Vik Verma

High Level Cybersecurity Architecture

Azure Sentinel

M365 Defender (Microsoft Threat Protection)

Azure Defender (Azure Security Center)

MONITOR

IoT　　SQL　　Server

Connectors, CEF Import, Syslog Import

Defender for Identity (Azure ATP)

Azure AD Premium

Cloud App Security

Defender for O365 (OATP)

Office 365

Defender for Endpoints (MDATP)

Unified Identity Protection

Microsoft Info Protection

Microsoft Endpoint Manager (Intune)

SECURE

On-prem active sensors

Protect　　**Manage**

Identity
| AD | Azure AD | Social ID |

Data
| On Prem | Endpoints & Servers | Cloud Storage |

Devices
Win 10	iOS
Autopilot	**Android**
Attack Surface Reduction	**Mac**
Next Gen Protection	**Servers**

IoT / OT Network
Mgmt Console
Sensors
Air Gap
Equipment

Azure SQL DB Resources

VM and Other Resources

Network & Other 3rd Party Appliances

CONSOLIDATE