Microsoft

Securing PROTECTED-level workloads in Azure

22nd August 2018

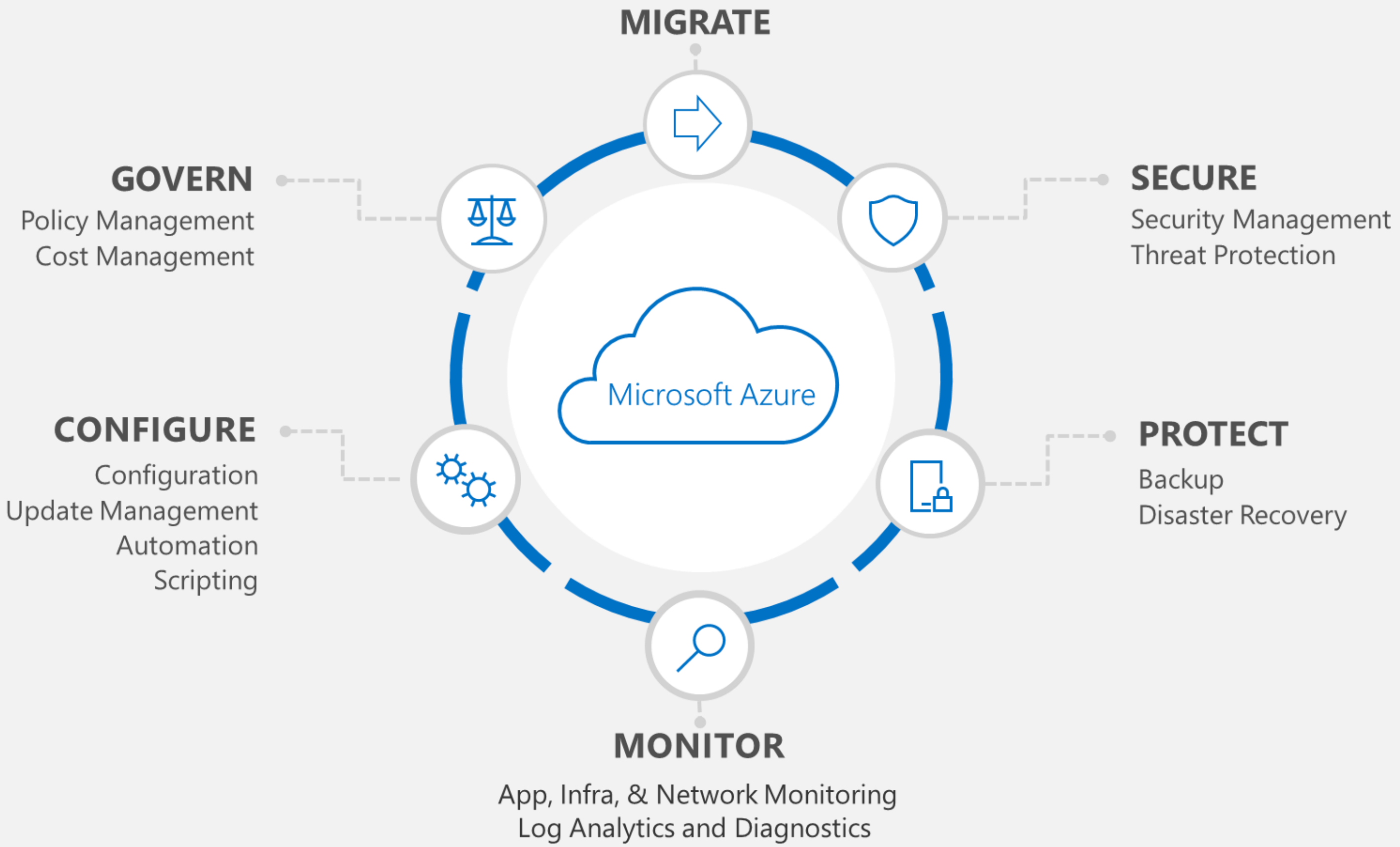
Nirmal Thewarathanthri

Cloud Solution Architect

Agenda

- Azure Security & Management Tools Overview
- Azure Security Centre
- DDOS Protection
- Demo
- Log Analytics
- Demo
- Q&A

Azure security & management tools



→ Built in

→ Intelligent

→ Hybrid

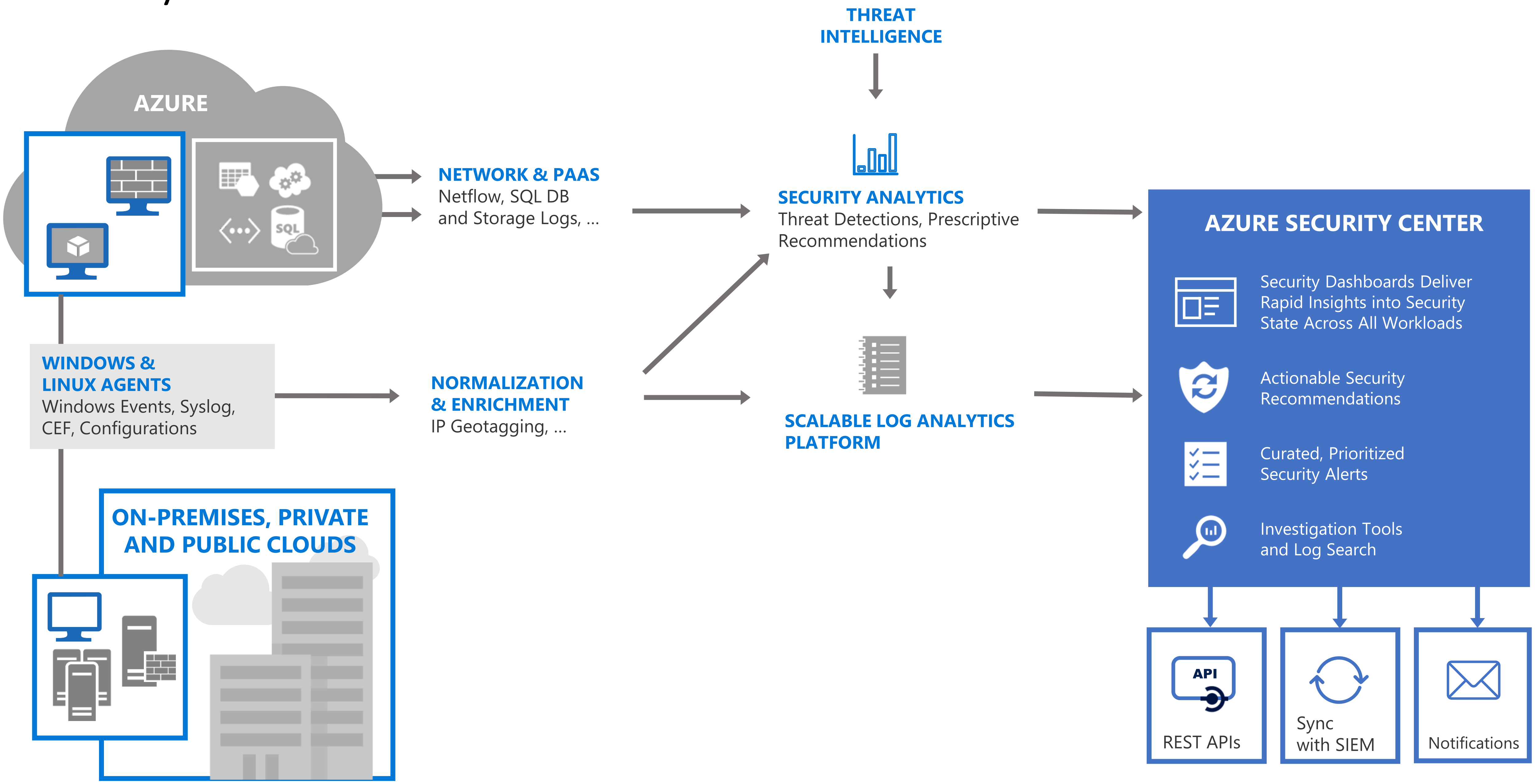
Unify security management and enable advanced threat protection for hybrid cloud workloads

Unified visibility and control

Adaptive threat prevention

Intelligent detection and response

Security Center Architecture



AZURE

NETWORK & PAAS
Netflow, SQL DB
and Storage Logs, …

WINDOWS &
LINUX AGENTS
Windows Events, Syslog,
CEF, Configurations

ON-PREMISES, PRIVATE
AND PUBLIC CLOUDS

NORMALIZATION
& ENRICHMENT
IP Geotagging, …

THREAT
INTELLIGENCE

SECURITY ANALYTICS
Threat Detections, Prescriptive
Recommendations

SCALABLE LOG ANALYTICS
PLATFORM

AZURE SECURITY CENTER

Security Dashboards Deliver
Rapid Insights into Security
State Across All Workloads

Actionable Security
Recommendations

Curated, Prioritized
Security Alerts

Investigation Tools
and Log Search

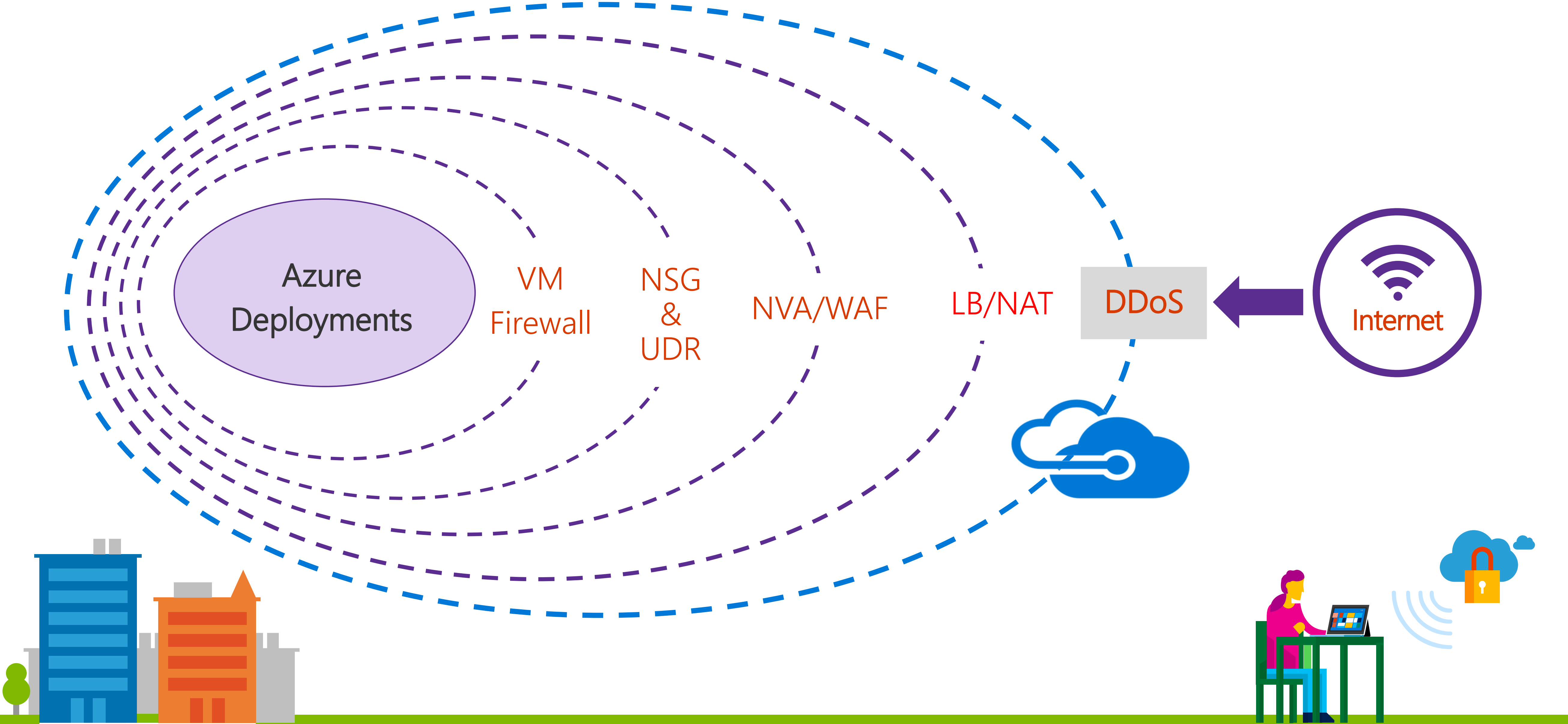
REST APIs

Sync
with SIEM

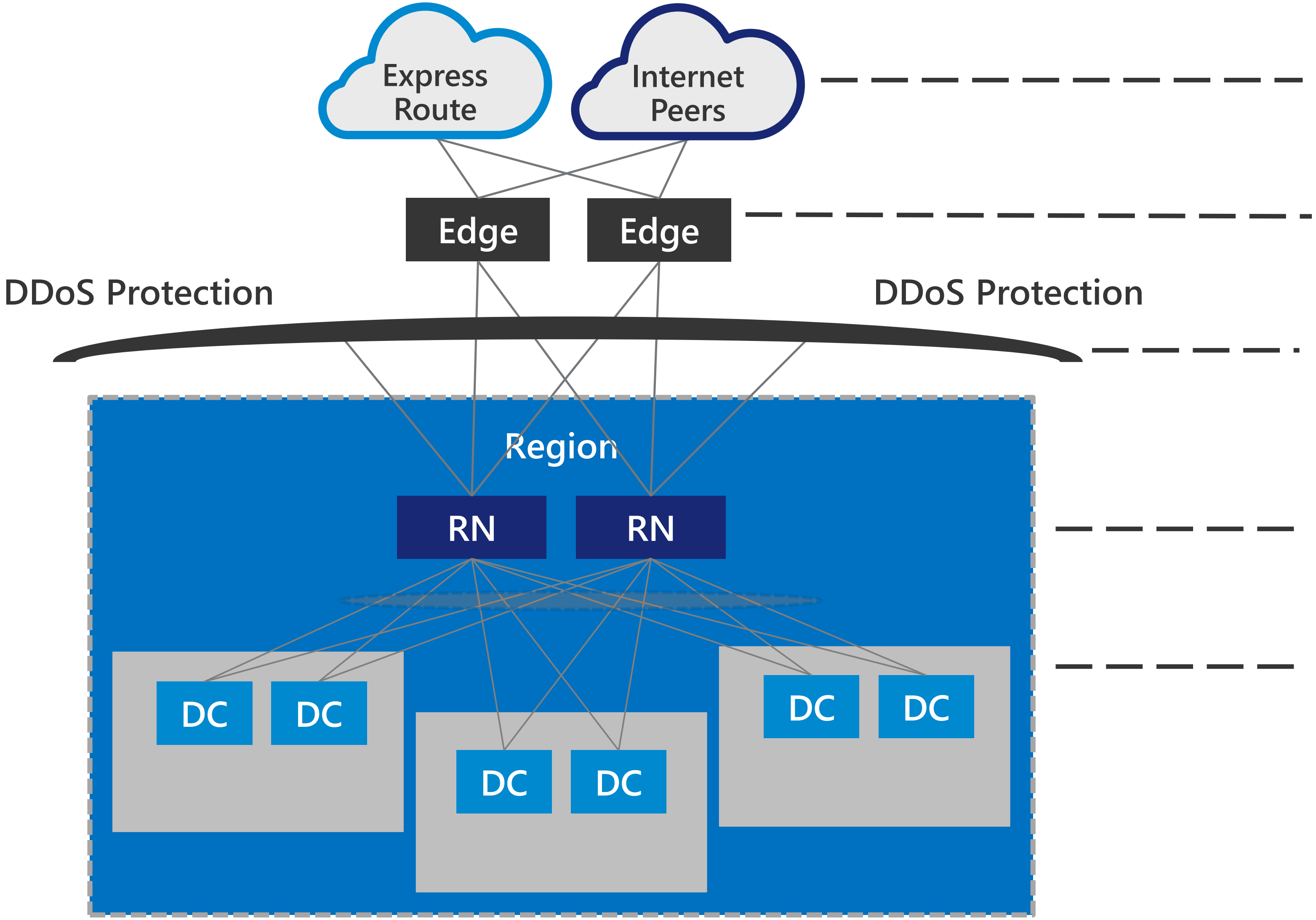
Notifications

Azure Security Centre Demo

Defense in Depth for Virtual Networks



Azure DDoS System Overview



Global mitigation platform

Continuous monitoring

Edge mitigation protects datacenter bandwidth

Global distribution of attack traffic

Regional failover

Azure

Always on monitoring

Office365

Enterprise availability

XBOX

Massive attacks defended

DDOS Protection Demo

The view from above

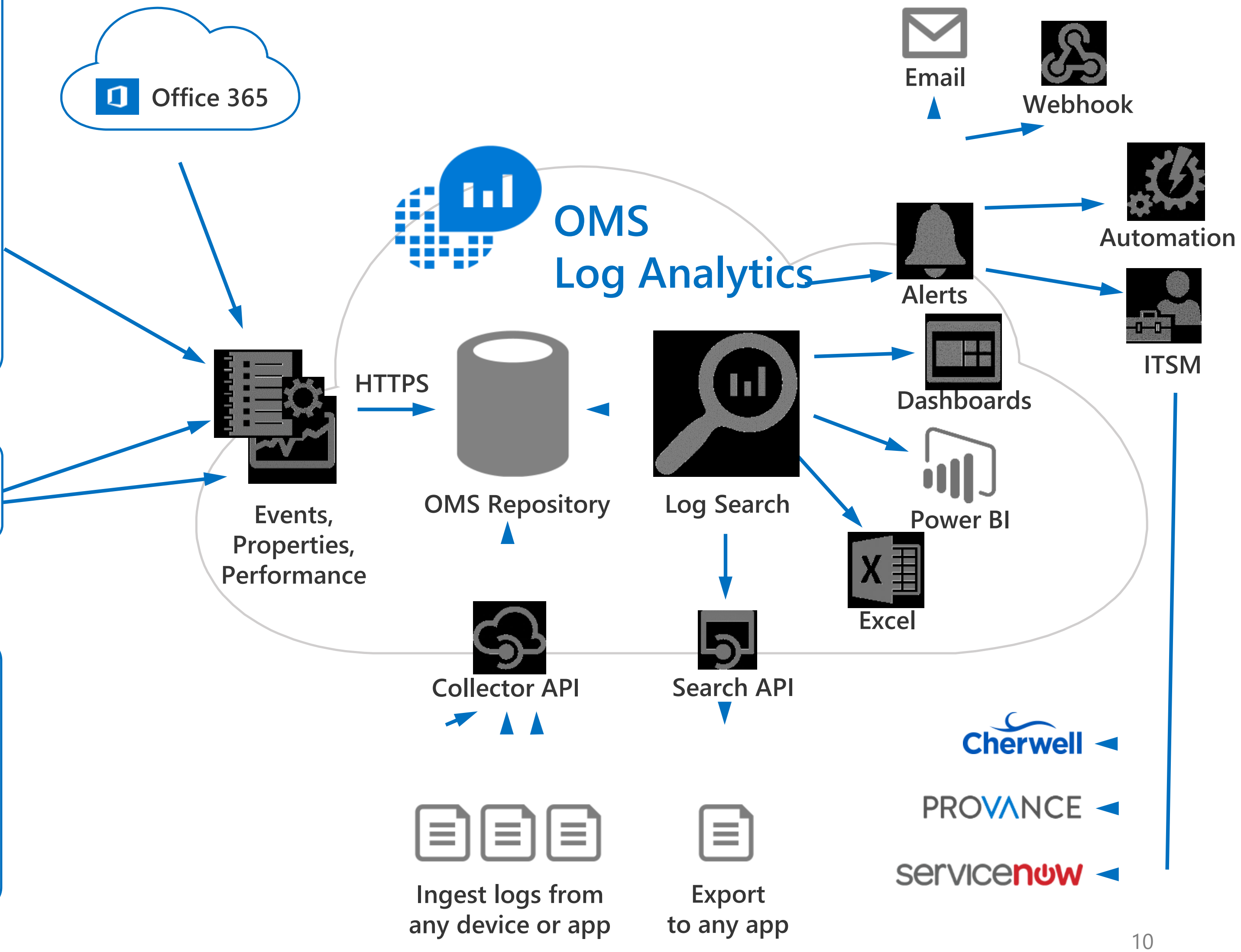
Azure

- Activity Log
- Application Gateway
- Application Insights
- Automation
- Batch Service
- Cognitive Services
- Containers
- Data Lake Store
- Event Hubs
- HDInsight HBase
- IoT Hub
- Key Vault
- Load Balancer
- Logic App
- Network Security Group
- Search
- Service Bus
- Service Fabric Cluster
- SQL Database
- Web App/Farm

Hybrid, On-Premises, Any Cloud

- CentOS
- Debian
- Oracle
- RHEL
- Ubuntu
- SLES
- Windows

- Active Directory
- Antimalware
- Capacity & Performance
- Change & File Tracking
- Network Performance
- Operations Manager
- Security & Audit
- Service Map
- SQL Server
- Update Management
- VMWare Monitoring
- Wire Data



Office 365

OMS Log Analytics

Events, Properties, Performance

HTTPS

OMS Repository

Log Search

Email

Webhook

Automation

Alerts

ITSM

Dashboards

Power BI

Excel

Collector API

Search API

Ingest logs from any device or app

Export to any app

Cherwell

PROVANCE

servicenow

Azure Log Analytics Demo

Built-in intelligence and advanced analytics

Threat intelligence

Looks for known malicious actors using Microsoft global threat intelligence

Partners

Integrates alerts from partner solutions, like firewalls and antimalware

Anomaly detection

Uses statistical profiling to build historical baselines

Alerts on deviations that conform to a potential attack vector

Behavioral analytics

Looks for known patterns and malicious behaviors

Fusion

Combines events and alerts from across the kill chain to map the attack timeline

Powered by Microsoft Intelligent Security Graph

Resources

https://docs.microsoft.com/en-us/azure/security-center/security-center-intro

https://docs.microsoft.com/en-us/azure/security/azure-ddos-best-practices

https://docs.loganalytics.io/index

https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-overview

https://aka.ms/23082018 for Demo Content & Slides

Microsoft

Q&A