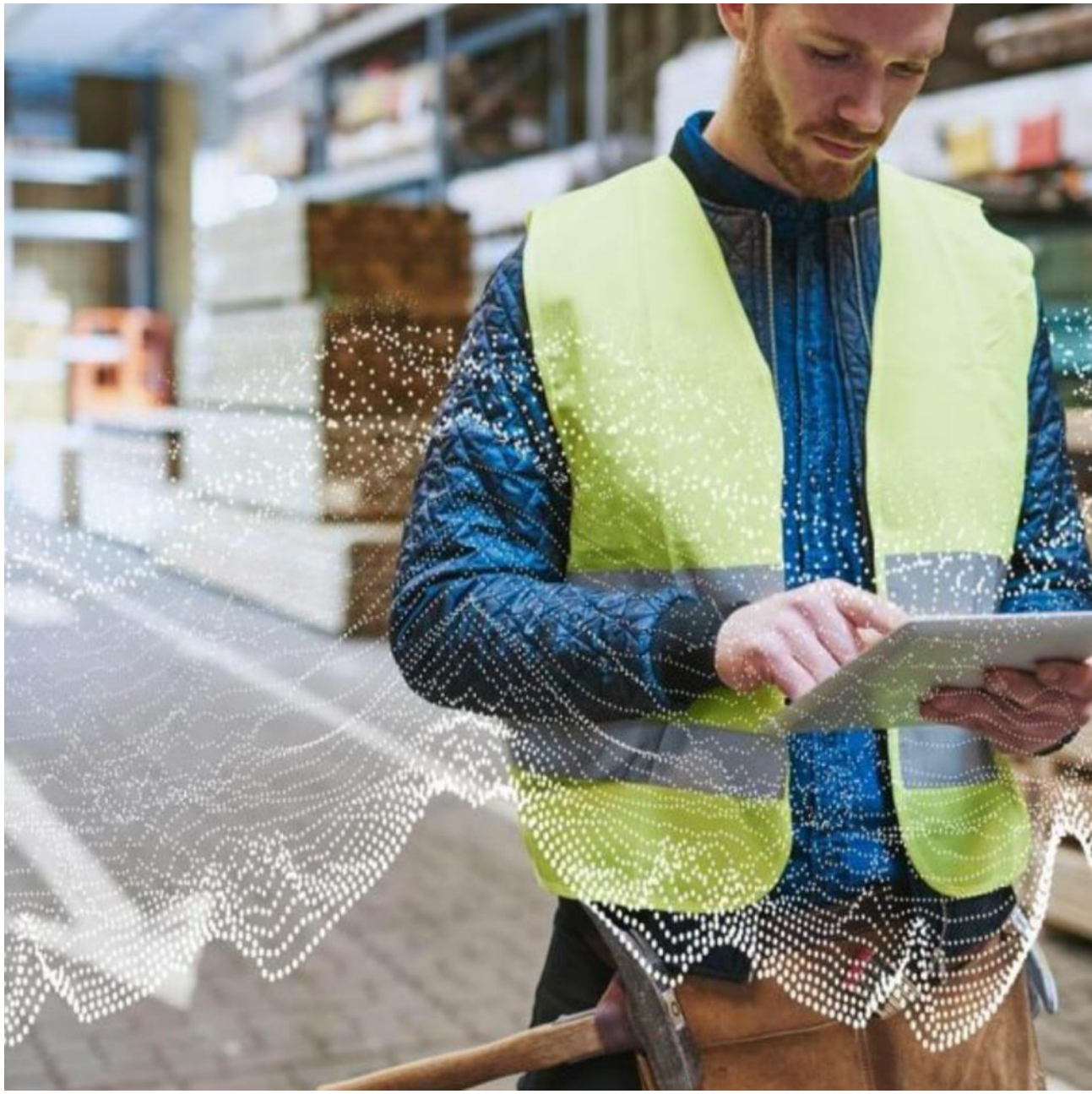
Microsoft Azure

Defender for IoT Overview



Erez Mizrachi – erezm@microsoft.com

Global Black Belt
IoT Security Technology Specialist

Differences between IT & OT security

IT Security

OT Security

Differences between IT & OT security

IT Security

Data confidentiality & privacy

Standard protocols & devices

High levels of connectivity

Multiple layers of controls & telemetry

OT Security

Safety & availability

Specialized protocols, devices & legacy OS platforms

Traditionally air-gapped (apparently)

Little or no visibility into IoT/OT risk

IoT/OT risk = Business risk

Financial

Destructive malware shuts down factories worldwide, causing billion of dollars in losses (WannaCry, NotPetya, LockerGoga, Ekans, …).

IP Theft

Manufacturers are 8x more likely to be attacked for theft of IP like proprietary formulas and designs than other verticals (DBIR).

Safety

Safety controllers in petrochemical facility compromised with purpose-built back door in TRITON attack.

Why IoT/OT cybersecurity is now a board-level concern

Digital transformation & IT/OT connectivity have significantly expanded the attack surface

Adversaries are motivated, sophisticated & increasingly destructive

Enterprise SOCs today have virtually no visibility into their IoT/OT risk

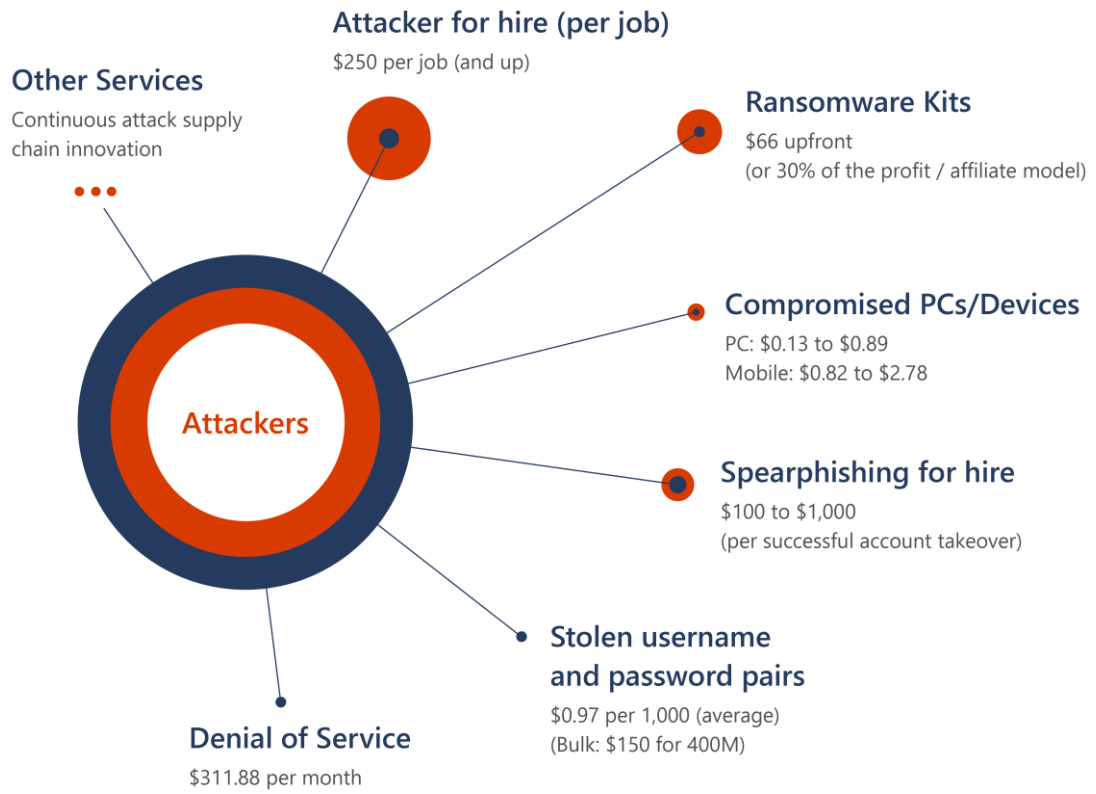
The growing threat of cybercrime

- A threat to national security
- Cybercriminals attacking all sectors
- Ransomware attacks increasingly successful
- Cybercrime supply chain continues to mature

POSITIVE TRENDS

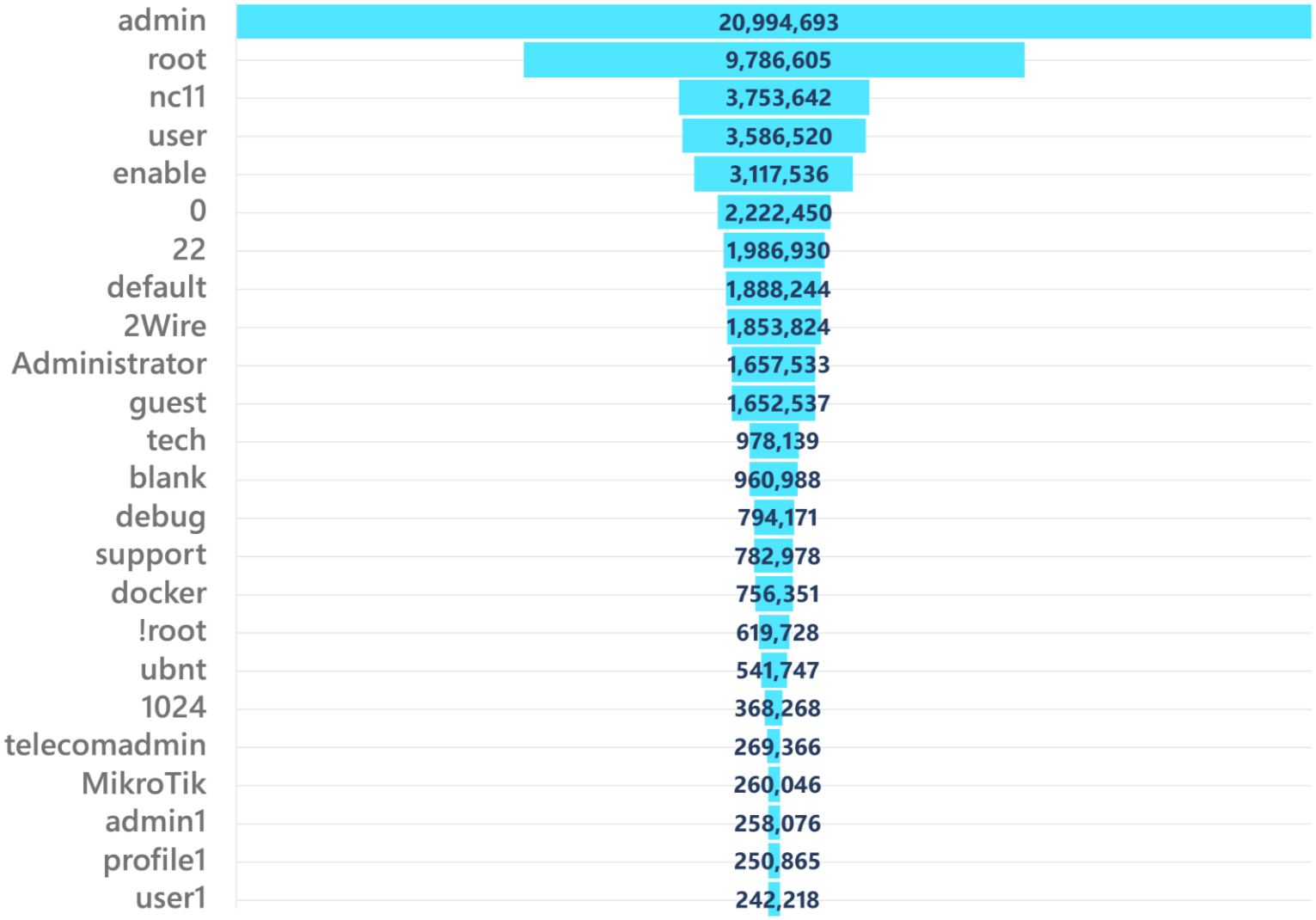
- Transparency: governments and companies coming forward
- Priority: new laws, task forces, resources, partnerships

The cybercrime economy and services



WITH NO TECHNICAL KNOWLEDGE OF HOW TO CONDUCT A CYBERCRIME ATTACK, AN AMATEUR THREAT ACTOR CAN PURCHASE A RANGE OF SERVICES TO CONDUCT THEIR ATTACKS WITH ONE CLICK.

Passwords seen in 45 days of sensor signals

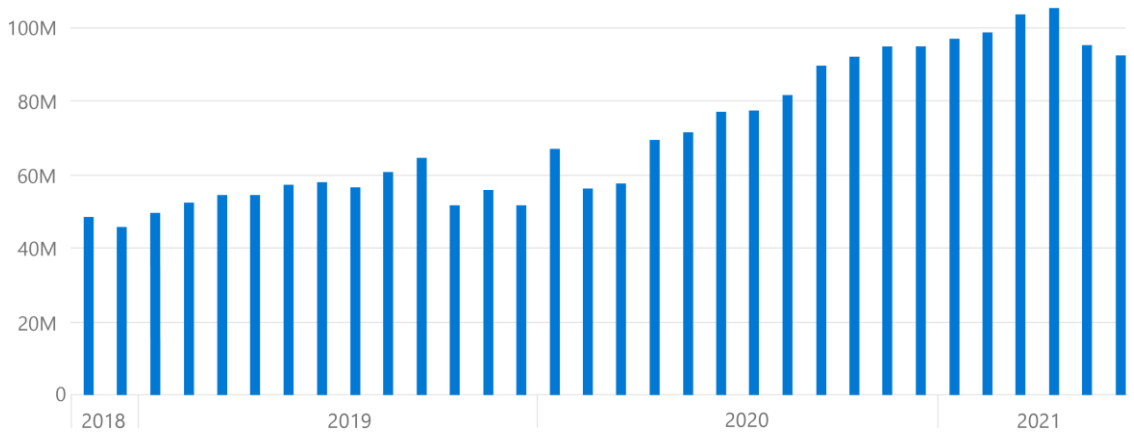


>20 Million

NUMBER OF TIMES WE OBSERVED THE PASSWORD "ADMIN" USED IN IOT DEVICES OVER A 45 DAY PERIOD.

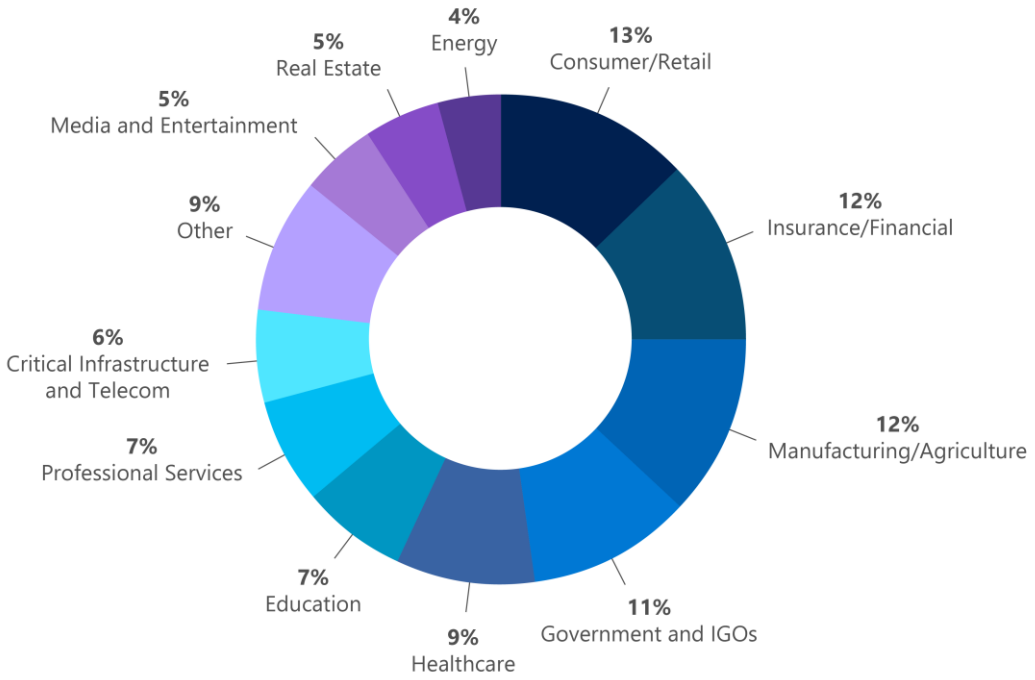
What we're seeing in ransomware data and signals

Ransomware encounter rate (machine count): Enterprise customers (Defender data)



Overall increase in ransomware encounters, with notable surge to consumer and commercial encounters in late 2019,6 when RaaS started to grow, and in early 2020 at the onset of the COVID-19 pandemic.

DART ransomware engagements by industry (July 2020-June 2021)



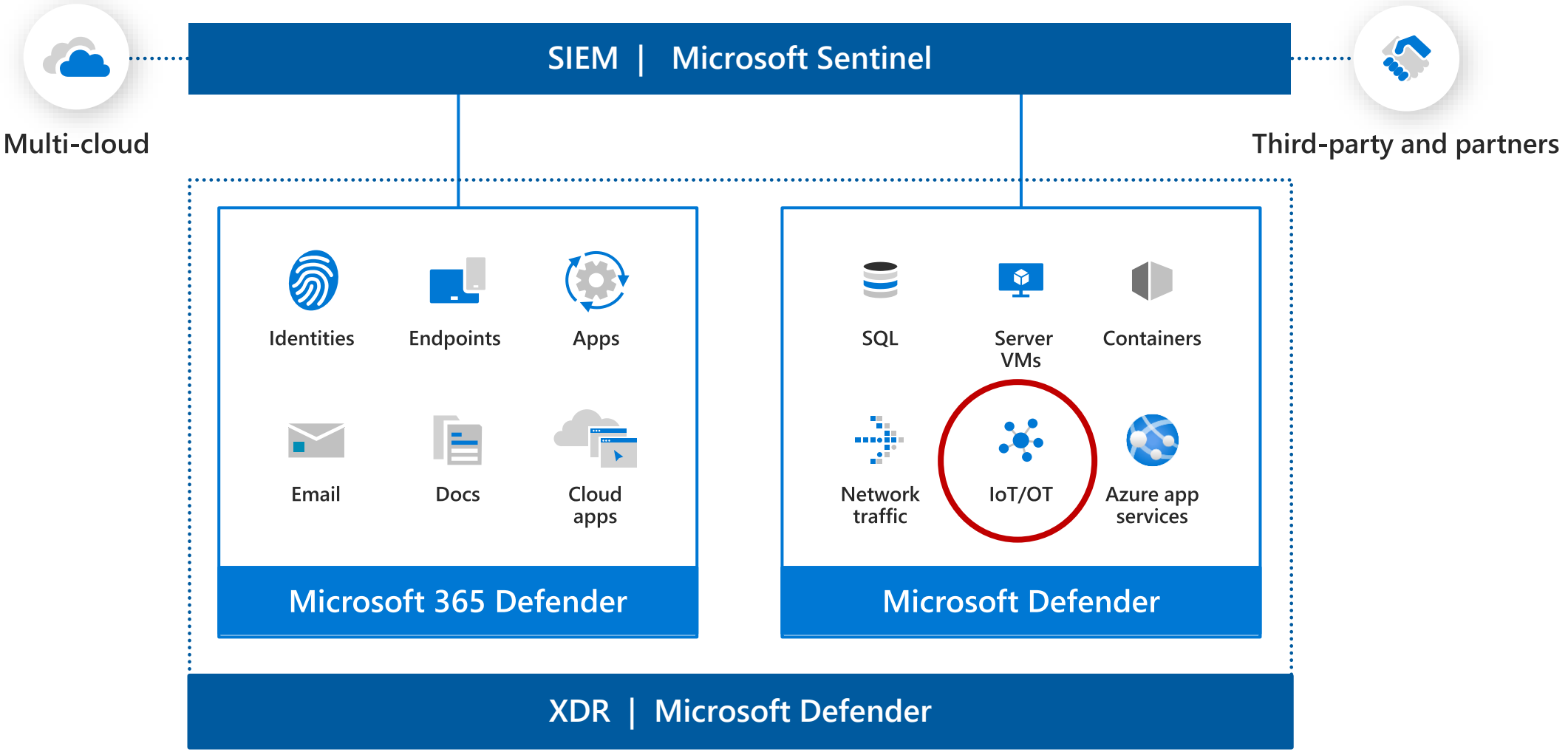
Deploy ransomware protection

The stakes have changed. There is a massive growth trajectory for ransomware and extortion.

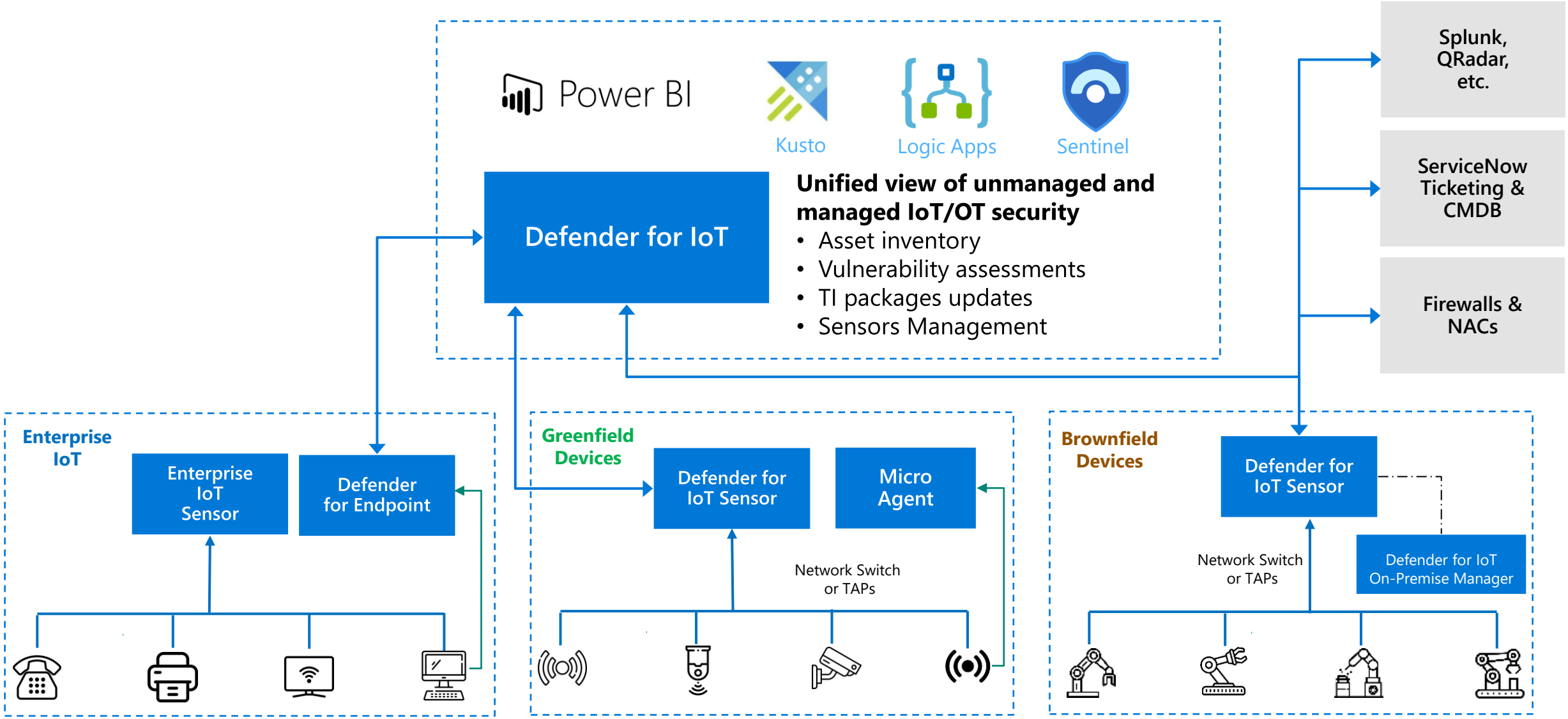
Microsoft

So, what can we do together to help you protect your organization?

A Unified SecOps Experience

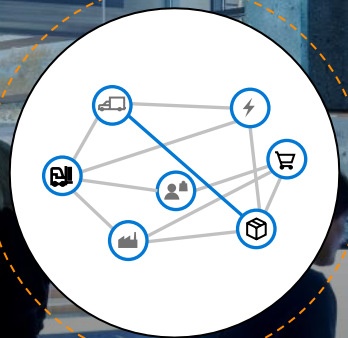


Defender for IoT — Architecture



Multiple deployment options

100% On-Premises
On-premises sensors connected to on-premises SIEM (Splunk, etc.)



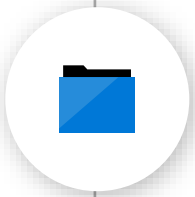
Hybrid
On-premises sensors managed locally & connected to cloud-based SIEM (e.g., Microsoft Sentinel)

Cloud
On-premises sensors managed via Azure Security Center and connected to Microsoft Sentinel

Agentless security for unmanaged IoT/OT devices

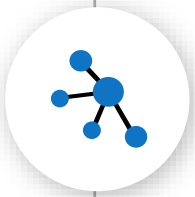
IoT/OT Asset Discovery

What devices do we have & how are they communicating?



Operational Efficiency

How do we identify the root cause of malfunctioning or misconfigured equipment?



Risk & Vulnerability Management

What are risks & mitigations impacting our crown jewel assets?

Continuous IoT/OT Threat Monitoring, Incident Response & Threat Intelligence

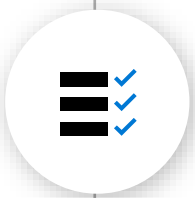
How do we detect & respond to IoT/OT threats in our network?

Unified IT/OT Security Monitoring & Governance

How do we break down IT/OT silos?

How do we leverage existing workflows & tools to centralize IT/OT security in our SOC?

How do we demonstrate to auditors that we have a safety- and security-first environment?



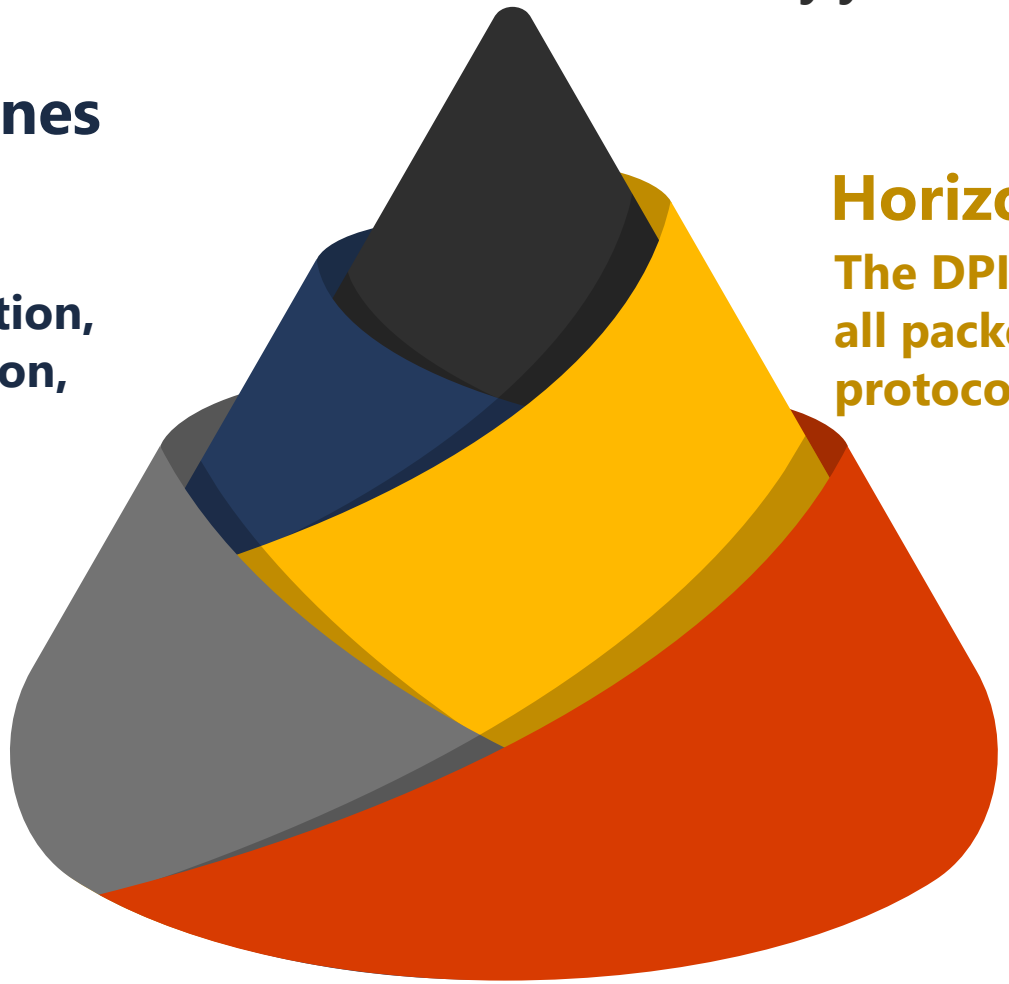
Defender for IoT – Data Flow View

Custom Alerts

Alerts that can be customized by you

Alerts engines

Malware,
Anomaly,
Protocol Violation,
Ppolicy Violation,
Operational



Horizon - DPI

The DPI layer that dissects all packets based on protocols / ports

Capture Filter

Filter traffic (include/exclude) based on IP's / subnets

NIC (Interface)

Connection to switches span ports / TAP devices

Notable customers across diverse verticals

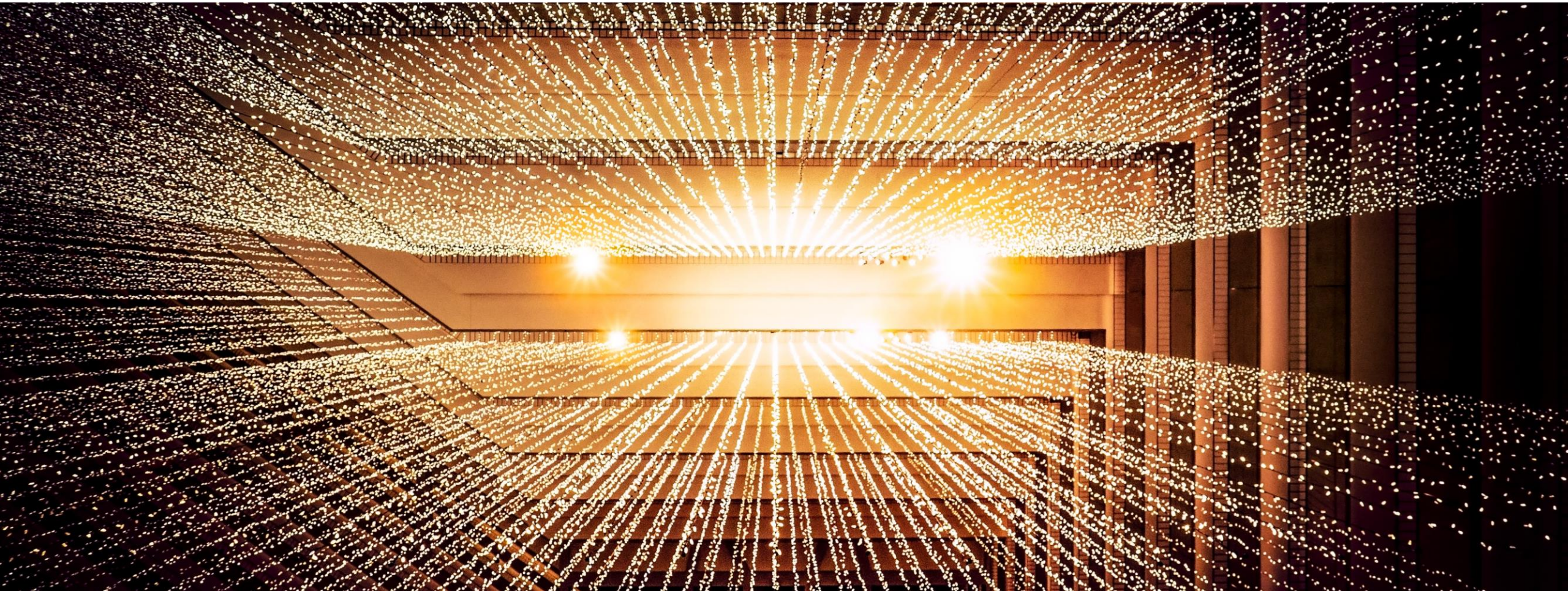
- Microsoft Azure data centers (BMS)
- 3 of the top 10 global pharmaceutical firms
- $40B Global Manufacturer
- $30B Automotive Manufacturer
- 3 of the top 10 US energy utilities
- Electric & gas utilities across EMEA & Asia
- $15B chemical company
- $23B oil & gas company
- $4B automotive parts manufacturer
- $7B CPG manufacturer
- $40B Japanese systems integrator
- F500 transportation manufacturer
- Largest US water district
- Government agencies including US DoE

Why D4IoT - Widest threat intel worldwide

As a result of more than 24 trillions daily security signals

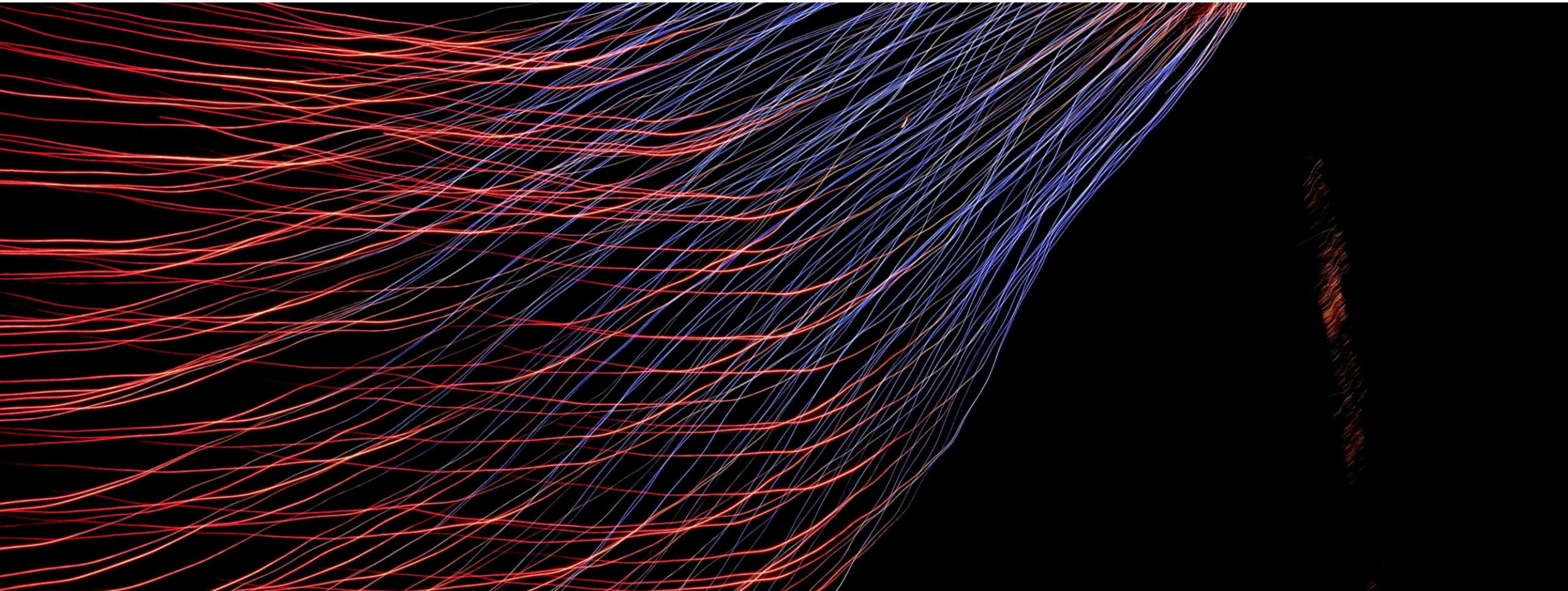
Why D4IoT – Cloud connectivity

Real time Threat Intel updates



Why D4IoT – Native Sentinel integration

Supports SIEM/SOAR



Why D4IoT – OT/ICS/IoT protocols support

Horizon SDK – Smart DPI layer

Why D4IoT – Ease of deployment

As fast as a site per day

Thank You