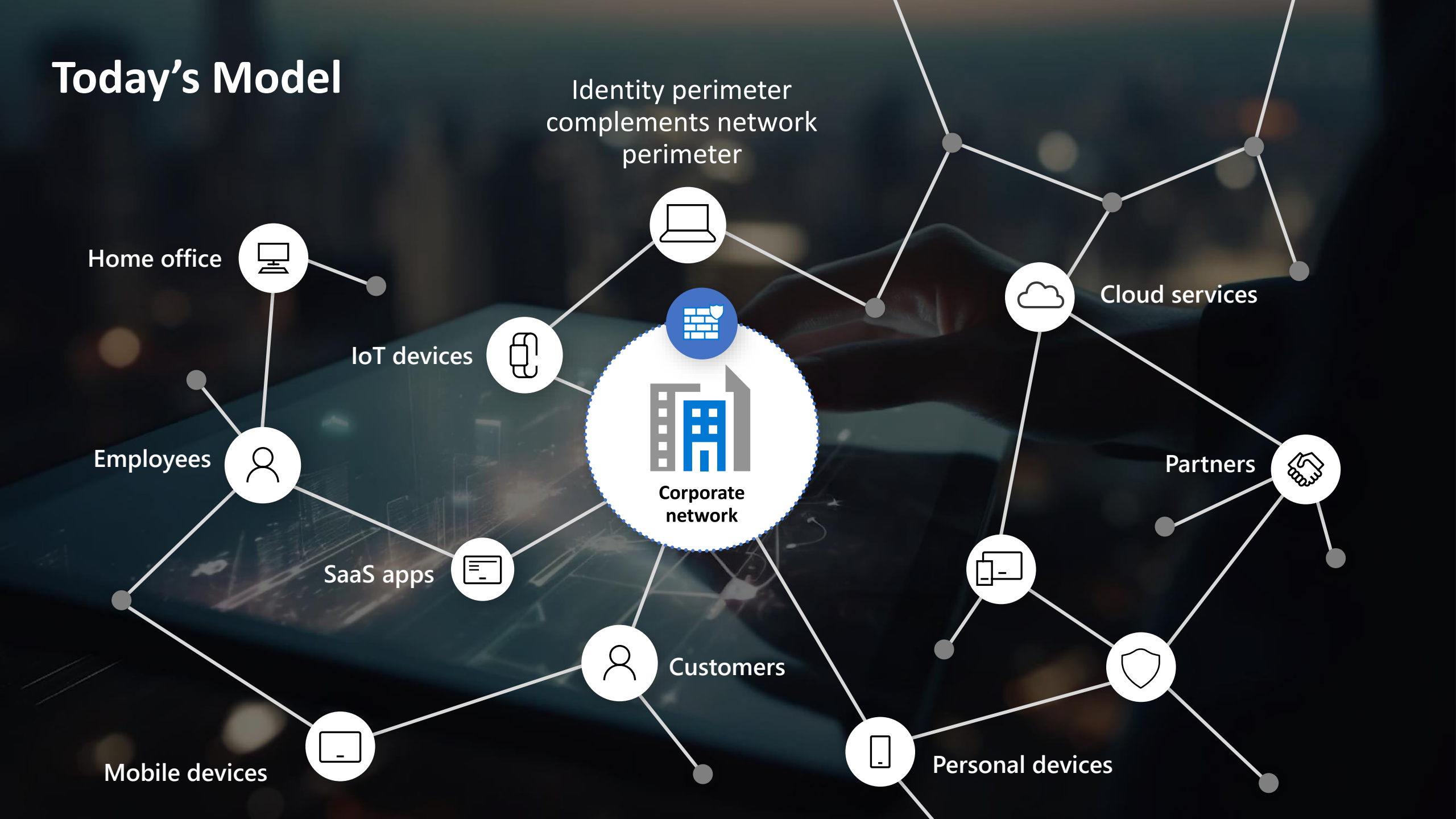
ROYAL CYBER

Microsoft Security Solutions

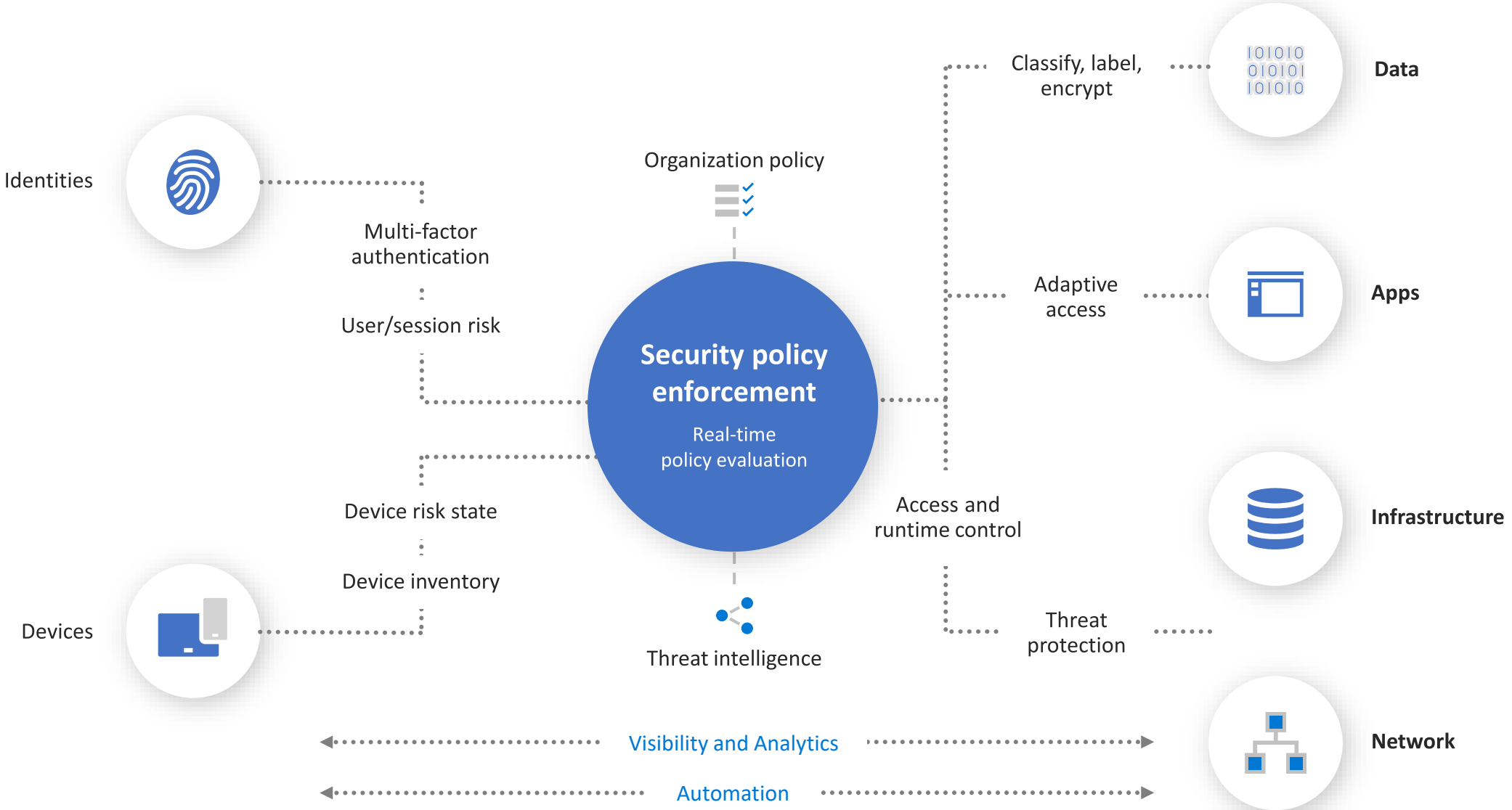
55 Shuman Blvd, Suite 275, Naperville, IL 60563

Tel: +1.630.355.6292 | Email: info@royalcyber.com

Today's Model



Microsoft Zero Trust architecture



Modernized security by utilizing Microsoft's Tools

Intune

- Device Management
- Application Management
- Autopilot
- Patch Management
- Compliance & Conditional Access

Defender for Identity

- Detection of identity-based attacks
- Anomalies and suspicious activity detection.
- AI based Investigation and response capabilities.
- Investigation and Forensics
- Attack Timeline Visualization:

Defender for Endpoint

- Behavior-based, real-time, heuristic antivirus protection
- Attack Surface Reduction
- Detects and blocks unsafe applications
- Automated Investigation and Remediation
- Generates a graphical attack timeline

Sentinel

- Machine Learning Based Advanced Threat Detection
- Security Orchestration and Automation
- Custom Detection Rules
- Playbooks and Workbooks
- Security Dashboards


Microsoft Intune

Problems without Intune

ROYAL CYBER

01 Are all your end-user devices encrypted?

02 Are web filtering policies centrally applied across all systems?

03 Are all your laptops patched on time and centrally managed?

04 Are all your organization's laptops synced with OneDrive for backup?

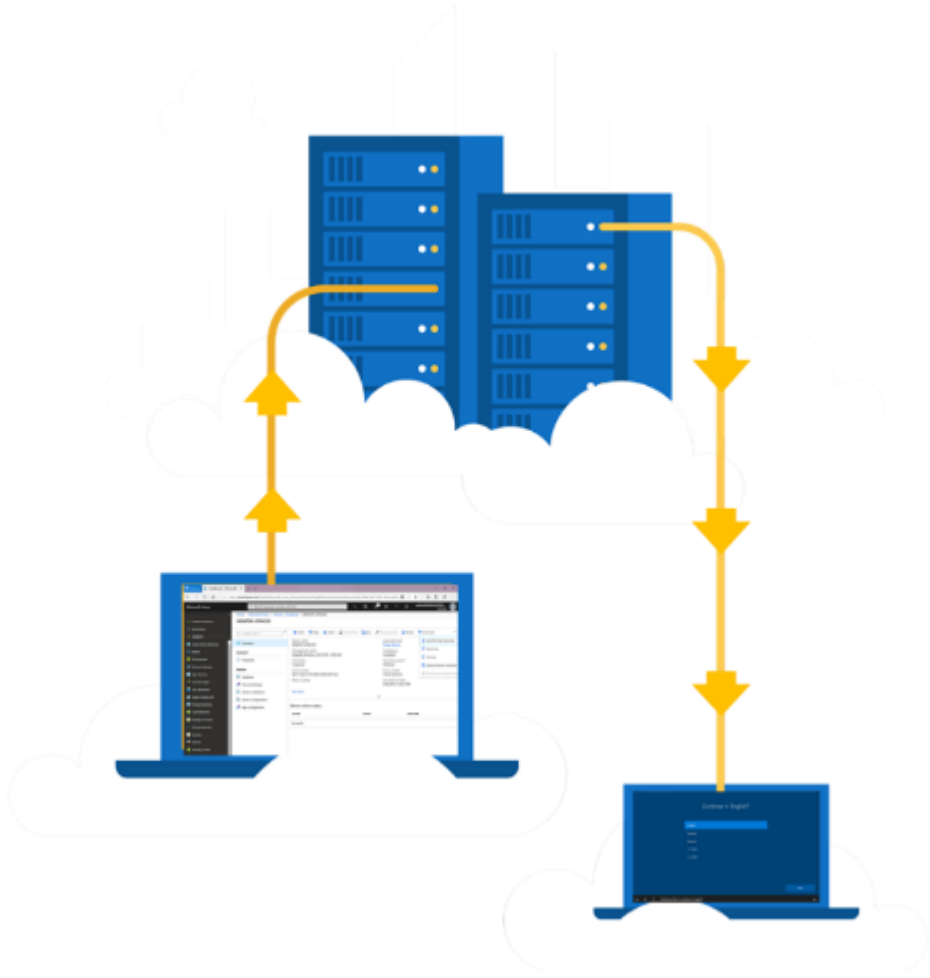
05 Are you centrally managing application deployment on end-user systems?

Windows Autopilot?

A **cloud-based deployment technology** available for all Devices

No need for **IT (NOC)** to touch the devices

Reset Device back to business ready state



Patch Management with Microsoft Intune

Patch Deployment:

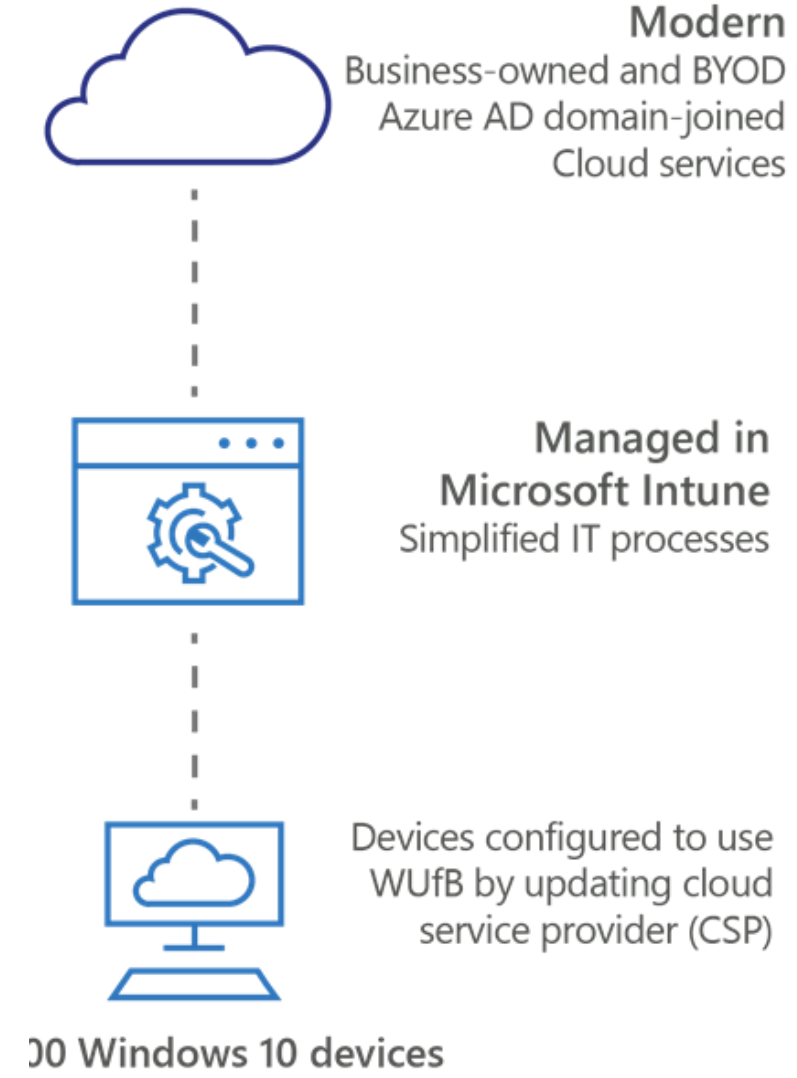
- deploy security and quality updates to Windows 10 and later devices. These updates include security patches, bug fixes, and feature updates.

Deployment Schedules:

- Intune provides the flexibility to schedule update deployments during maintenance windows or specific times, minimizing disruption to users' productivity.

Reporting and Monitoring:

- Intune offers reporting and monitoring capabilities that allow administrators to track the status of update deployments, assess device compliance, and identify any update-related issues.



Intune Policy Dashboard

ROYAL CYBER

Policy name	Platform	Policy type
RC- D drive Write Protection	Windows 10 and later	Custom
RC-Block Local Users	Windows 10 and later	Settings catalog
RC-Bookmarked -Important Links	Windows 10 and later	Administrative templates
RC-Defender-Onboarding Profile	Windows 10 and later	Microsoft Defender for Endpoint (
RC-Device Gaurd Policies	Windows 10 and later	Settings catalog
RC-Disable C Drive Access Policy	Windows 10 and later	Settings catalog
RC-Disable uninstalling the Apps	Windows 10 and later	Settings catalog
RC-Disable Windows Hello for Business	Windows 10 and later	Identity protection
RC-Disabled adding Non Microsoft Accounts	Windows 10 and later	Settings catalog
RC-File Explorer Policies	Windows 10 and later	Settings catalog
RC-Local User Bloackage	Windows 10 and later	Settings catalog
RC-Onedrive Policy	Windows 10 and later	Administrative templates
RC-Outlook-default app	Windows 10 and later	Administrative templates
RC-Personalization Policy	Windows 10 and later	Device restrictions
RC-Restrict access to Add/Remove page	Windows 10 and later	Administrative templates
RC-USB Blockage Policy	Windows 10 and later	Device restrictions
RC-Windows Health Monitoring	Windows 10 and later	Windows health monitoring

Intune Complaint devices Dashboard

ROYAL CYBER

Search

OS: Windows, Windows Mobile, Windows Holographic | Add filters

Device name	Managed by	Ownership	Compliance	OS	OS version	Primary user UPN	Last check-in
shaik.masthanvali_Windows	Intune	Unknown	Not evaluated	Windows	0.0.0.0	ıanvali@royalcyb...	
CN012	Intune	Corporate	Compliant	Windows	10.0.19045.4651	andersy@royalcy...	07/22/2024, 12:23 AM
RC2134	Intune	Corporate	Compliant	Windows	10.0.19045.4651	usuf@royalcyber....	07/22/2024, 01:42 AM
RC2216	Intune	Corporate	Compliant	Windows	10.0.19045.4651	ssan@royalcyber...	07/22/2024, 02:08 AM
RC2217	Intune	Corporate	Compliant	Windows	10.0.19045.4651	@royalcyber.com	07/22/2024, 08:28 AM
RC2264	Intune	Corporate	Compliant	Windows	10.0.19045.4651	ıani@royalcyber....	07/22/2024, 10:41 AM
RC2280	Intune	Corporate	Compliant	Windows	10.0.19045.4651	royalcyber.com	07/22/2024, 10:40 AM
RC2321	Intune	Corporate	Compliant	Windows	10.0.22631.3880	id@royalcyber.c...	07/22/2024, 02:02 AM
RC2349	Intune	Corporate	Compliant	Windows	10.0.19045.4651	d@royalcyber.co...	07/22/2024, 08:23 AM
RC2354	Intune	Corporate	Compliant	Windows	10.0.19045.4651	hid@royalcyber....	07/21/2024, 08:25 AM
RC2396	Intune	Corporate	Compliant	Windows	10.0.22631.3880	d.aleem@royalcy...	07/21/2024, 08:13 AM
RC2461	Intune	Corporate	Compliant	Windows	10.0.22621.3880	on@royalcyber.c...	07/22/2024, 10:39 AM
RC2504	Intune	Corporate	Compliant	Windows	10.0.19045.4651	d@royalcyber.com	07/22/2024, 10:41 AM
RC2506	Intune	Corporate	Compliant	Windows	10.0.19045.4651	on@royalcyber.c...	07/22/2024, 10:39 AM
RC2507	Intune	Corporate	Compliant	Windows	10.0.19045.4651	@royalcyber.com	07/22/2024, 01:22 AM
RC2508	Intune	Corporate	Compliant	Windows	10.0.19045.4651	dali.rehman@roy...	07/21/2024, 06:22 AM
RC2525	Intune	Corporate	Compliant	Windows	10.0.19045.4651	f@royalcyber.com	07/22/2024, 03:00 AM
RC2529	Intune	Corporate	Compliant	Windows	10.0.22631.3880	atima@royalcyb...	07/22/2024, 10:38 AM
RC2532	Intune	Corporate	Compliant	Windows	10.0.19045.4651	royalcyber.com	07/21/2024, 02:47 PM
RC2548	Intune	Corporate	Compliant	Windows	10.0.19045.4529	@royalcyber.com	07/22/2024, 10:42 AM
RC2556	Intune	Corporate	Compliant	Windows	10.0.19045.4651	aq@royalcyber.c...	07/22/2024, 01:25 AM


Microsoft Defender
for Identities

Why we need defender of identities

Microsoft Defender for Identity (MDI) helps organizations reduce their attack surface and identify security issues before they are exploited. It uses machine learning to monitor user accounts and entities for malicious activities and advanced hacking attempts in real time. MDI's capabilities include:

1. Detecting identity-based attacks and known malicious techniques.

2. Identifying anomalies in user activity and behavior.

3. Visualizing attack timelines to assist in incident response.

4. Proactively searching for threats using advanced hunting queries.

5. Identifying areas of concern in Active Directory, such as insecure account attributes and dormant accounts.

Why Royal Cyber?

Our experts can help you configuring the right polices & Automations tailored to your business needs

ROYAL CYBER

Incidents

Alert service settings | Email notification

Defender for Cloud alerts and incidents are now available in Microsoft Defender XDR. For non-admin users to view them, give unified RBAC permissions. Learn more about permissions.

Set permissions

The incident queue now displays incidents according to the latest automatic or manual updates made on incidents. For more information, see incident queue details.

Most recent incidents and alerts

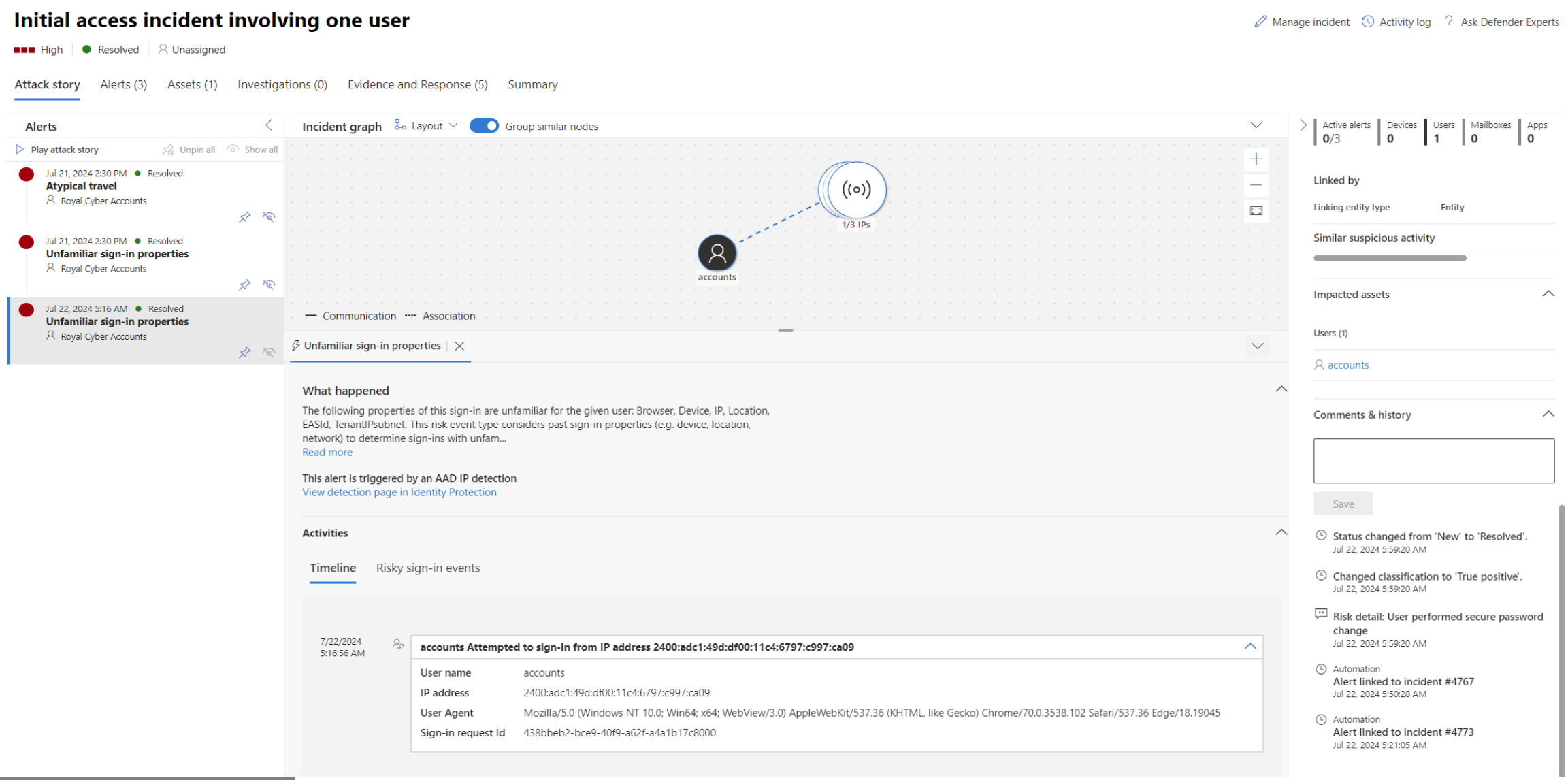
Export | Search for name or ID | 1 Week | Customize columns

Filter set: Save

Service/detection sources: AAD Identity Protection | Add filter | Reset all

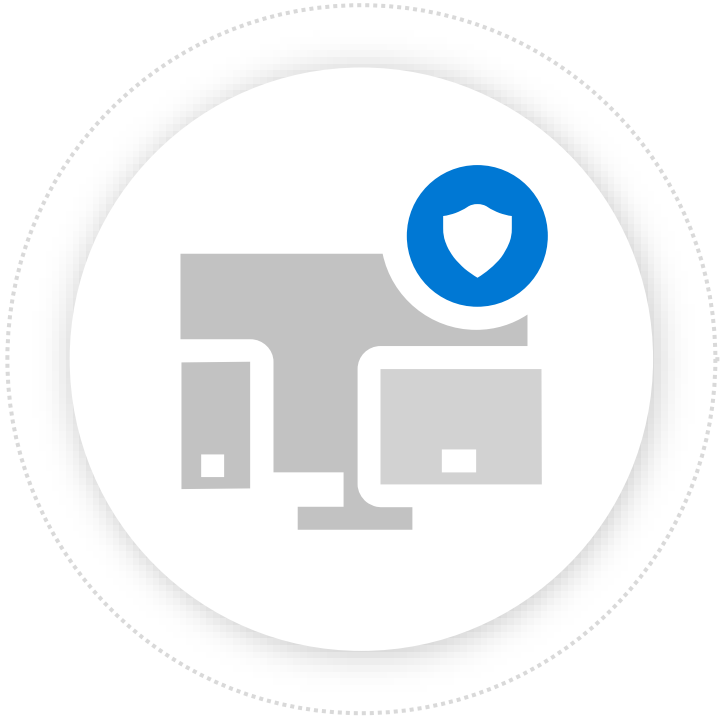
Incident name	Incident Id	Status	Severity	Investigation state	Categories	Impacted assets	Active alerts	Service sources	Detection sources	Last update time	Last activity
Atypical travel involving one user	4788	Resolved	Low		Initial access	Arun J	0/1	Identity Protection	AAD Identity Protection	Jul 22, 2024 11:54 AM	Jul 22, 2024
Unfamiliar sign-in properties involving one user	4774	Resolved	Low		Initial access	Arun J	0/1	Identity Protection	AAD Identity Protection	Jul 22, 2024 11:54 AM	Jul 22, 2024
Unfamiliar sign-in properties involving one user	4785	Resolved	Low		Initial access	Rana Usman Ahmad	0/1	Identity Protection	AAD Identity Protection	Jul 22, 2024 10:34 AM	Jul 22, 2024
Unfamiliar sign-in properties involving one user	4777	Resolved	Medium		Initial access	Maruthi Ellendula	0/1	Identity Protection	AAD Identity Protection	Jul 22, 2024 9:32 AM	Jun 17, 2024
Initial access incident involving one user	4767	Resolved	High		Initial access	Royal Cyber Accounts	0/3	Identity Protection	AAD Identity Protection	Jul 22, 2024 5:59 AM	Jul 22, 2024
Initial access incident involving one user	4708	Resolved	Low		Initial access	Royal Cyber Accounts	0/2	Identity Protection	AAD Identity Protection	Jul 22, 2024 5:58 AM	Jul 19, 2024
Anomalous Token involving one user	4766	Active	Medium		Initial access	Go Test Pro	1/1	Identity Protection	AAD Identity Protection	Jul 21, 2024 10:32 AM	Jul 21, 2024
Atypical travel involving one user	4758	Resolved	Low		Initial access	Rayhan Shirazi	0/1	Identity Protection	AAD Identity Protection	Jul 19, 2024 6:36 PM	Jun 14, 2024
Atypical travel involving one user	4757	Resolved	Low		Initial access	Rayhan Shirazi	0/1	Identity Protection	AAD Identity Protection	Jul 19, 2024 6:35 PM	Jun 14, 2024
Unfamiliar sign-in properties involving one user	4756	Resolved	Medium		Initial access	Rayhan Shirazi	0/1	Identity Protection	AAD Identity Protection	Jul 19, 2024 6:35 PM	Jun 14, 2024
Unfamiliar sign-in properties involving one user	4755	Resolved	Medium		Initial access	Rayhan Shirazi	0/1	Identity Protection	AAD Identity Protection	Jul 19, 2024 6:35 PM	Jun 14, 2024
Unfamiliar sign-in properties involving one user	4404	Resolved	High		Initial access	Meeran Khan	0/1	Identity Protection	AAD Identity Protection	Jul 19, 2024 3:55 PM	Jul 15, 2024
Initial access incident involving one user	4391	Resolved	Medium		Initial access	Chandra Jeyandran Mouli	0/2	Identity Protection	AAD Identity Protection	Jul 19, 2024 3:54 PM	Jul 15, 2024
Multi-stage incident involving one user reported ...	3390	Resolved	High	2 investigation states	Credential access, Suspicio...	Royal Cyber Accounts	0/2	Defender XDR, Identity Pro...	Defender XDR, AAD Identit...	Jul 19, 2024 3:52 PM	Jun 26, 2024
Anomalous Token involving one user	4709	Resolved	Medium		Initial access	Rabindra Shrestha	0/1	Identity Protection	AAD Identity Protection	Jul 19, 2024 3:51 PM	Jul 18, 2024

Incident Example:




Microsoft Defender
for Endpoints

Visibility into device health and compliance



Device information detection:

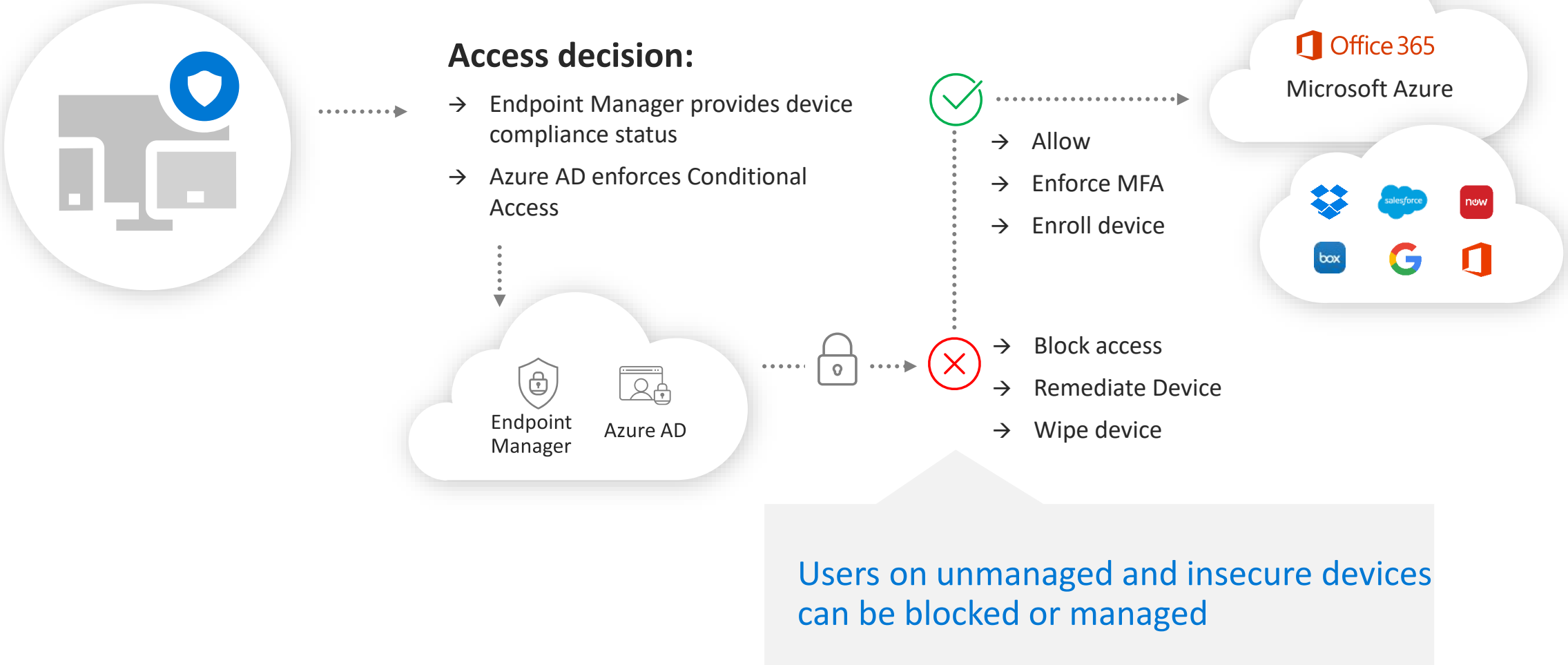
- Malicious Apps
- Device manipulation
- Network exploits
- Data privacy violations
- Device health
- Encryption
- OS version
- Email profile

Microsoft Defender ATP

Mobile threat defense partners

Microsoft, Lookout, Symantec, ZIMPERIUM, pradeo, Google Play Protect, Check Point SOFTWARE TECHNOLOGIES LTD

Restrict access from vulnerable and compromised devices



Incident Example:

ROYAL CYBER

Ransomware-linked emerging threat activity group detected on multiple endpoints

Manage incident | Activity log | Ask Defender Experts

High | Resolved | hassan.mehmood@royalcyber.com | Ransomware

Attack story | Alerts (4) | Assets (4) | Investigations (0) | Evidence and Response (4) | Summary

Alerts

Play attack story | Unpin all | Show all

Jul 9, 2024 1:06 PM ● Resolved
Ransomware-linked emerging threat activity group detected
rc2388 AbdullahMahmood

Jul 9, 2024 1:06 PM ● Resolved
Ransomware-linked emerging threat activity group detected
rc2388 AbdullahMahmood

Jul 10, 2024 3:37 PM ● Resolved
Ransomware-linked emerging threat activity group detected
rc2081 AbdulBasitJunejo

Jul 10, 2024 3:37 PM ● Resolved
Ransomware-linked emerging threat activity group detected
rc2081 AbdulBasitJunejo

Incident graph Layout | Group similar nodes

Communication ┈┈ Association

Ransomware-linked emerging threat activi...

Process tree | Alert timeline

Expand all | Copy story to clipboard

7/10/2024 9:01:31 AM — [21308] **explorer.exe**

9:01:49 AM — [18656] **msedge.exe** --no-startup-window --win-session-start

9:01:50 AM — [16732] **msedge.exe** --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --field-trial-handle=2356,i,...

3:37:07 PM — [16732] msedge.exe established **Outbound connection from 192.168.1.231:59067 to 192.64.119.19:80** Observed Device: Unknown device

Ransomware-linked emerging threat activity group detected Medium ● Detected ● Resolved (True positive)

3:37:22 PM — [16732] msedge.exe established **Outbound connection from 192.168.1.231:59059 to 192.64.119.19:443** Observed Device: Unknown device

Ransomware-linked emerging threat activity group detected Medium ● Detected ● Resolved (True positive)

Impacted assets

Devices (1)	Risk Level	Exposure Level
rc2081	Medium	Medium

Users (1)

AbdulBasitJunejo

Comments & history

Save

User-wasey.ameen@royalcyber.com
Changed determination to Malicious user activity.
Jul 22, 2024 3:30:39 PM

User-wasey.ameen@royalcyber.com
Changed classification to 'True positive'.
Jul 22, 2024 3:30:39 PM

User-wasey.ameen@royalcyber.com
Status changed from 'New' to 'Resolved'.
Jul 22, 2024 3:30:39 PM

User-wasey.ameen@royalcyber.com
Alert was assigned to hassan.mehmood@royalcyber.com.
Jul 22, 2024 3:30:39 PM

Automation
Alert linked to incident #4059
Jul 10, 2024 3:39:17 PM

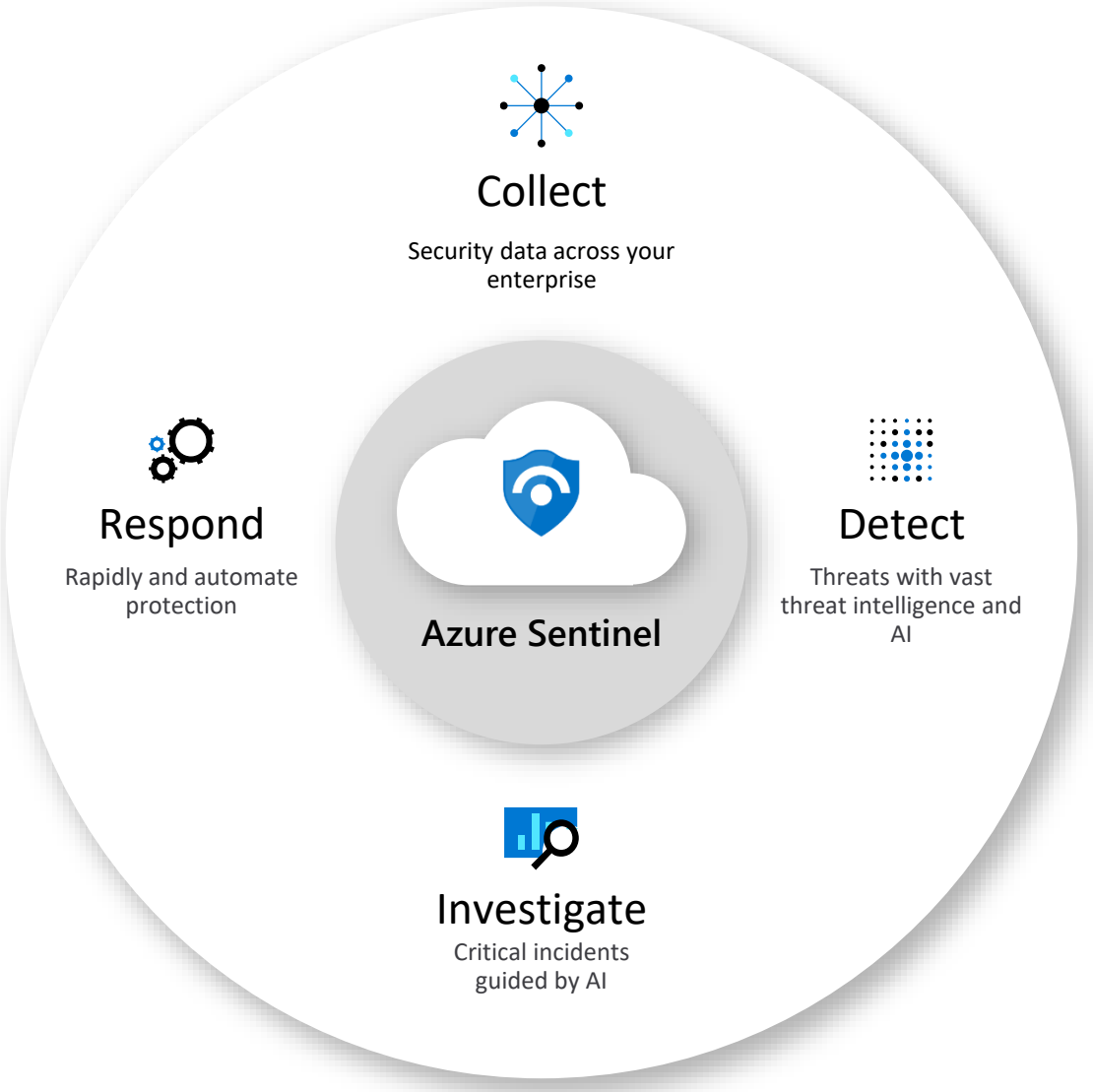
Automation
Alert linked to incident #4154
Jul 10, 2024 3:38:45 PM


Microsoft Sentinel

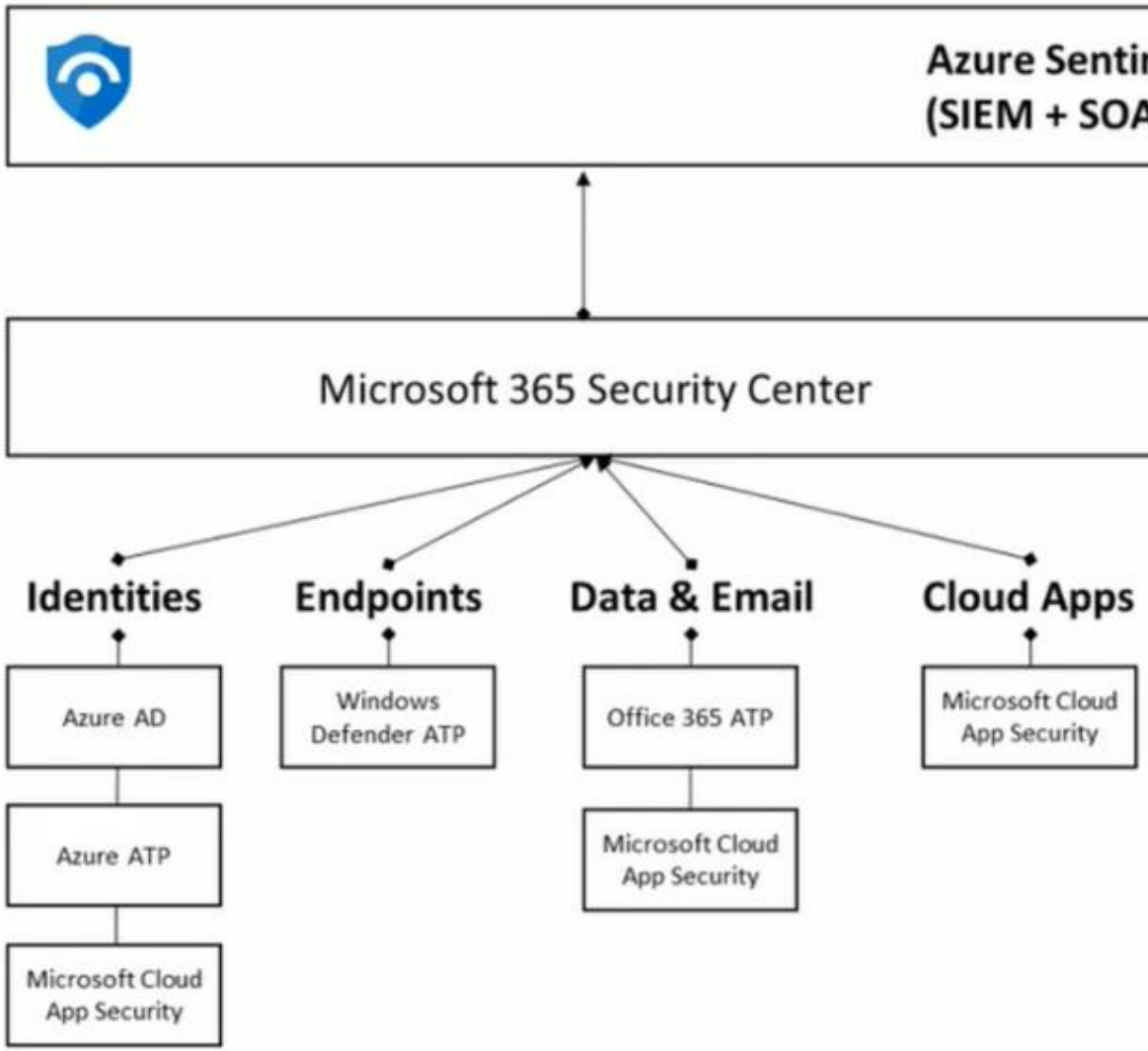
Introducing Microsoft Azure Sentinel

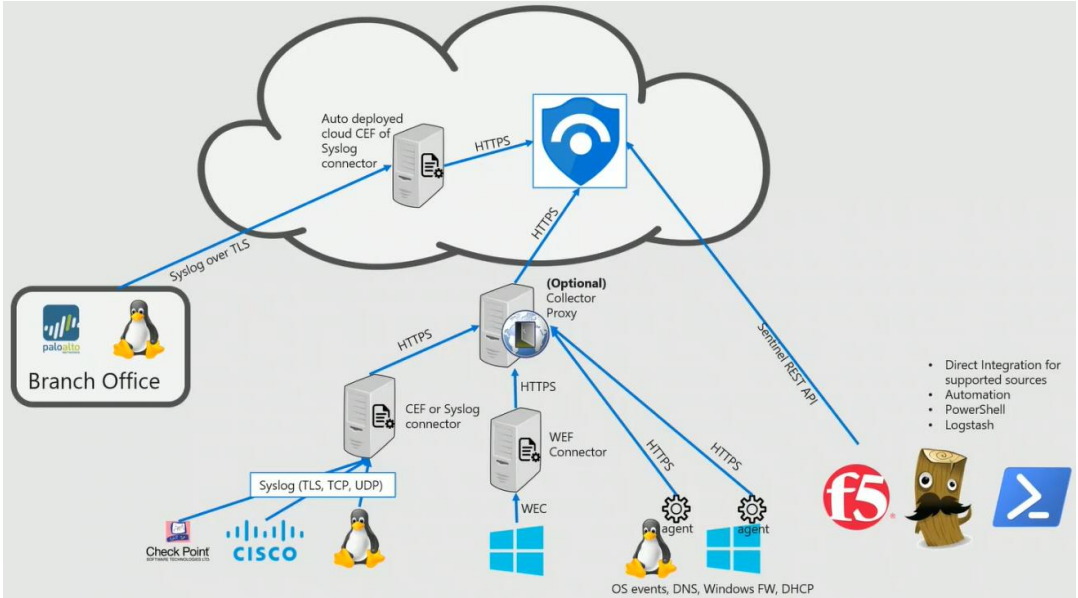
Cloud-native SIEM + SOAR (Security Orchestration, Automation and Response) for intelligent security analytics for your entire enterprise

- Limitless cloud speed and scale
- Bring your Office 365 data for Free
- Easy integration with your existing tools
- Faster threat protection with AI by your side



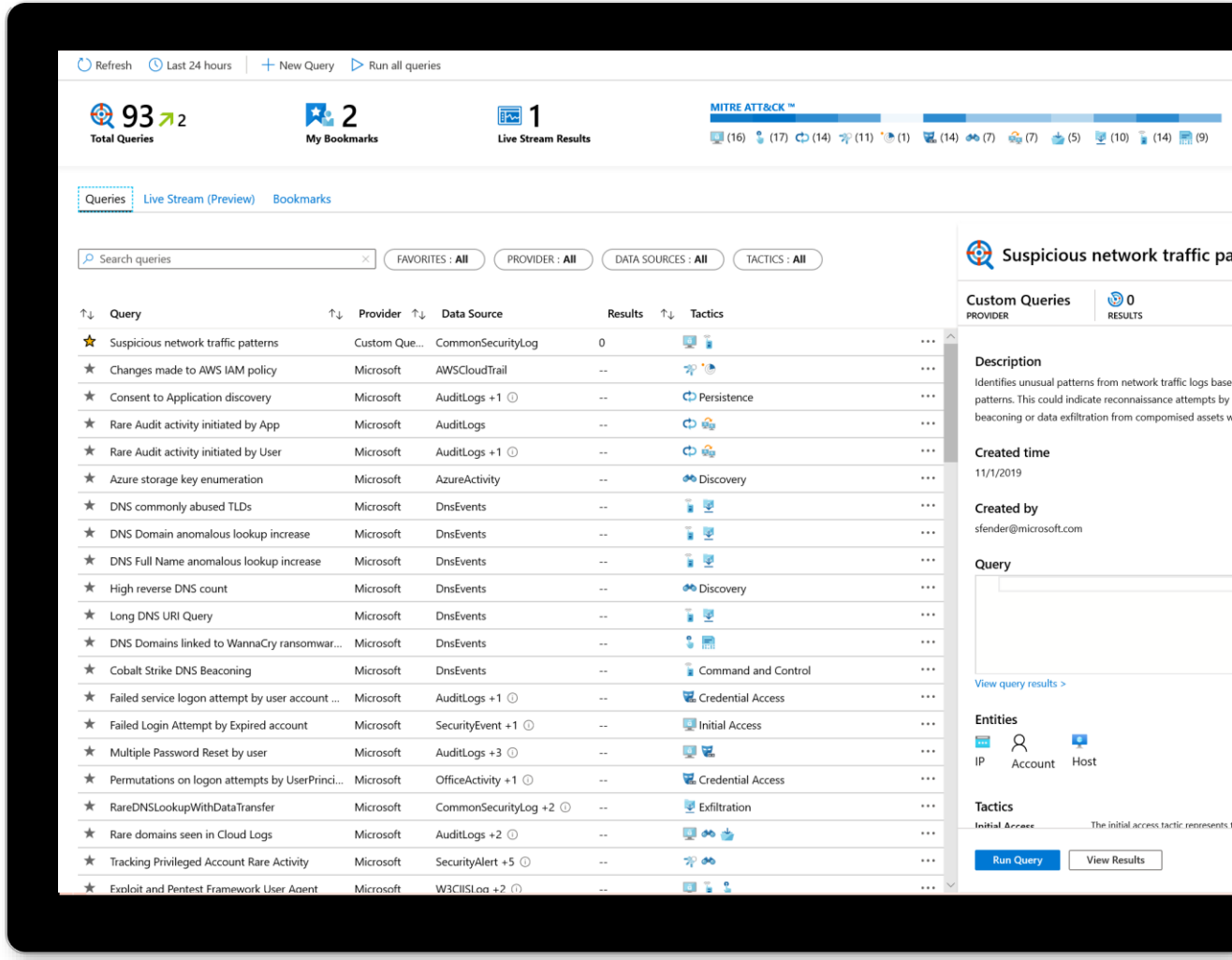
Azure Sentinel – Across Security Center





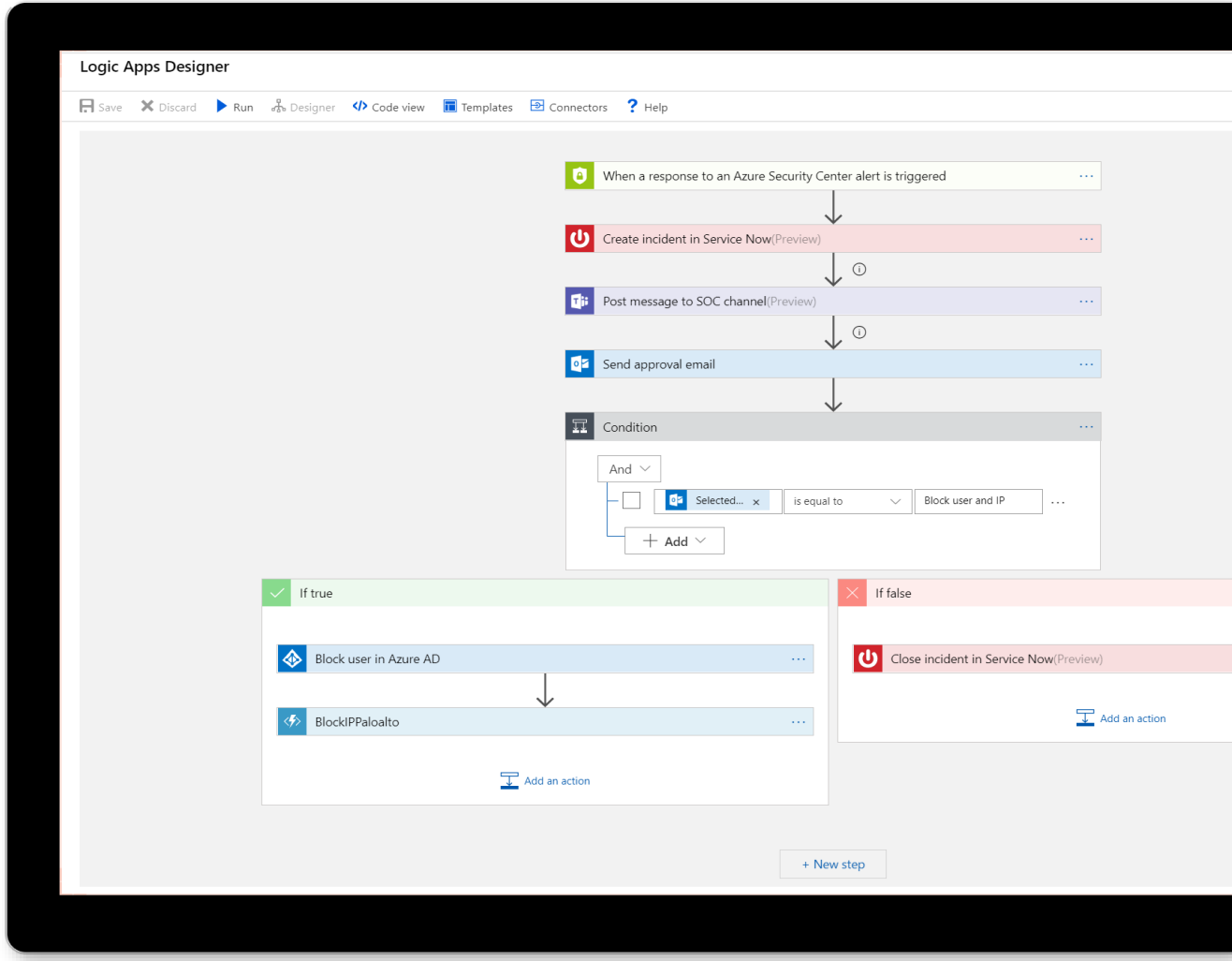
Start hunting over security data with fast, flexible queries

- Run built-in threat hunting queries - no prior query experience required
- Customize and create your own hunting queries using KQL
- Integrate hunting and investigations



Automate and orchestrate security operations using integrated Azure Logic Apps

- Build automated and scalable playbooks that integrate across tools
- Choose from a library of samples
- Create your own playbooks using 200+ built-in connectors
- Trigger a playbook from an alert or incident investigation



Capabilities

01 Zero Trust Security Assessment:

- Conduct a comprehensive assessment of the organization's current security posture.
- Identify vulnerabilities, risks, and compliance gaps.
- Provide a detailed report with recommendations.

02 Zero Trust Security Strategy and Roadmap:

- Develop a customized Zero Trust security strategy aligned with the organization's objectives.
- Create a roadmap outlining the implementation steps and timelines.

03 Identity and Access Management (IAM) Implementation:

- Set up and configure Azure Active Directory for centralized identity management.
- Define and enforce Conditional Access policies for fine-grained access control.

04 Zero Trust Network Access (ZTNA) Deployment:

- Design and deploy secure network connectivity solutions, such as Azure Private Link and VPN Gateway.
- Implement network segmentation and isolation to reduce attack surface.
- Configure secure remote access for users.

05 Endpoint Security Implementation

- Deploy and configure Microsoft Defender for Endpoint to protect endpoints from advanced threats.
- Define and enforce security policies for endpoints.
- Conduct initial threat assessments and remediation.

06 Identity and Threat Protection Setup:

- Implement Microsoft Defender for Identity (formerly Azure Advanced Threat Protection) for identity-based threat detection.
- Configure monitoring and alerting for suspicious activities and compromised accounts.

07 Data Protection and Compliance:

- Deploy Azure Information Protection for data classification, labeling, and encryption.
- Create and enforce data loss prevention (DLP) policies to prevent data leakage.
- Assist with compliance initiatives and audits.

08 Security information and event management(SIEM):

- Configure and manage Azure Sentinel for centralized security monitoring and analytics.
- Develop custom dashboards and alerts for real-time threat detection.
- Conduct incident response planning and setup.


Any Question

Our Offices

US Headquarters
Royal Cyber
55 Shuman Blvd, Suite 275, Naperville, IL 60563 USA.
Tel: +1.630.355.6292

Australia Office
Royal Cyber
Level 1, 86-90 Bay Street,
Broadway NSW 2007, Australia
Tel: +61 (2) 9959 1058

South Africa Office
Royal Cyber Pty Ltd.
3rd Floor, 5 Sturdee Ave 2196 Rosebank,
Johannesburg, Gauteng, South Africa
Tel: +27.10.500.8120

India Office
Hallmark Towers, 7th Floor,
Developed Plot Estate, Guindy
Chennai – 600032, Tamil Nadu
Tel: +91 044-4266 7042

UK Office
RC Technologies Limited
20-22 Wenlock Road, London, UK N1 7GU
Tel: +44 203 818 5902

Canada Office
Royal Cyber Technology Inc.
1285 W Broadway #600,
Vancouver, BC V6H 3X8
Tel: +1.416.549.1646

Saudi Arabia Office
Office #503, 5th Floor, Building #1, Al Nour Street, Al Olaya District,
P.O. Box 2504, Riyadh – 12214.
Tel: +966.11.461.1906

MS SARAF TOWERS, #15/7,
1st Floor, Prime Rose Road,
Bangalore – 560001, Karnataka
Tel: +91 08040983128

Contact Us

Global Infrastructure Relationship Quality Solutions