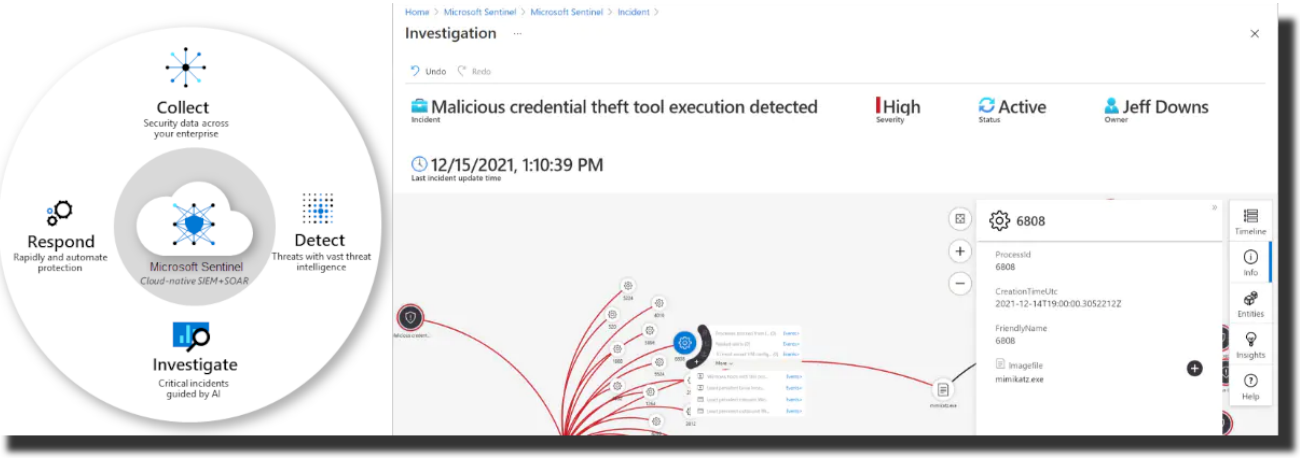
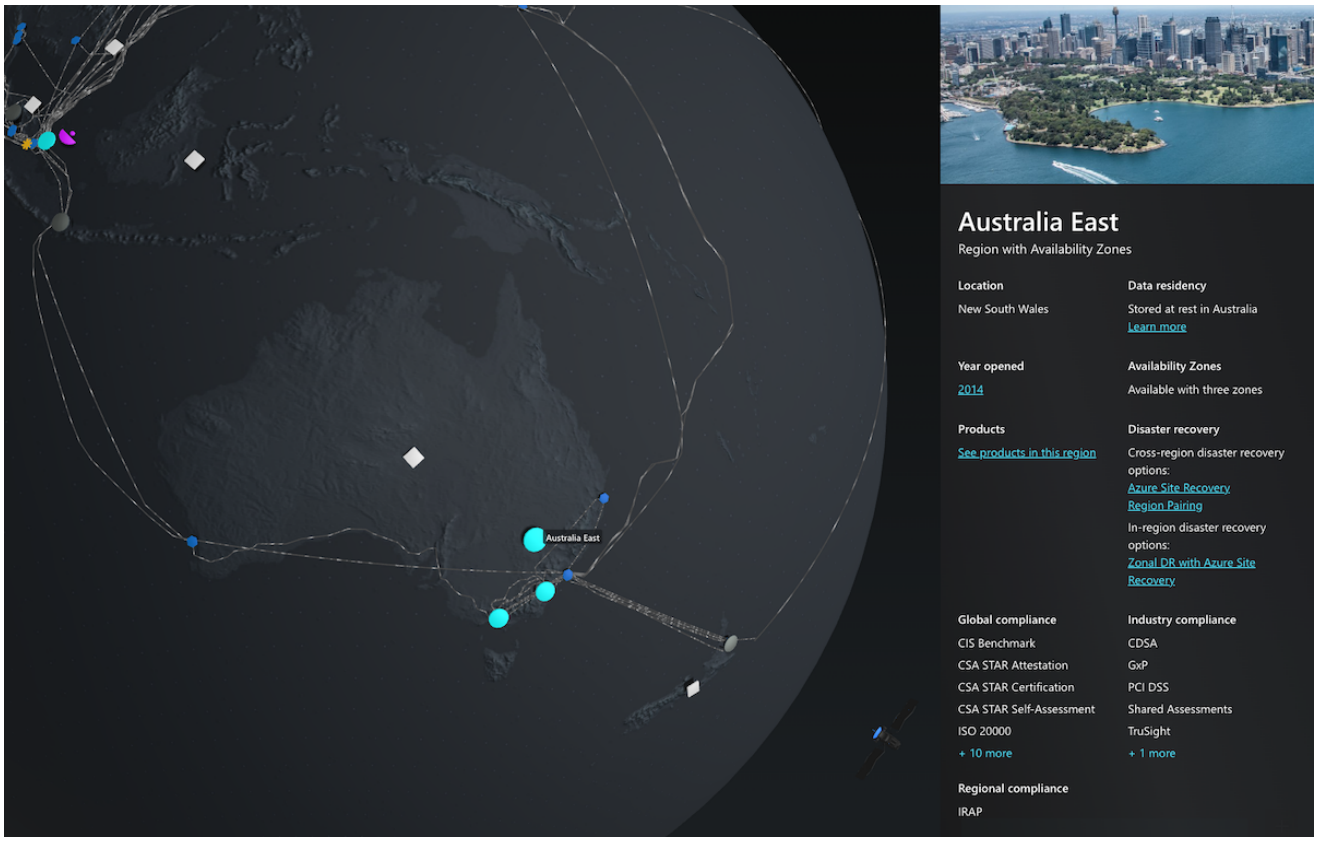
WA SOC Microsoft Sentinel Connector Guidance

Microsoft Sentinel *Collect => Detect => Investigate => Respond* overview.



The below guide has been constructed by the WA Security Operations Centre (SOC) to prioritise connectors and configuration based on cost and complexity. There are several free data sources for Microsoft Sentinel, however the best approach is to connect as much as you can, then monitor costs and run queries to understand your data ingestion to reduce your costs where possible.

1. Sentinel Deployment Notes



It is recommended to deploy Microsoft Sentinel in the **Australia East** region. If you have not already done so, you can follow the steps below:

- Create a Log Analytics Workspace
- Enable Microsoft Sentinel

If you have Log Analytics setup in another region, it is recommended to move it to Australia East where possible, as query performance is reduced when spanning multiple regions, and the majority of existing deployments are in Australia East.

2. High value / low-cost connections

These connectors are largely built into the cost of the services they protect, and provide a high value in terms of assets protected. Some additional context is provided on how to best configure and onboard devices and services, however only **the emphasised steps** need to be completed to establish a baseline SIEM environment.

2.1. Connect Azure Active Directory (Azure AD)

Ensure that Identity management activities are picked up, including Audit logs, Sign-in logs, Provisioning logs, Risky users logs, Risk detections logs

2.2. Turn on Microsoft 365 Defender

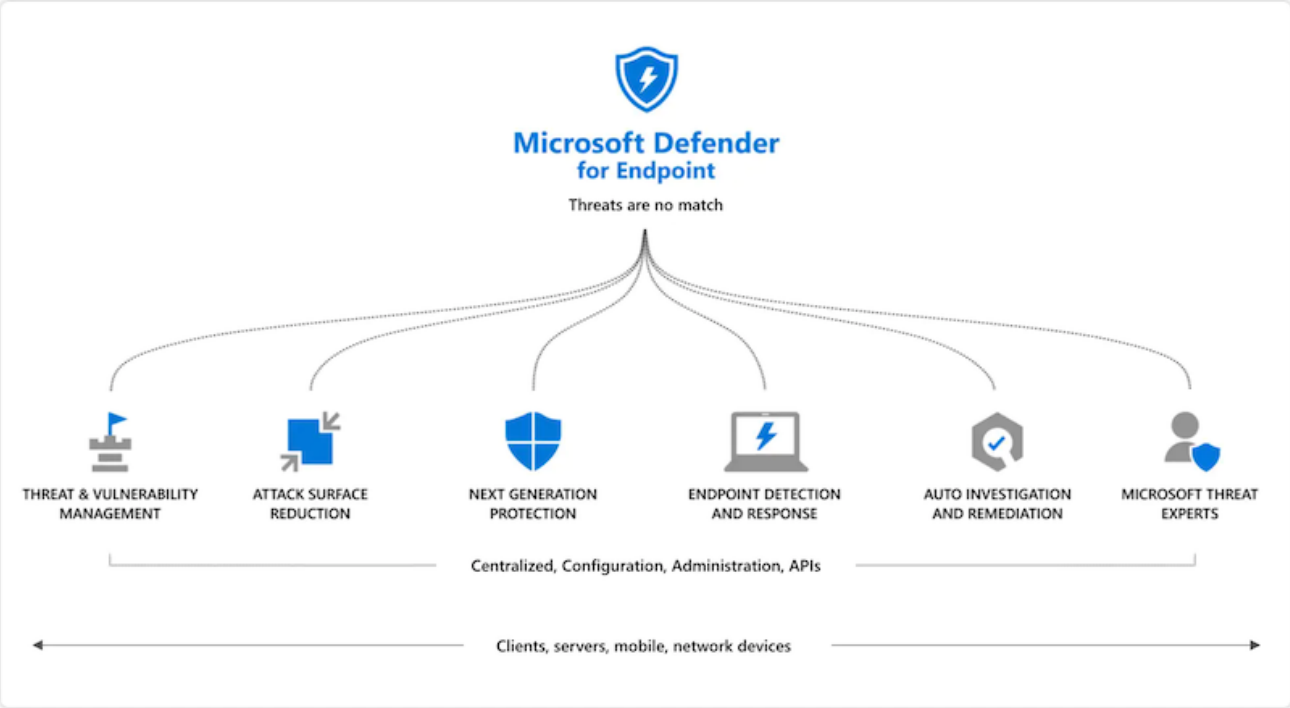
This includes Office 365, Endpoint, Identity and Cloud Apps

2.2.1. Protect against Threats using Defender for Office 365

Align with the ACSC Essential Eight Maturity Model

- Use Exchange Online and SharePoint Online for all staff email & file services
- Integrate with Defender for Endpoint

2.2.2. Configure Microsoft Defender for Endpoint in Intune

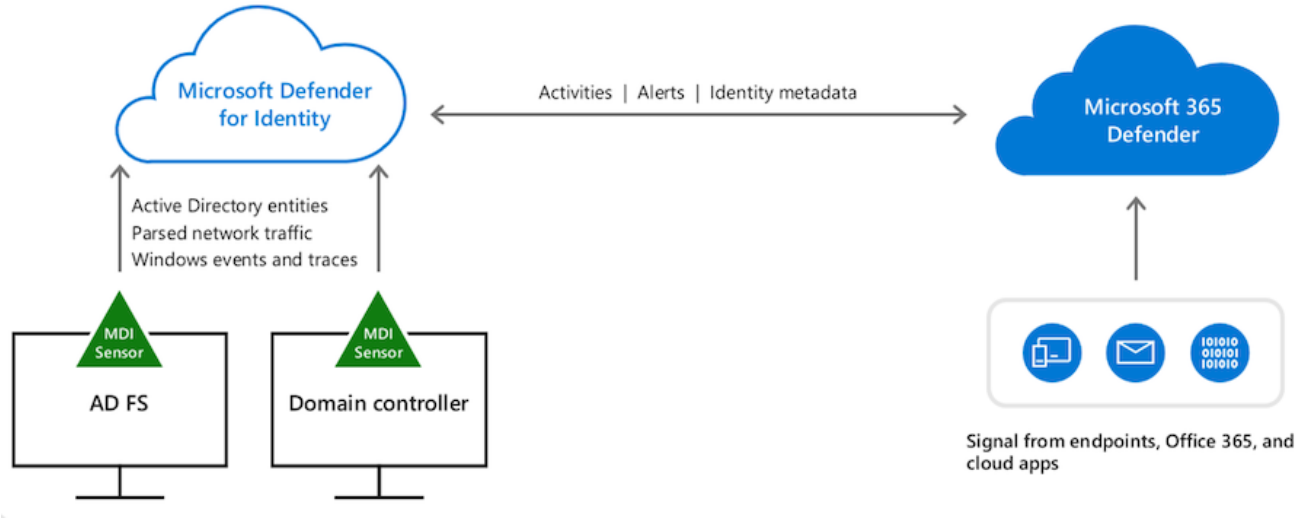


- Use Intune for endpoint management and mobile device management

- Windows, macOS and Linux servers should also be onboarded into Microsoft 365 Defender for Endpoint unless they are separately sending the above data to Sentinel via another connector (e.g. Microsoft Defender for Cloud or Container Insights)
- Windows devices in Defender for Endpoint - Windows 7+, Windows Server 2008 R2+
- Defender for Endpoint on Mac - macOS 10.15+ (Catalina)
- Defender for Endpoint on Linux - Debian 9+, Ubuntu 16.04+, RHEL6+, SLES12+, CentOS6+, OEL7+, Fedora33+
- Align with the ACSC Strategies to Mitigate Cyber Security Incidents by moving endpoints to Windows cloud configuration which includes Security Baseline for Windows, then configure WDAC policy for Application Control, Defender for Endpoint Baseline and Edge Baseline.

This is the lowest cost way per device to get baseline monitoring in place.

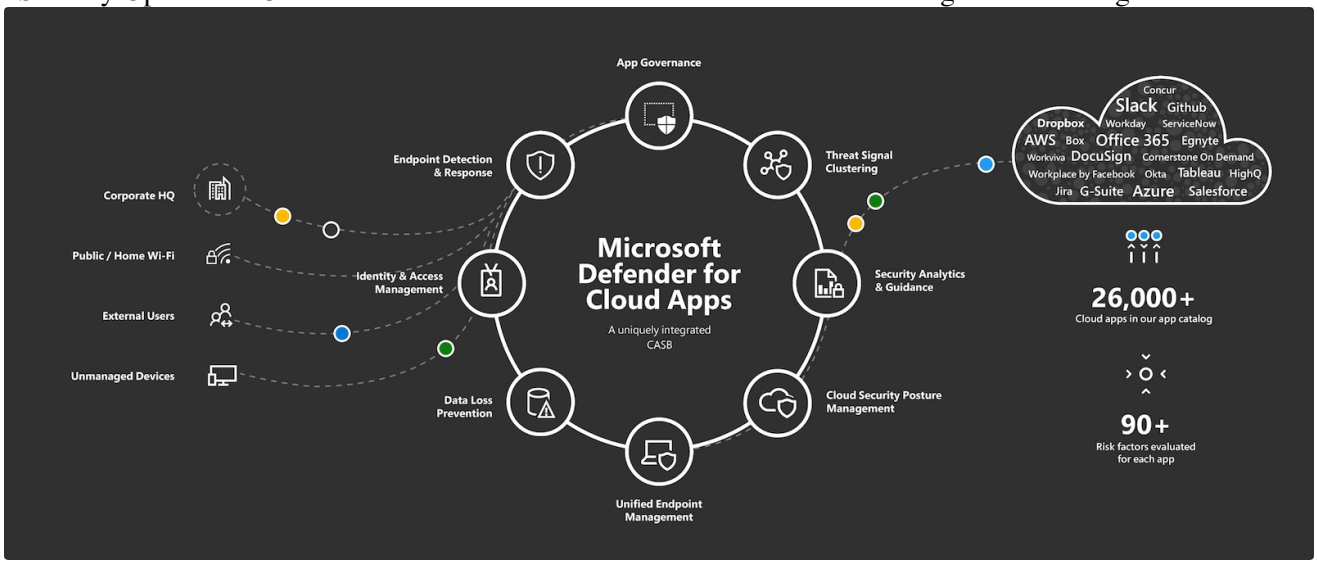
2.2.3. Install Identity Sensors



Install on all domain controllers and ADFS servers

- This is only relevant where on-premise Active Directory syncs to Azure AD, if entirely using Azure AD this is not required
- Configure RADIUS Accounting on 802.1X networks & VPNs - Capture 802.1X events via RADIUS accounting traffic forwarded to Identity Sensors (VPNs, wireless, 802.1X ports)

2.2.4. Integrate Defender for Cloud Apps



2.2.5. Connect Microsoft 365 Defender

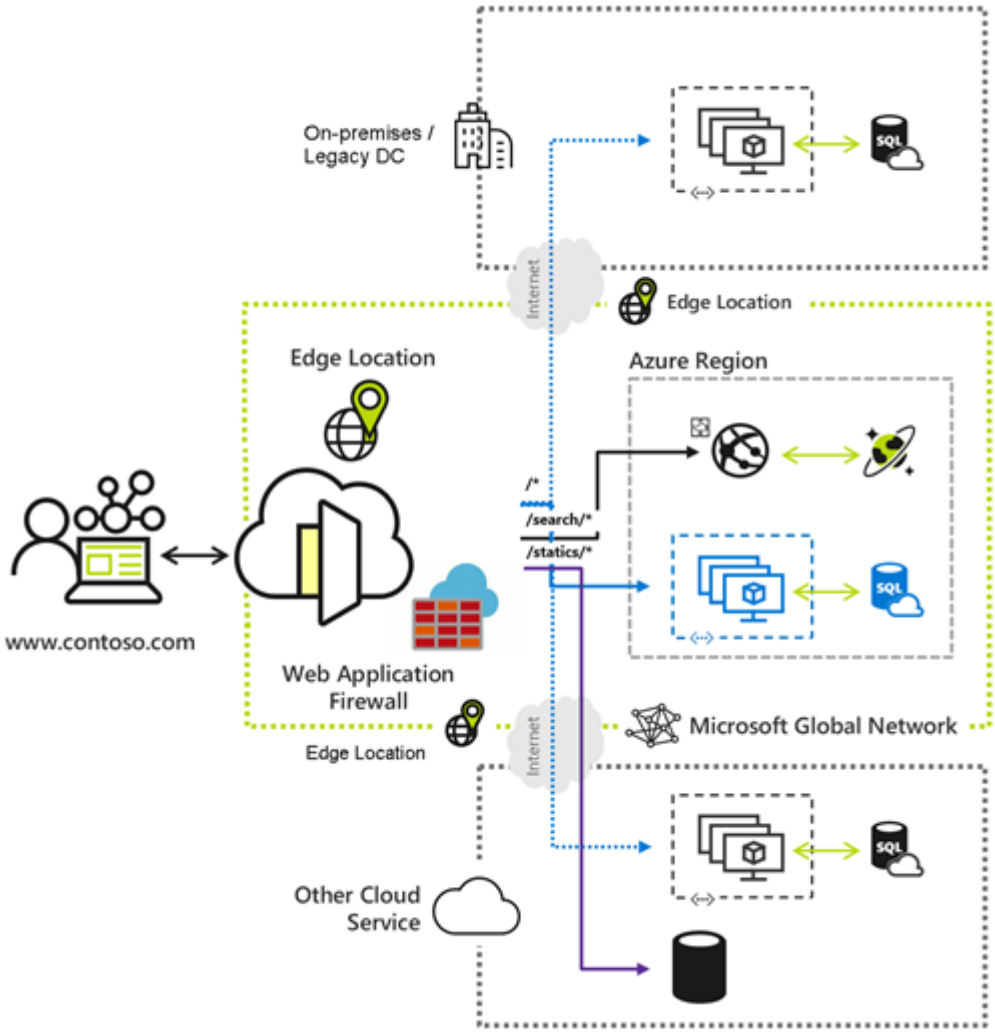
Collect events from Defender for Office 365 and Defender for Endpoint

- Enable collection of events from all Advanced Hunting tables (Defender, Office 365, Identity, Cloud Apps & Alerts)

2.3. Connect Azure Activity log

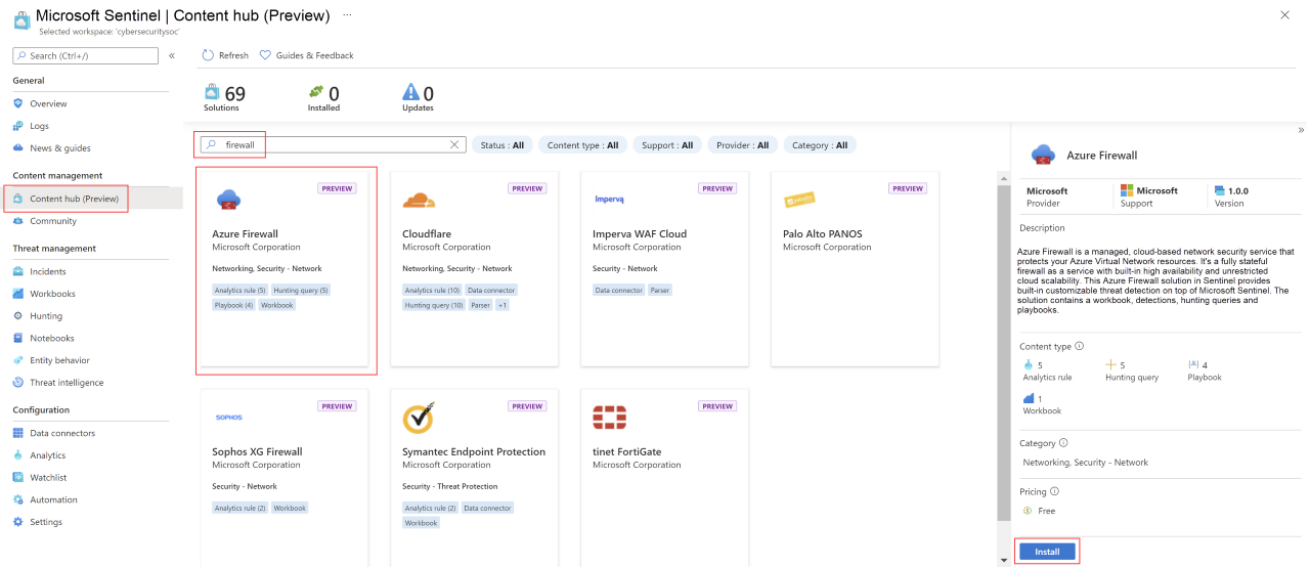
Ensure all azure activity is logged and retained.

2.4. Ingest WAF events (Azure Front Door) into Sentinel



WAF events are a high quality security event source for monitoring ingress to applications. Third party WAF integration options are listed on the Sentinel content hub

2.5. Review the Sentinel content hub



Check and enable security relevant connections to other services or products your organisation is using.

3. Complex connections

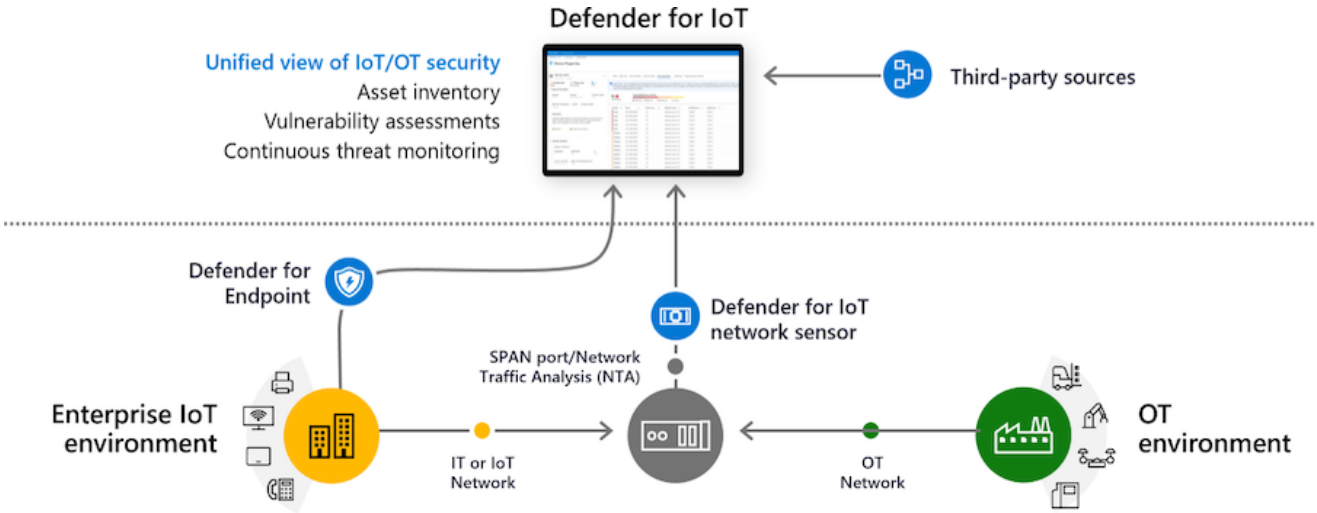
These are good for querying manually, however most require some work to Normalise using the Advanced Security Information Model (ASIM) to be incorporated into automatic incident generation using standard Sentinel rules.

1. AWS S3 Connector - This collects data via S3 buckets so has some delays compared to higher level integrations like Microsoft 365 Defender or Container Insights
2. Logstash to connect data sources to Microsoft Sentinel - For third party platforms without microsoft documented connection guidance, this is the best integration option.
3. CEF-formatted logs from your device or appliance
4. Linux-based sources using Syslog

4. Potentially high-cost connections

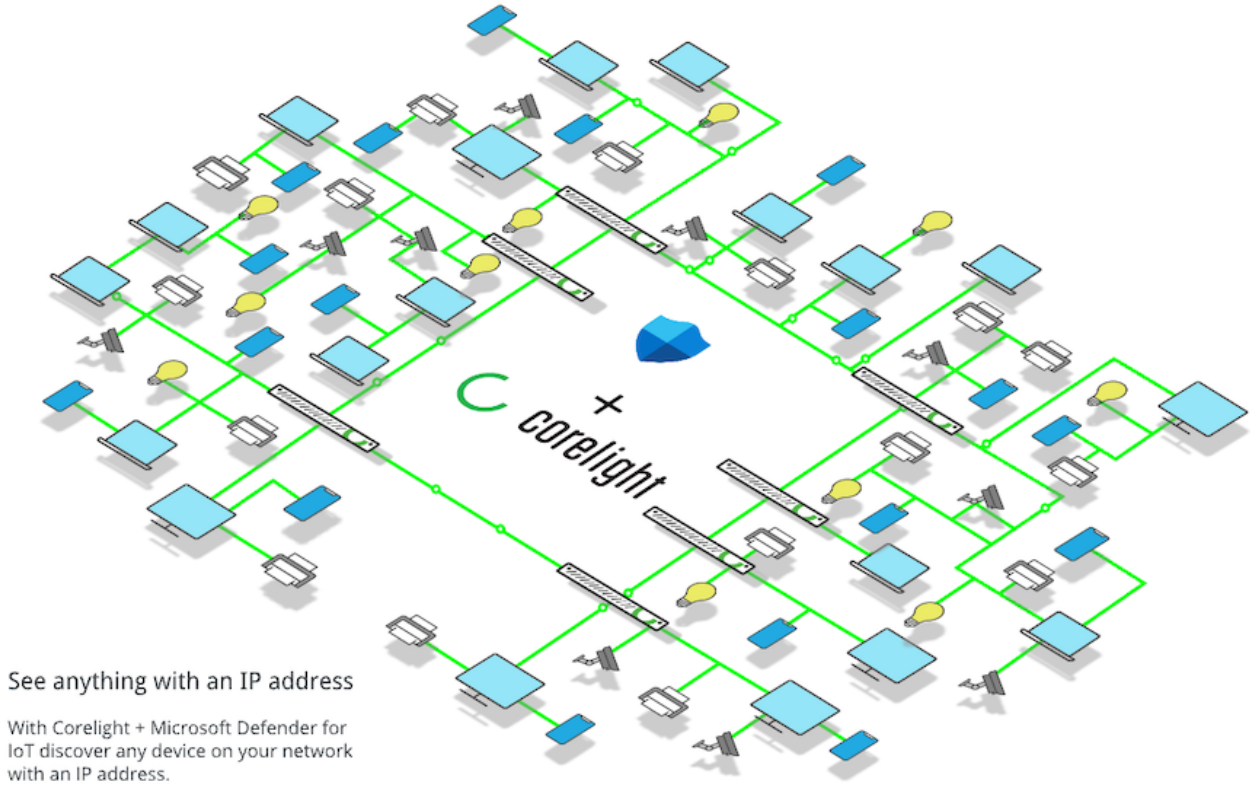
1. Container Insights - Centrally monitor Kubernetes cluster performance and query logs
2. Microsoft Defender for Cloud - If possible Enable all Microsoft Defender plans for your high value systems (such as Domain Controllers and SQL Databases, approx. 2-3% of total servers usually)

4.1. Operational Technology passive network monitoring



Use Microsoft Defender for IoT/OT for passive network monitoring for devices not supported by Defender for Endpoint/Cloud via TAP/packet broker (previously CyberX), this is a very high quality egress monitoring event source. Microsoft makes significant volume discounts available.

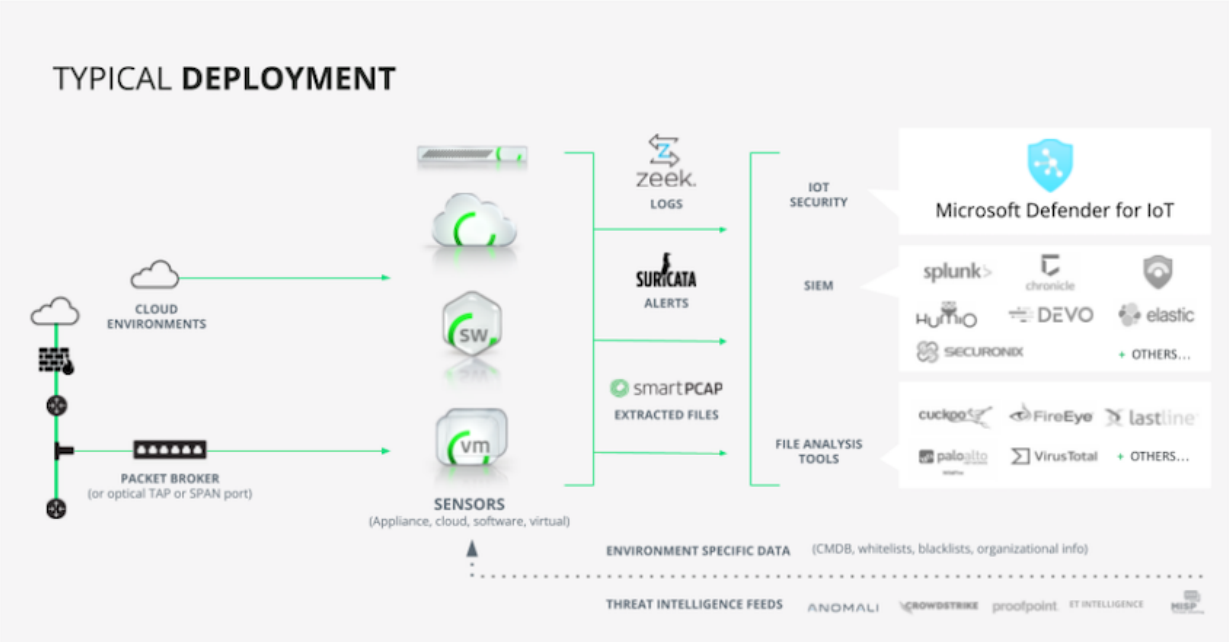
- To manage costs it is recommended to use policy based routing or L3 segmentation to separate your endpoint traffic from OT devices, and utilise a packet broker to push OT traffic into the OT sensor, enterprise firewall packet broker config guides are listed below:
  - Firewalls (best option): Palo Alto Packet Broker, Checkpoint Mirror and Decrypt
  - Switches: Cisco SPAN, Cisco Meraki Port Mirror, Fortinet SPAN
  - A scalable architecture supporting SD-WAN's would be using IPSEC to route OT egress traffic via a public cloud provider (Azure Site to Site, AWS Site to Site) and then monitor the egress using a cloud firewall supporting packet brokering (e.g. Palo Alto VM Series) to a sensor hosted on the public cloud environment itself.
- If passively monitoring over 1K devices using a per Gbps metric sensor such as Corelight may be a more cost effective option



Joint Solution: Microsoft Defender for IoT + Corelight

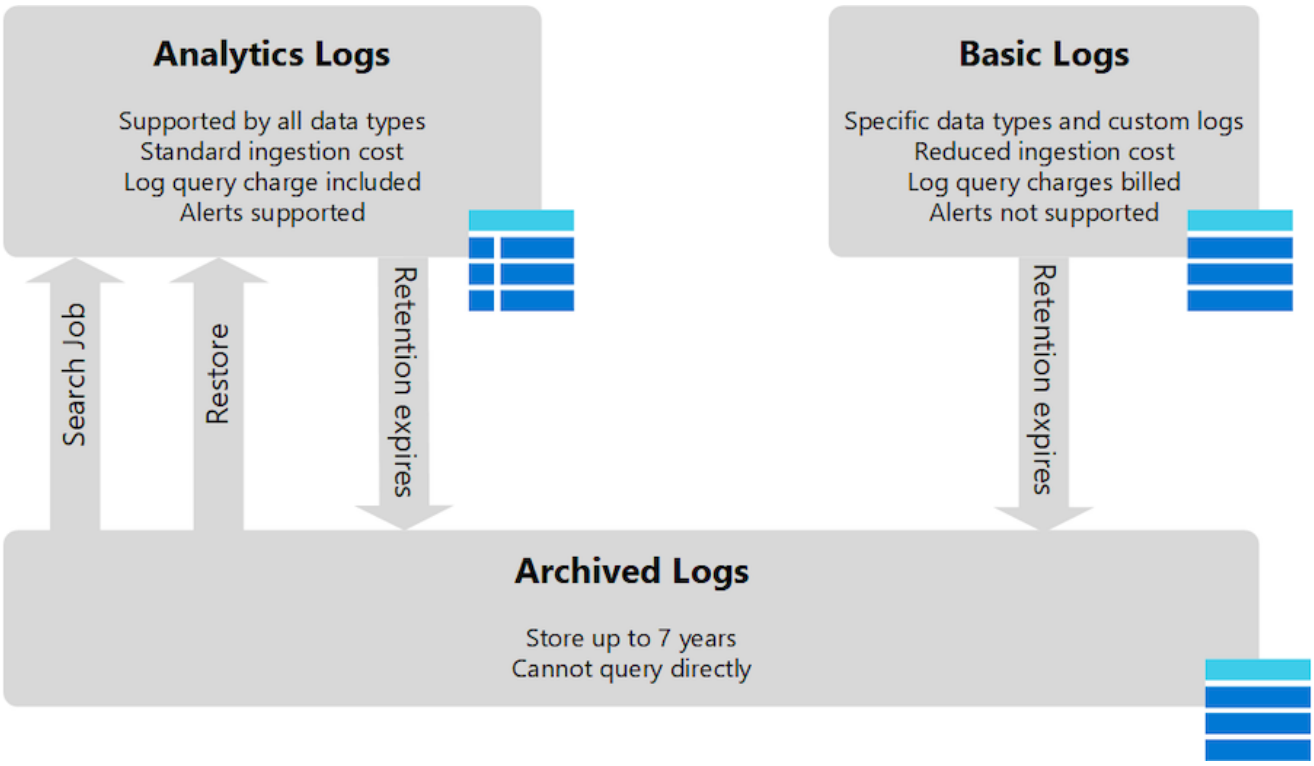
How it works

Corelight Sensors transform every network connection into Zeek data that's comprehensive, structured, and correlated. Microsoft Defender for IoT/OT uses this data for device discovery and classification, vulnerability management, and detection and response, forgoing the need to deploy Defender for IoT's IoT/OT specific network sensor.



Microsoft Defender for IoT applies its behavioral analytics and machine learning to Zeek network data from Corelight Sensors. Corelight can also send data to multiple other destinations simultaneously, including Microsoft 365 Defender, Microsoft Sentinel, Splunk, and other analytic tools.

5. Cost optimisation



Microsoft Sentinel has builtin queries to understand your data ingestion at a per table level. To get further granularity you can look at specific devices sending a lot of data using additional usage queries or directly run manual queries from Investigate your Log Analytics usage.

Once you have identified the high cost items, you can reduce the events generated at the source, using a Logstash filter for a custom source or with configuration in Sentinel itself:

- Ingestion time transformations - should be used to eliminate low value logs before they are persisted within Log Analytics & Sentinel
- Basic Logs - should be used for high volume tables that aren't queried regularly (approx 1/4 cost per GB ingested)