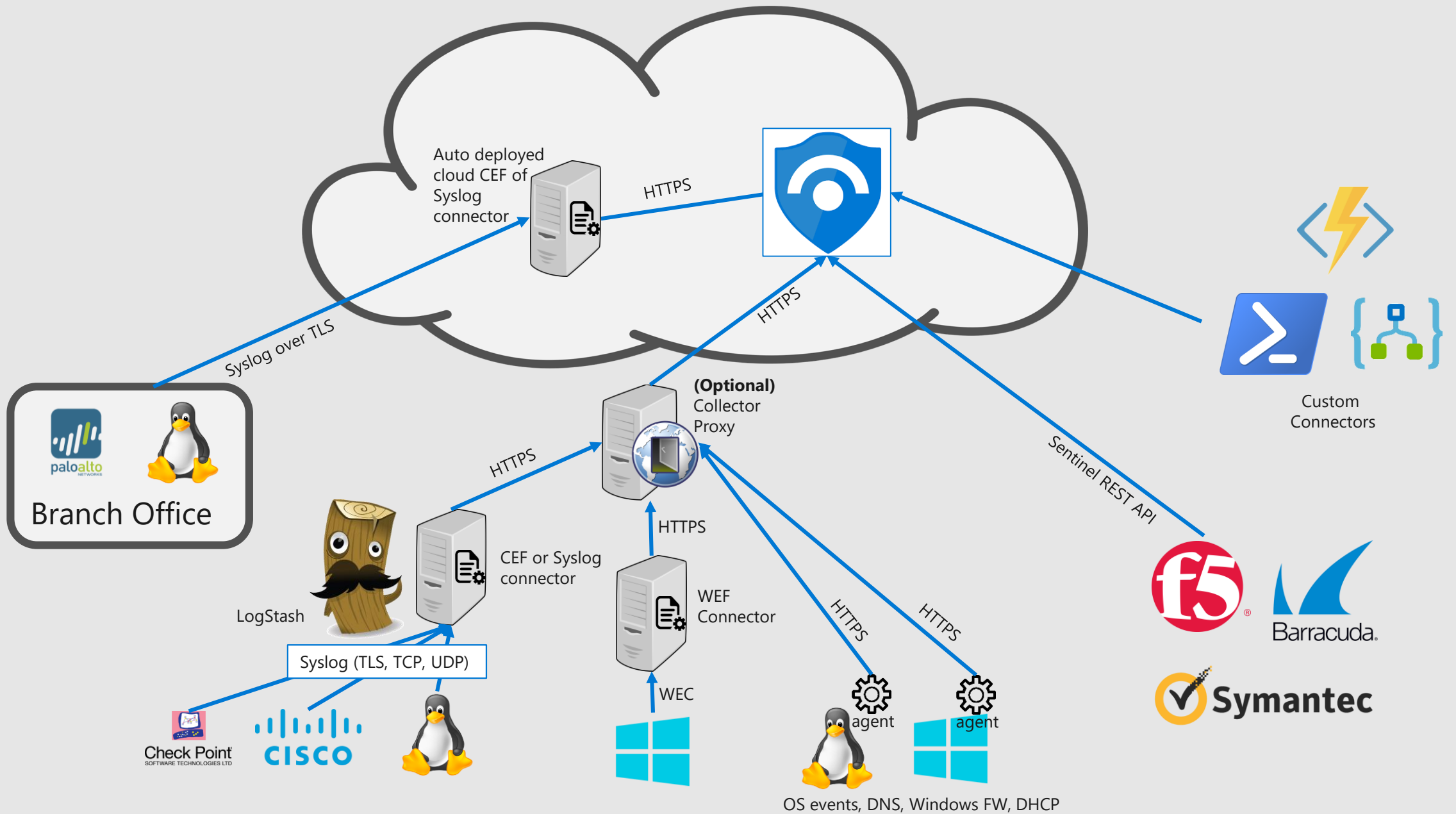


Agenda

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





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

The screenshot displays the Azure portal interface. The main pane shows a table of virtual machines under the 'Virtual machines' heading. The table includes columns for NAME, LOG ANALYTICS CONNECTIVITY, OS, SUBSCRIPTION, RESOURCE GROUP, and LOCATION. The first row, 'ADE-WinVM1', is highlighted and shows a 'Not connected' status. To the right, a sidebar for 'ADE-WinVM1' provides details: Status is 'Not connected', Workspace Name is 'None', and a message states 'VM is not connected to Log Analytics.'.

NAME	LOG ANALYTICS CONNECTIVITY	OS	SUBSCRIPTION	RESOURCE GROUP	LOCATION
ADE-WinVM1	Not connected	Windows	44e4eff8-1fcb-4a22-a...	CxE-Tiander	westeurope
BitlockerTest	This workspace	Windows	44e4eff8-1fcb-4a22-a...	CXE-Anthony	eastus2
BitlockerTest2	This workspace	Linux	44e4eff8-1fcb-4a22-a...	CXE-Anthony	westus
BitlockerTest3	This workspace	Windows	44e4eff8-1fcb-4a22-a...	CXE-Anthony	centralus
bitlockertest4	Error	Linux	44e4eff8-1fcb-4a22-a...	CXE-Anthony	westus
bitlockertest5	This workspace	Linux	44e4eff8-1fcb-4a22-a...	CXE-Anthony	eastus
ContosoVM1	This workspace	Windows	44e4eff8-1fcb-4a22-a...	SOC	canadacentral
LoginTest	This workspace	Windows	44e4eff8-1fcb-4a22-a...	SOC	eastus2
mor-dns-test	Error	Windows	44e4eff8-1fcb-4a22-a...	SOC	francecentral
Romeo-GoldenBox	This workspace	Windows	44e4eff8-1fcb-4a22-a...	CXE-ROMEO	eastus2

Virtual machines
CyberSecurityDemo

Refresh ? Help

Filter by name... 8 selected 2 selected Microsoft Azure Sp... 5 selected 7 selected

NAME **LOG ANALYTICS CONNECTIVITY** **OS** **SUBSCRIPTION** **RESOURCE GROUP** **LOCATION**

ADE-WinVM1 Not connected Windows 44e4eff8-1fcb-4a22-a... CxE-Tiander westeurope

BitlockerTest This workspace Windows 44e4eff8-1fcb-4a22-a... CXE-Anthony eastus2

BitlockerTest2 This workspace Linux 44e4eff8-1fcb-4a22-a... CXE-Anthony westus

BitlockerTest3 This workspace Windows 44e4eff8-1fcb-4a22-a... CXE-Anthony centralus

bitlockertest4 Error Linux 44e4eff8-1fcb-4a22-a... CXE-Anthony westus

bitlockertest5 This workspace Linux 44e4eff8-1fcb-4a22-a... CXE-Anthony eastus

ContosoVM1 This workspace Windows 44e4eff8-1fcb-4a22-a... SOC canadacentral

LoginTest This workspace Windows 44e4eff8-1fcb-4a22-a... SOC eastus2

mor-dns-test Error Windows 44e4eff8-1fcb-4a22-a... SOC francecentral

Romeo-GoldenBox This workspace Windows 44e4eff8-1fcb-4a22-a... CXE-ROMEO eastus2

ADE-WinVM1
Virtual machine

Connect Disconnect Refresh

Not connected

Status
Not connected

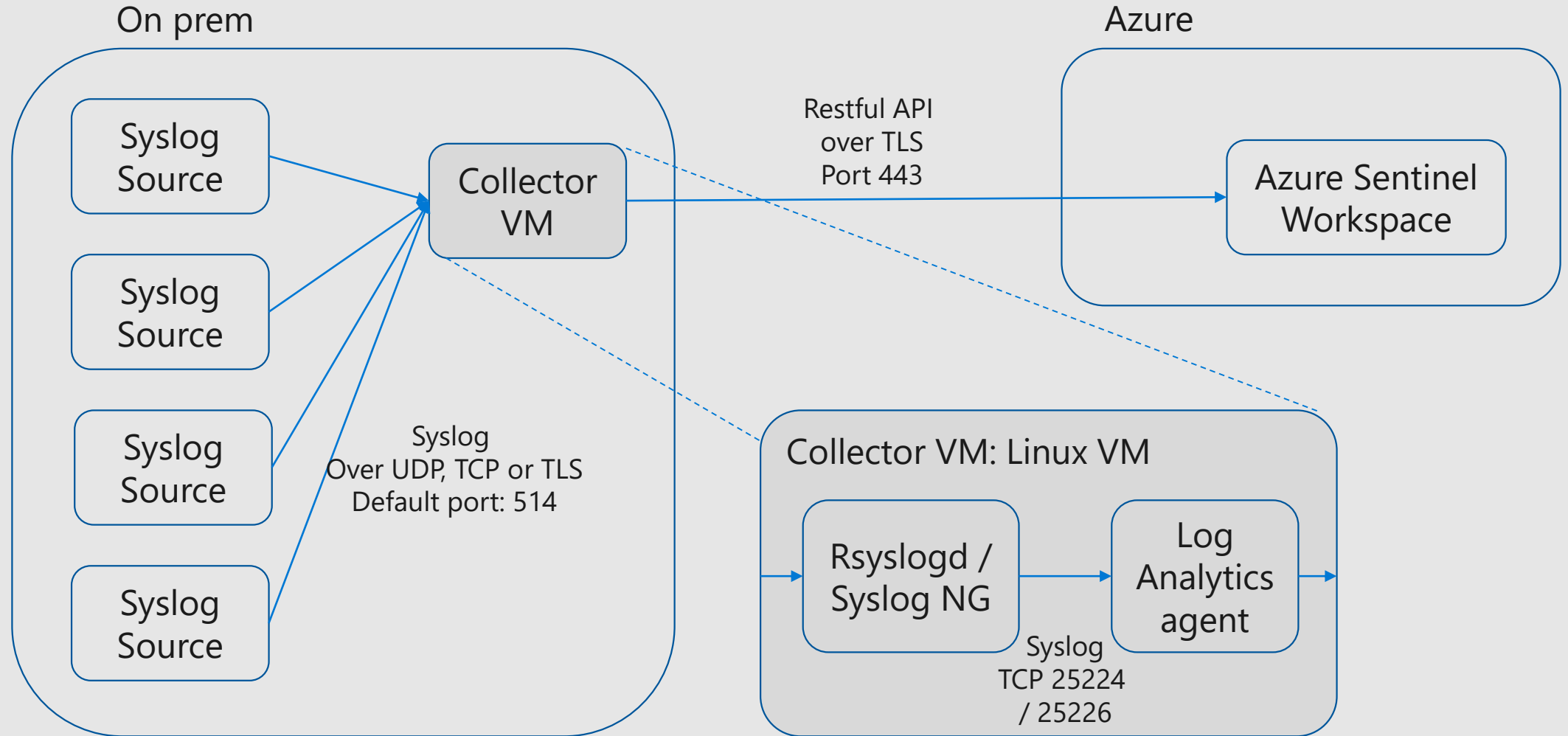
Workspace Name
None

Message
VM is not connected to Log Analytics.

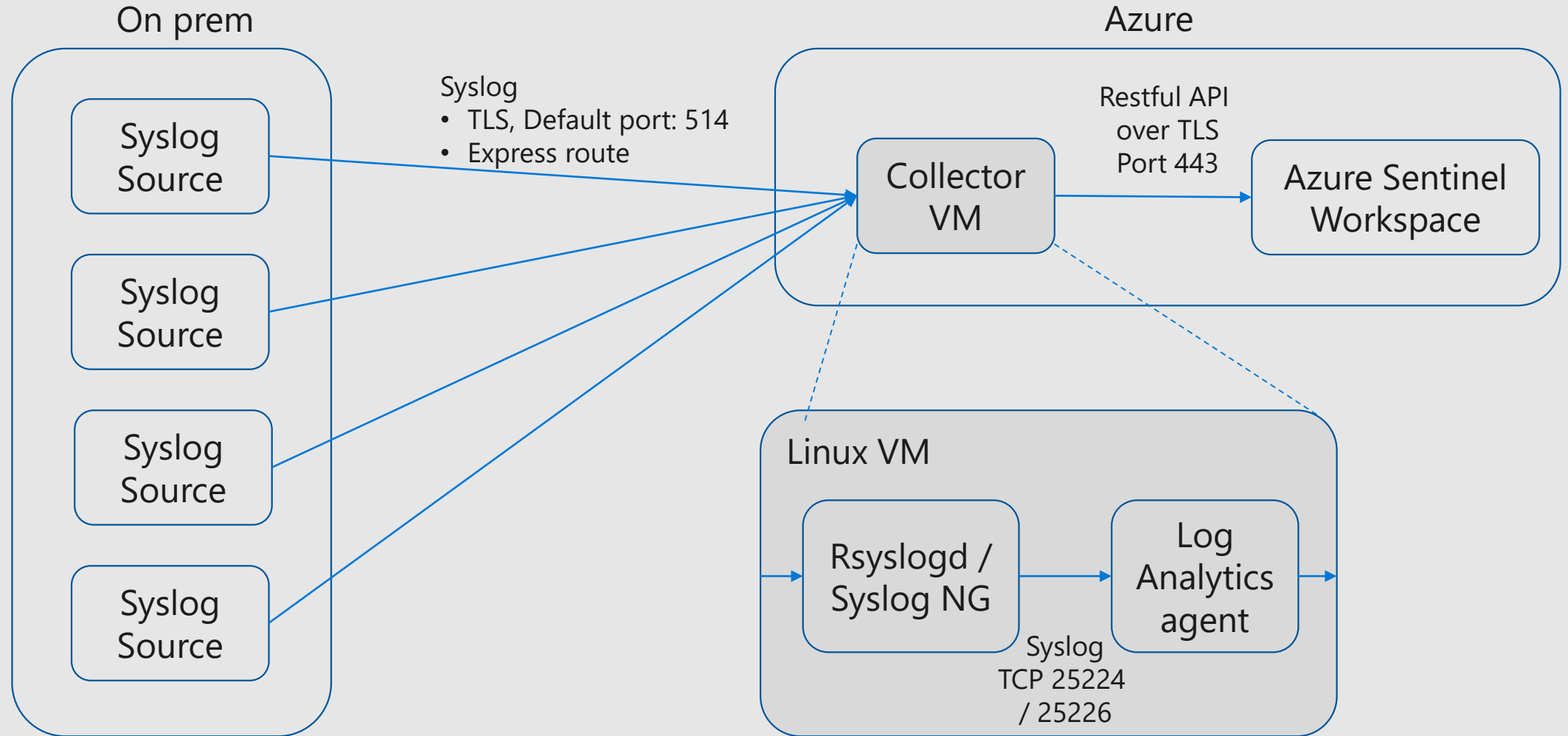
CEF and Syslog collection



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.

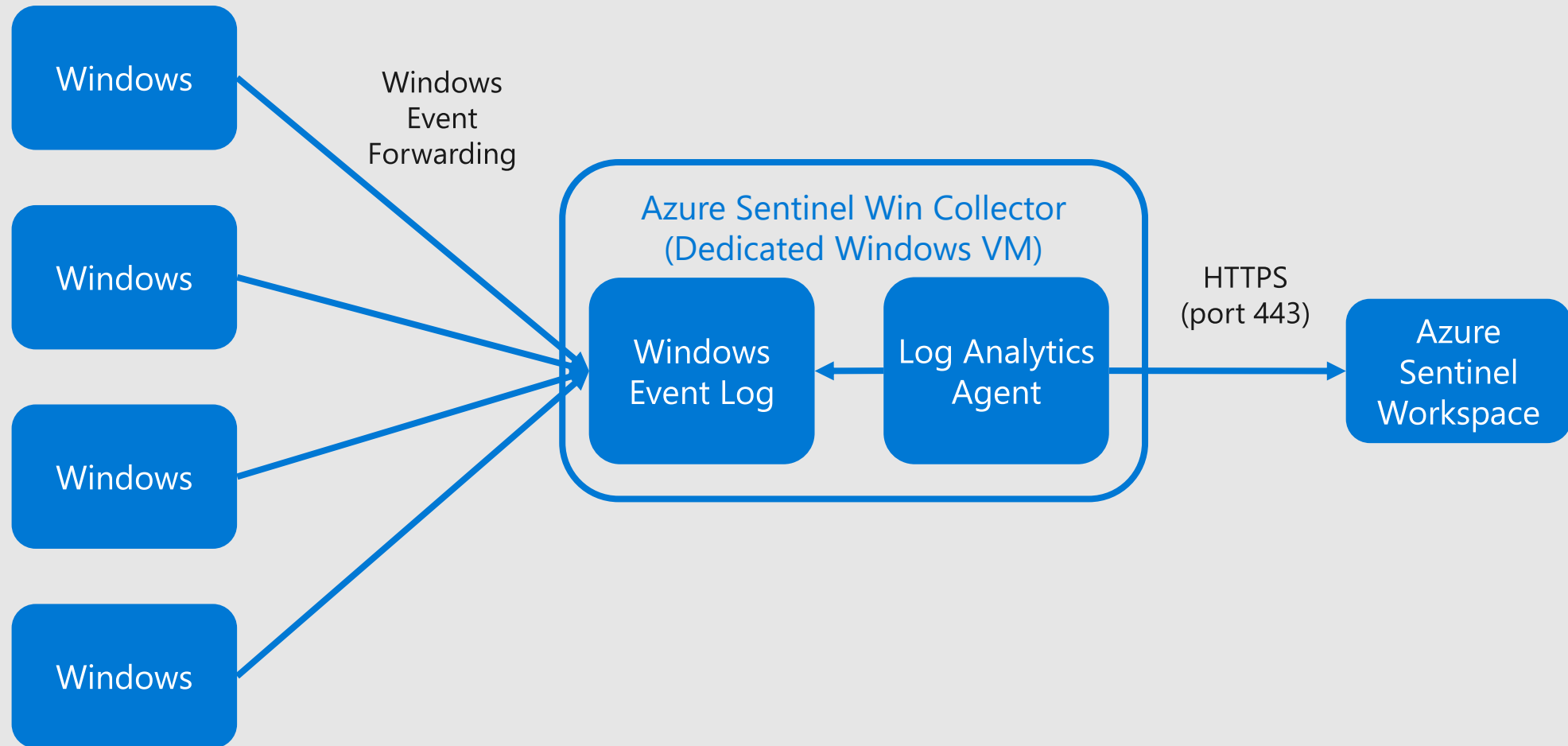
Syslog:

```
<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

