Vik Verma (LinkedIn)

Zero Trust Mindset - Provide only sufficient permissions for the job. Instead of believing everything behind corporate firewall is safe, start with assumption that the request is coming from unsafe conditions and then find reasons to trust. Leverage each of below six foundational elements as a source of signals as well as plane of enforcement.

	1 Identity	2 Endpoints	3 Data	4 Apps	5 Infra	6 Network
	People, service principals, device identities	Apply device security principles regardless of ownership, device type or connection.	Inventory, classify and protect data.	Legacy, Cloud migrated, and SaaS apps.	Manage and protect all IT infra - hardware, apps, and serverless	Segment the network, monitor and restrict permitted traffic.
Verify explicitly	• Federate on-premises identity with Cloud (Azure AD) • Put Azure AD in the path of every access request • Verify explicitly with strong auth	• Register all endpoints – corporate, contractor and personal. • Create policies to measure endpoint health. • Enable password-less logon to devices	• Define enterprise data classification taxonomy. • Define default labels and protection policies. • Automatically classify content and encrypt where needed. • Leverage pattern matching and template-based identification.	• Discover apps and in-app activities. • Identify usage pattern and evaluate risk exposure	• Leverage security baselines • Use RBAC to centrally govern access	• Segment network by workload and control ingress/egress points. • Create subnets and allow required traffic between workload components.
Least Privilege Principle (Limit Default Permissions)	• Identify and secure privileged identities. • Control the app consent process. • Entitlement management • Streamline identity lifecycle	• Leverage role-based endpoint DLP to restrict untrusted actions. • Restrict access to apps and data based on risk status	• Implement DLP policies across services and repositories. • Remove permissions, block or encrypt files based on scenario	• Tag and sanction / un-sanction apps as needed. • Session control apps to prevent risky behavior	• Enable JIT resource access • Enforce policies for resource creation and in-guest config. Standardize policies across premises. • Create deployment package and standardise resource creation	• Implement firewall to monitor and protect. • Only allow HTTPS traffic to internet facing services and encrypt VPN traffic. • Limit public access to VM. Connect with RDP / SSH. • Implement DDoS protection • Restrict cross-app traffic to private IP space
Assume Breach	• Monitor identity risk and integrate with overall secops • Leverage password-less authentication • Use runtime behaviour to control access (Allow, Block or Limit) • Implement holistic threat monitoring and response	• Monitor device risk and include in threat management practice. • Measure device health posture and evaluate exposure risk • Automate prompt response for known threats.	• Track and monitor usage of sensitive data • Create policies to take prompt actions under suspicious conditions • Include content sensitivity and asset value in threat assessment process	• Block or monitor un-sanctioned apps. • Apply governance actions for targeted activities • Monitor for anomalous usage (e.g. spike in download) and create block / alert policy • Leverage progressive access evaluation	• Establish rules for monitoring resource creation and raising alerts • Monitor access and detect identity threats	• Monitor app traffic and use ML to baseline normal traffic behaviour. • Create alerts for anomalous traffic and apply automatic mitigation

7

- Establish visibility and Proactive detection
- Enable Automatic Detection and Response (AIR)

Footnotes:

1.1 Provide a single-identity experience across all users - internal and external (B2B and Consumers)
Connect apps to Azure AD for SSO App registration and prevents users from leaving copies of their credentials in various apps.
Streamline permission provisioning in LOB apps by using Outbound Provisioning (SCIM).
Connects devices to Azure AD to enable modern management of devices.

1.2 Strengthen identity security by leveraging identity protection features (such as conditional access). Reduce identity attack surface by blocking legacy authentication.
Control the risk of users giving access to insecure apps by restricting and managing user consent process.
Identify & Protect organisationally (user admin, compliance admin) and functionally privileged identities (application owner, developer with prod pipeline access).

1.3 Setup monitoring and auditing process for authentication and identity setup changes
Plan a passwordless authentication deployment with Azure AD
Get more granular session/user risk signal and automate response with Identity Protection.
Enable MCAS monitoring to enrich the identity signals.
Enable Azure ATP integration with Microsoft Cloud App Security to bring on-premises signals into the risk signal and check the combined Investigation Priority score for holistic monitoring.

2.1 Register all endpoints to ensure security policies are rolled out and maintained in seamless fashion
Control access so that only cloud-managed and compliant endpoints can access apps and data.
Enable secure password login with *Windows Hello for Business*

2.2 Control flow of confidential data with Data loss prevention (DLP) policies and app protection
Access control is gated on endpoint risk for both corporate devices and BYOD.
Configure remote device update management and distribution

2.3 Get visibility to device health posture and exposure
Use Endpoint threat detection to monitor device risk.
Defend against never-before-seen and polymorphic threats with Defender for Endpoint

3.1 Define your Data Classification and Sensitivity Label Taxonomy
Create policies to automatically classify and label content
Leverage machine learning to go beyond pattern matching to identify sensitive content.

3.2 Govern access to data based on automatically assigned permissions.
Prevent data leakage through DLP policies based on a sensitivity label and content inspection.

3.3 *Audit data to understand user labeling, classification, and protection behaviors*
Integrate with Defender for Endpoint to include content sensitivity in threat value evaluation
Leverage Information protection in Windows for Endpoint content summary and monitoring

4.1 Connect apps to get visibility and control
Integrate with Microsoft Defender ATP to immediately start collecting data on cloud traffic across your Windows 10 devices, on and off your network.

4.2 Evaluate compliance and analyse usage
Leverage MCAS to discover and protect sensitive information in your organization
Protect apps with controlled session under risky conditions

4.3 Detect suspicious user activity with behavioral analytics (UEBA)
Dive deeper to identify risky apps and activities
Control cloud app usage by creating policies

5.1 Start with Azure Security Benchmark V2 to improve the security of workloads, data, and services.
Enforce rules for compliance with business standards using Policy Built-Ins

5.2 Create custom policies to enforce resources creation standards. Incorporate Guest Configuration policies.
Establish a Protect the Administrator program
Use Azure Arc to implement cross-premise configuration standards

5.3 Azure Blueprints to govern how resources are deployed, ensuring that only approved resources can be deployed
Enable Azure Defender to monitor and protect resources and enforce enrollment with policies
Follow Azure security best practices

6.1 Follow common design patterns for segmenting your network according to the Zero Trust model.
Add virtual network subnets so that discrete components of an application can have their own perimeters.

6.2 Use Azure Web Application Firewall (WAF) with default ruleset. Cover OWASP top 10 and create other custom rules.
Use WAF with Azure Front door for global load balancing, and Application gateway for in region resource load balancing.
Turn on Azure DDoS Protection Standard to protect from volumetric network layer attacks.
Use the PrivateLink connectivity with Azure PaaS services to keep all data exchanges over the private IP space.

6.3 Azure Network Watcher | Microsoft Docs

7 Establish visibility by enabling Microsoft Threat Protection
Set up rules for Automated Investigation and Remediation.
Connect MTP, other Microsoft data connectors, and relevant third-party products to Azure Sentinel in order to provide a centralized platform for incident investigation and response.