Microsoft Security Solutions
What Are They Good For?

OWEN ALLEN, SOLUTION ARCHITECT, BLUEVOYANT
29 OCTOBER 2021, ISSA-PITTSBURGH CHAPTER
SECURITY FORUM 2021
Microsoft as a Vendor

**Infrastructure**
- Azure
- Stack HCI
- Azure SQL
- Data Factory
- AKS
- Azure Function
- CosmosDB
- Github
- DevOps
- Monitor
- Azure Arc
- Windows Server 2022
- Windows 11
- Windows 365

**Productivity**
- Outlook
- Word
- Excel
- PowerPoint
- SharePoint
- Teams
- PowerBI
- PowerApps
- Dynamics365
- Exchange Online
- OneDrive

**Security**
- Azure Sentinel
- Azure Active Directory
- Endpoint Manager
- Cloud App Security
- Azure Security Center
- Defender for Endpoint
- Defender for Office 365
- Defender for Identity
- Defender for MCAS
- Defender for Microsoft 365

**Compliance**
- Trainable classifiers
- Endpoint
- on-prem and cloud Data Loss Prevention
- Insider Risk Management
- Compliance Manager
- Communication Compliance
Customer Demands

“I don’t want data leaving my environment”

“I want to consolidate my core security tools”

“I need help controlling my cloud consumption costs”

“I want my entire security stack managed”

“I want to zap the attachment in email before it gets downloaded to the endpoint”

“I need to stop malicious activity in my cloud workloads”
Attackers are Like Water

Attackers take path of least resistance to achieve objectives

Established paths/methods  Easiest new openings

Attackers are goal-oriented and technology agnostic, using any type of attack that works. They don’t care if you spent tons of money on Splunk, FireEye, Cisco, CrowdStrike, or Microsoft security solutions.

With few exceptions, the slowest antelope get consumed first.

No target is “off limits”.

HIGHLY CONFIDENTIAL
Why are We Having a Zero Trust Conversation?

Keep Assets away from Attackers

“Trusted Network” Security Strategy
- Initial attacks were network based
- Seemingly simple and economical
- Accepted lower security within the network

IT Security is Complex
Many Devices, Users, & Connections

Assets Increasingly Leave the Network
BYOD, WFH, Mobile, and SaaS

Attackers Shift to Identity Attacks
- Phishing and credential theft
- Security teams often overwhelmed
Secure assets where they are with Zero Trust

Simplify security and make it more effective

Classic Approach
Restrict everything to a ‘secure’ network

Zero Trust
Protect assets anywhere with central policy
Zero Trust

**Strategy to Increase Security** Assurances

*for business assets* data and applications

*everywhere* including public & untrusted networks

---

**User Access**

Policy Driven Access Architecture for Productivity Environment

- Explicitly validate trust of access requests
- Dynamically address insufficient trust

**Modern SecOps**

Pervasive detection and response

- Deep asset visibility inside & outside the firewall
- Rapid remediation with automation and integrated workflows

**OT and Datacenter**

Monitor and segment assets by business risk

- Workload, App, API, and Device Security
- Operational Technology (OT) + Industrial Internet of Things (IIoT)

---

Increases Security

Increases Productivity
Microsoft Zero Trust Principles

Guidance for technical architecture

**Verify Explicitly**
Always validate all available data points including
- User **identity** and **location**
- Device **health**
- Service or **workload** context
- Data classification
- Anomalies

**Use Least Privilege Access**
To help secure both data and productivity, limit user access using
- Just-in-time (JIT)
- Just-enough-access (JEA)
- Risk-based **adaptive** polices
- Data protection against **out of band** vectors

**Assume Breach**
Minimize blast radius for breaches and prevent lateral movement by

- **Segmenting access** by network, user, devices, and app awareness.
- **Encrypting** all sessions end to end.
- **Use analytics** for threat detection, posture visibility and improving defenses
**Compromised Endpoint**

**Risk:** Devices can be infected by personal email, USB, and other vectors

**Mitigation:** Rapidly detect and clean all managed devices, email, and other resources across environment and customers

- Open attachment from personal email
- Malicious payload detected
- Microsoft Defender for Endpoints
  - Disable user access from device while infected
- Share intelligence
  - Microsoft Threat Intelligence
- Share telemetry and remediate infected endpoints.
- Microsoft Defender for O365
  - Search companywide email and remove attachment from affected mailboxes
  - Block the attachment from future attacks
Attacker's Have Options

To compromise privileged access

Privileged Access

User Access

Potential Attack Surface
Limit and protect pathways to privileged access

Prevention and rapid response

Privileged Access

- Devices/Workstations
- Account
- Intermediaries
- Interface

User Access

- Devices/Workstations
- Account
- Intermediaries
- Interface

Complete End-to-end approach
Required for meaningful security

Asset Protection also required
Security updates, DevSecOps, data at rest / in transit, etc.

Business Critical Assets
Across On-Premises, Cloud, OT, & IoT

Identity Systems

- Ping
- CYBERARK
- Okta

Cloud Service Admin

- AWS
- SailPoint

Business Critical Systems

- ABB
- Honeywell
Suspend access during compromise

**Risk:** Devices can be infected by personal email, USB, and other vectors

**Mitigation:** Rapidly detect and clean all managed devices, email, and other resources across environment and customers
Defend Across Attack Chains

Insider and external threats

Defender for Office 365
- Phishing mail
- Open attachment
- Click a URL
- Browse a website

Defender for Endpoint
- Exploitation and Installation
- Command and Control

Azure AD Identity Protection
- Brute force account or use stolen account credentials
- User account is compromised
- Attacker attempts lateral movement
- Privileged account compromised

Microsoft Cloud App Security
- Attacker accesses sensitive data
- Attacker collects reconnaissance & configuration data

Exfiltration of data

Azure Defender
- History of violations
- Distracted and careless
- Disgruntled or disenchanted
- Subject to stressors

Leading Indicators
- Insider has access to sensitive data
- Anomalous activity detected

Insider Risk Management
- Data leakage
- Potential sabotage
Cross-cloud and cross-platform

Comprehensive Security, Compliance and Identity capabilities that integrate with your existing solutions

Industry Partnerships

- NIST / CIS / The Open Group / Others
- Microsoft Intelligent Security Association
- Solution Integration and MDR/MSSP Partners
- CERTs / ISACs / Others
- Law Enforcement

Microsoft Security, Compliance, and Identity Capabilities

- **Access Control**
  - Identity and Network

- **Modern Security Operations**
  - Rapid Resolution with XDR, SIEM, SOAR, UEBA and more

- **Asset Protection**
  - Information Protection and App Security / DevSecOps

- **Technical Governance**
  - Risk Visibility, Scoring, and Policy Enforcement

**People Security** – User Education/Empowerment and Insider Threats

**Endpoints & Devices**

**Software as a Service (SaaS)**

**Hybrid Infrastructure** – IaaS, PaaS, On-Premises

**Security Operations [Center] (SOC)** – Reduce attacker time/opportunity to impact business

**IoT Devices**

Operational Technology (OT)

Microsoft Security, Compliance, and Identity Capabilities

- **Threat Intelligence** – 8+ Trillion signals per day of security context
## Multi-Cloud and Cross-Platform Technology

Secure the enterprise you have

### Microsoft Information Protection and Azure Purview

Discovery, Classify, Protect, and Monitor unstructured data (documents, spreadsheets, files, etc.), structured data (SQL, Databases, etc.) and identify critical risks (Open S3 buckets, SaaS Sharing Risks, etc.)

<table>
<thead>
<tr>
<th>Identity &amp; Access</th>
<th>Information Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identity Enablement</strong></td>
<td>Access cloud and legacy applications for Enterprise users, Partners (B2B), and Customers/Citizens (B2C)</td>
</tr>
<tr>
<td><strong>Azure Active Directory</strong></td>
<td>Zero Trust Access Control using Behavioral Analytics, Threat Intelligence, and integration of device and app trust signals</td>
</tr>
</tbody>
</table>

### Hybrid Infrastructure – IaaS, PaaS, On-Premises

<table>
<thead>
<tr>
<th>Software as a Service (SaaS)</th>
<th>Security Operations [Center] (SOC)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GitHub Advanced Security – Secure development capabilities</strong></td>
<td><strong>Microsoft 365 Defender</strong></td>
</tr>
<tr>
<td><strong>Microsoft Endpoint Manager</strong> Unified Endpoint Management (UEM)</td>
<td><strong>Microsoft Cloud App Security</strong></td>
</tr>
<tr>
<td><strong>Hybrid Infrastructure – IaaS, PaaS, On-Premises</strong></td>
<td><strong>Extended Detection and Response (XDR)</strong></td>
</tr>
<tr>
<td><strong>On-Premises</strong></td>
<td><strong>Threat visibility and capabilities tailored to resources</strong></td>
</tr>
<tr>
<td><strong>IaaS</strong></td>
<td><strong>Threat &amp; Vulnerability Management</strong></td>
</tr>
<tr>
<td><strong>AWS</strong></td>
<td><strong>Threat Detection &amp; Response</strong></td>
</tr>
<tr>
<td><strong>PaaS</strong></td>
<td><strong>Policy Audit &amp; Enforcement</strong></td>
</tr>
<tr>
<td><strong>Continuous Cross-Platform Cloud Security Posture Management (CSPM) and Cloud Workload Protection (CWPP)</strong></td>
<td><strong>Threat analytics on top attacks</strong></td>
</tr>
</tbody>
</table>

### IoT Devices

| Azure Sentinel – Cloud Native SIEM, SOAR, and Ueba for IT, OT, and IoT |
|--------------------------|--------------------------|
| **Azure Defender** | XDR for IaaS, PaaS, and On-Premises |
| **Azure Defender for IoT** | **Threat & Vulnerability Management** |
| | **VMs, Servers, App Environments** |
| | **Storage and Databases** |
| | **Containers and Orchestration** |
| | **and more** |

### Operational Technology (OT)

<table>
<thead>
<tr>
<th><strong>Azure Arc</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threat Intelligence – 8+ Trillion signals per day of security context</strong></td>
</tr>
</tbody>
</table>

---

May 2021 – [https://aka.ms/MCRA](https://aka.ms/MCRA)
Security Operations Model – Functions and Tools

Threat Intelligence

Strategic and Business Threat Insights/Trends

- Hunt (TIER 3)
  Proactive Hunting, Advanced Forensics, and Detection Tuning
  Any/All tools, data, intelligence sources

Investigation (TIER 2)
Advanced Analysis and Remediation

- Primary Tools: XDR (Microsoft 365 Defender & Azure Defender)

Triage (TIER 1)
Rapid Remediation or Escalation

- Primary Tools: XDR (Microsoft 365 Defender & Azure Defender)

AUTOMATION
Automated Investigation & Remediation

Tactical Threat Trends and Indicators of Compromise (IOCs)

Incident Management
Business Coordination
Assess Impact & Manage Stakeholders

Major Incident

High Complexity Incidents
- Escalations & multi-stage incidents
- Alerts on business-critical assets
- Monitoring known campaigns

High Volume Incidents
- High true positive rate
- Consistent/predictable

Well known attacks
- XDR (Microsoft 365 Defender and Azure Defender) Alerts

External Intelligence Sources

Partner Teams
IT Operations, DevOps, & Insider Threat, and more

CDOC Example Alert Ratio:
- XDR Alerts (~65%)
- User Reporting (~10%)
- Log/Event/Other (~25%)
Microsoft Threat Intelligence

Built on diverse signal sources and AI

- **Trillions of signals**
- **Billions of predictions**
- **Millions of actions**

**Microsoft Cloud**
Machine learning and AI systems

- **1.2B+** PCs, servers, and IoT
- **1.8PBs** Other clouds and network logs
- **1B+** Apps and service users
- **470B+** Emails analyzed
- **630B+** Identities authenticated
- **4.1B+** Meeting minutes delivered
- **5B+** Threats blocked
- **600B+** Documents scanned
- **18M+** URLs scanned
- **470B+** Emails analyzed
- **630B+** Identities authenticated
- **4.1B+** Meeting minutes delivered
- **5B+** Threats blocked
- **600B+** Documents scanned
- **18M+** URLs scanned
- **470B+** Emails analyzed
- **630B+** Identities authenticated
- **4.1B+** Meeting minutes delivered
- **5B+** Threats blocked
- **18M+** URLs scanned
- **1B+** Apps and service users

iOS, macOS, Android, Linux and IoT devices

- **1.2B+** PCs, servers, and IoT
- **1.8PBs** Other clouds and network logs
- **1B+** Apps and service users
- **470B+** Emails analyzed
- **630B+** Identities authenticated
- **4.1B+** Meeting minutes delivered
- **5B+** Threats blocked
- **600B+** Documents scanned
- **18M+** URLs scanned
- **470B+** Emails analyzed
- **630B+** Identities authenticated
- **4.1B+** Meeting minutes delivered
- **5B+** Threats blocked
- **600B+** Documents scanned
- **18M+** URLs scanned
- **470B+** Emails analyzed
- **630B+** Identities authenticated
- **4.1B+** Meeting minutes delivered
- **5B+** Threats blocked
- **18M+** URLs scanned
- **1B+** Apps and service users
Inside View of Microsoft Threat Intelligence

DATA COLLECTION AND ANALYSIS

Products instrumented to strict privacy/compliance standards
See Microsoft Trust Center

Analytics help fuel new discoveries
Products make data available
Products use Interflow APIs to access results
Products generate data which feeds back into system
Humans identify attacks, improve analytics, feed back into databases and product design
Silos are the Bane of Security Operations

Defender Silos make chasing them difficult

Attackers traverse rapidly across the enterprise

Integrating Silos is Challenging

MAPPING CHALLENGES
Tools Pivot on Different Attributes
- Network IP address
- Computer Name
- Documents
- Device ID
- Email
- Etc.

STRONG BIASES/TENDENCIES
Identity
- Reports only high-quality alerts because
  - Analysts have alert fatigue, resist new tools
  - Analysts have network background and value of Identity isn’t self evident

Endpoint
- Verbose alert reporting
  - AV testing focuses on “not missing” malware
  - Reporting more improves showing in AV Testing reports
Microsoft Strategy | Microsoft Defender

SIEM
Azure Sentinel

Multi-cloud

3rd party and partners

Data
Endpoints

Users
Apps

SQL
Server VMs
Containers

Network Traffic
IoT
Azure App Services

365 Defender

Azure Defender

Extended Detection and Response (XDR)
Converging Tools & Data

Engineering a single seamless system with automation

- Single Portal Experience
- Playbook Automation
  Ensure automation runs across all systems
- Semantics and Meaning
  Correlation, prioritization, orchestration, etc.
- Unified entity definitions
  Reputation for Users, machines, email, IPs, etc.
- Signal sharing
- Intelligent Capabilities
  High Quality Detection and Data

Microsoft 365 Defender
- Incidents, investigations, threat hunting, threat analytics

Portal Integration

Azure Sentinel

Identity
Endpoint
Email & Collab
Applications
Others

MAY 2021 – https://aka.ms/MCRA

HIGHLY CONFIDENTIAL | 24
M365 E5 Value Proposition

“Best of Suite”
$57.00 user/month

Infrastructure
Windows 11 & Endpoint Manager

Productivity
Office 365

Security
(4) Defenders & Azure AD

Compliance
Microsoft Information Protection, Insider Risk, & Compliance Manager

Identity & Access Management
- Single Sign-on
- Multi-Factor Authentication
- Access Control
- Privileged Access Management (PAM)
- Secret Management

Information Protection
- Data Loss Prevention (DLP)
- Data Encryption
- Information Protection
- Data Classification
- Data Governance
- Cloud Access Security Broker (CASB)
- Key Management
- Mobile Application Management
- Database Security
- Encrypted Cloud Storage
- Back Up
- Disaster Recovery
- Virtual/Private Networks (VPN)

Threat Protection
- Secure Email Gateway
- Endpoint Detection and Response (EDR)
- Endpoint Protection (EPP)
- Anti-malware/piriforming
- Anti-spyware
- Antivirus Software
- User and Entity Behavior Analytics (UEBA)
- Anomaly Detection
- Threat Intelligence Feeds
- Remote Browser
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- IOT Protection
- Cloud Workload Protection
- EDG Protection
- Incident Response Services

Security Management
- Security Scoring
- Reporting
- Cloud-based Management
- Asset Discovery
- Pen Testing/ Risk Assessment
- Vulnerability Assessment
- Web Application Testing
- Managed detection and response (MDR)
- SOC
- Security training
- SIEM (SIM/ SEM/ Log management)
M365 E5 Security Add-on for E3 Value Proposition

“Best security bundle for 365 customers”

NGAV+EDR-Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is a security platform that empowers infosec teams to prevent with mature endpoint security policy sets, detect with custom KQL detections, investigate with graphs & alert stories, and mitigate & respond to advanced threats with integrated risk & exposure assessments and built-in automation actions.

CASB-Microsoft Cloud App Security

Deeply integrated with Azure AD and the Defender products, MCAS controls Microsoft native applications and the most popular SSO applications and public cloud providers. MCAS helps identity shadow IT usage and restrict usage via unsanctioning and app control.

IAM-Azure AD

Microsoft Defender for Endpoint is a security platform that empowers infosec teams to prevent with mature endpoint security policy sets, detect with custom KQL detections, investigate with graphs & alert stories, and mitigate & respond to advanced threats with integrated risk & exposure assessments and built-in automation actions.

Communication Security-Defender for Office 365

Microsoft Defender for Office 365 is a cloud-based email filtering service that helps protect your organization against advanced threats to email and collaboration tools, like phishing, business email compromise, and malware attacks.

ADDS Monitoring-Defender for Identity

Microsoft Defender for Identity is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
M365 E5 Security Add-on for E3 Value Proposition

“Best security bundle for 365 customers”

**NGAV+EDR-Microsoft Defender for Endpoint**

Microsoft Defender for Endpoint is a security platform that empowers infosec teams to prevent with mature endpoint security policy sets, detect with custom KQL detections, investigate with graphs & alert stories, and mitigate & respond to advanced threats with integrated risk & exposure assessments and built-in automation actions.

**CASB-Microsoft Cloud App Security**

Deeply integrated with Azure AD and the Defender products, MCAS controls Microsoft native applications and the most popular SSO applications and public cloud providers. MCAS helps identity shadow IT usage and restrict usage via unsanctioning and app control.

**IAM-Azure AD**

Microsoft Defender for Endpoint is a security platform that empowers infosec teams to prevent with mature endpoint security policy sets, detect with custom KQL detections, investigate with graphs & alert stories, and mitigate & respond to advanced threats with integrated risk & exposure assessments and built-in automation actions.

**Communication Security-Defender for Office 365**

Microsoft Defender for Office 365 is a cloud-based email filtering service that helps protect your organization against advanced threats to email and collaboration tools, like phishing, business email compromise, and malware attacks.

**ADDS Monitoring-Defender for Identity**

Microsoft Defender for Identity is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
Who is BlueVoyant?


At BlueVoyant, we recognize that effective cybersecurity requires active prevention and defense across both your organization and supply chain. Our proprietary data, analytics and technology, coupled with deep expertise, works as a force multiplier to secure your full ecosystem.

Exemplary Leadership
Co-Founded in 2017 by F500 Executives and Former officials NSA, FBI, Unit 8200, and GCHQ, together with private sector experts

Global Footprint
New York City (Headquarters), Maryland, Tel Aviv, San Francisco, London, Manila and Latin America

Leadership, Experience, Global Presence
BlueVoyant | Services

Managed Detection and Response Services
- Consulting and Implementation Services
- MDR for Azure Sentinel
- MDR for 365 Defender
- MDR for Endpoint
- Splunk Security Services

Professional Services
- Full-Service Incident Response
- Consulting Services
  - Cyber Maturity Assessment
  - Cyber Consulting Retainers
  - Incident Response Planning
  - Penetration Testing
  - Vulnerability Management Services

Digital Risk Protection
- Global Cyber Threat Detection
- Predictive Analysis
- BIN Watcher™
- Watcher™
- Credential Watcher™
- Executive Cyber Guard

3rd Party Cyber Risk Management
- Comprehensive Assessments and Monitoring
- Risk Improvement
- Supply Chain and Third-Party Risk Management
Thank You

Owen Allen
owen.allen@bluevoyant.com
+1 425-442-9272
@owenallen