ZERO TRUST SECURITY



Microsoft 365



Why Security is Relevant to You

- 33% of Australian Businesses have experienced cybercrime with an average cost of \$276,000 (23 to 51 days to recover).
- COVID has resulted in an unprecedented adoption of cloud services – functionality taking precedence over security.
- Many businesses have not addressed the changes to the security landscape.







Agenda

Today we will:

- Discuss what Zero Trust is and explore its key components
- Review Microsoft's solutions to these modern threats and challenges
- Present some of Jasco's security offerings powered by the Microsoft engine

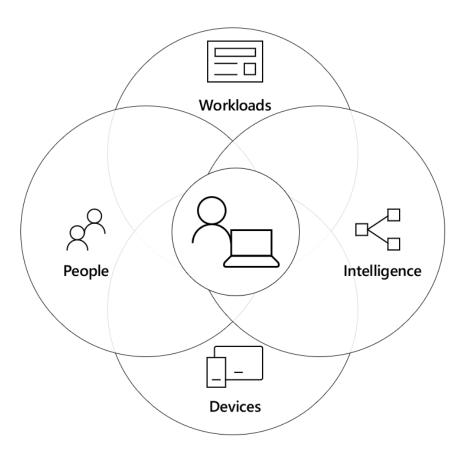




MODERN SECURITY



What is Zero Trust?



Principals

access

•

• Verify explicitly

Least privileged

Components

- Identity
- Devices
- Applications
- Data
- Infrastructure

- Network
- Assume breach



Why is Identity important?

CLOUD!!!

- The security boundary is no longer the firewall
- Is the first line of defence in a cloud first world
- Aligned with every sign-in, application or data transaction, and defines privilege

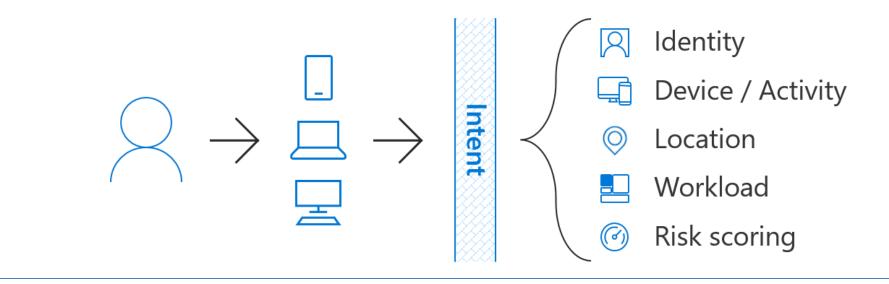




Devices

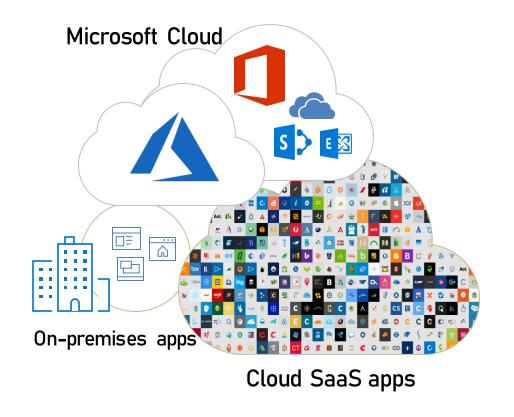
- Remote work demands greater levels of control, access, and device management
- Traditional device management solutions do not reach past the (old) security boundary

 Key to facilitating a successful and secure BYOD strategy





Applications

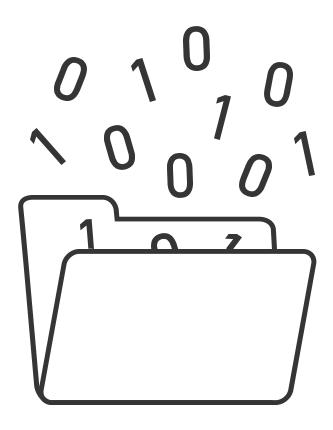


- Shadow IT is often an important but invisible risk to the business
- Unsanctioned apps pass on their own insecurities to the business
- May impact upon regulatory compliance responsibilities



Data

- Corporate data is the life blood of a business
- Leakage of sensitive information may result in stolen IP, fines due to noncompliance, and impact to company brand





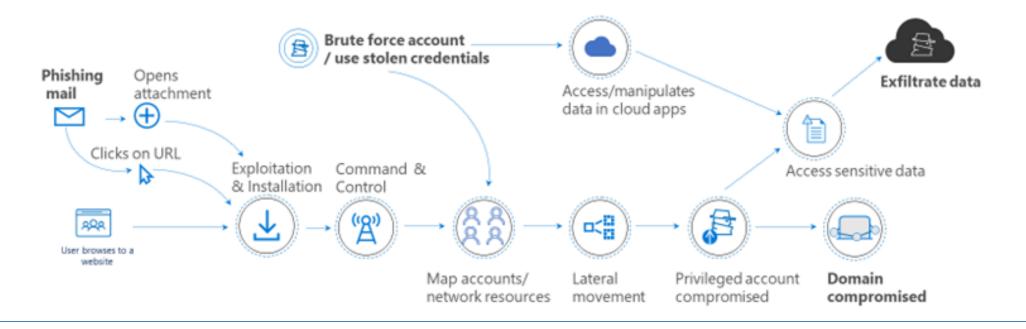
External Threats

• Malware

• Credential theft and infiltration

• Email threats

• Ransomware





Internal Threats

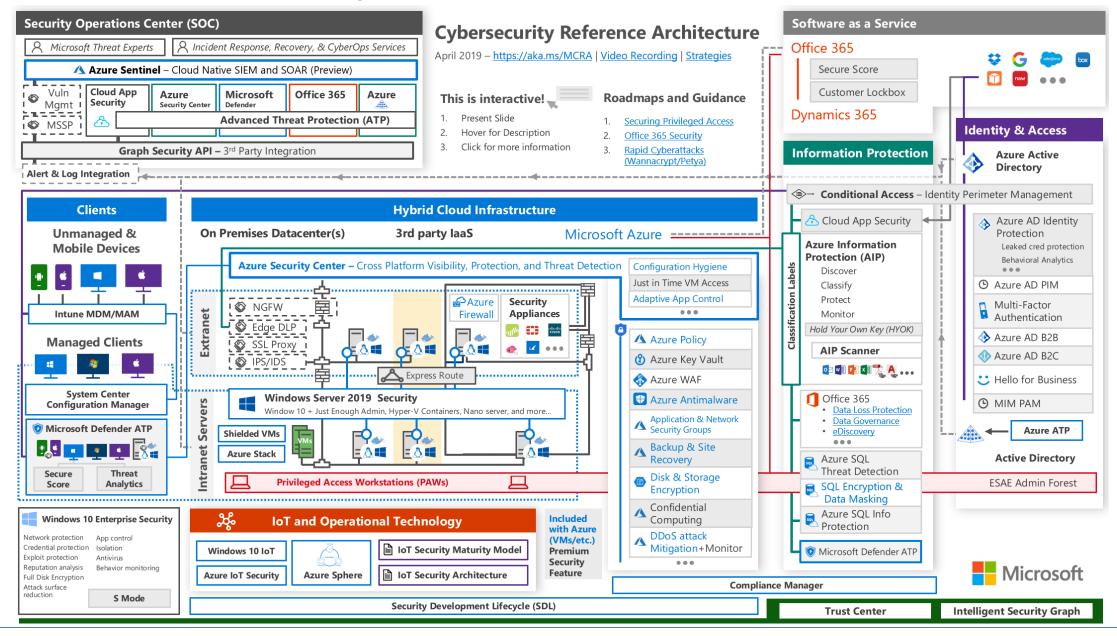
128	5875	3861	9.5тв	¥ 17 TB	Cloud Discovery open alerts	
120	5075	5001	J.JIB	± 7.8 TB	8 Nerve appe allerts	14 Suprema wage days
App categories			(1640) • (166)		Risk levels	Alterngeles 🚺 by thes
	Sectional X Unarchined	er sa Differences	d DUnunctioned	0 108e		Users using high risk appr
Coluberation I	- 00w	27.68		120.68		Overs using medium risk apps
Cloud Maringe				114 GB	890	Litera using low-mit appo
Webmail Internet				91 GB	Users [Nigh risk	A many and a second state
Social tetres and				68 GB		
Online meeting				60.08		Configure score metric
Discovered apps	. 41	1.16.of 20 • View of eggs Case E Ser	career by the	10ter	Top users Top IP addresses	
C-0-0-4						Vex sluxes (bats) Total 1201 1181
			channel I chramathene 11 GB		Over Sames Lake	Tetal 520 (
Ondeline			charved Ethnamitiana H CR 10.9 CR	10ther	Class Samuel Linka Microsel Specificity	Tetal 120 1 118 1
Duchus Des Des Syngelisty			channel di chaamatieren 11 GB 10 9 GB 10 4 GB	10ther	User Sames Lake Monuel Spelling Daryf Smaw	1014 120 / 118 / 110 /
Chathian Inn Dhagtan Singalain Maga			channel Universitienen 11 Ga 169 GB 104 GB 104 GB	10ther	Uner Samer Lähe Michael Spalling Ceryl Smare Lany Bloomberg	1014 1201 118 1 110 1 58 5
Condition Designed Designed Sprogelicity			ctured Unumber 11 Ga 129 Ga 134 Ga 133 Ga 133 Ga 133 Ga 133 Ga	10ther	User James Lake Microel Spotting Deryf Snaw Llony Boomberg Mike Maple	1014 120 1 118 1 110 1 98 M 97 M
Conclose Examples Desition Desition Service Service Examples Exam			ctured Unumber 11 Ga 129 Ga 134 Ga 134 Ga 133 Ga 133 Ga 135 Ga 135 Ga 135 Ga	10ther	Uner Samer Lähe Michael Spalling Ceryl Smare Lany Bloomberg	1014 1201 118 1 110 1 58 5
Condition Condi			ctared Unardone 11 Ga 129 Ga 134 Ga 133 Ga 133 Ga 133 Ga 133 Ga 135 Ga 135 Ga 135 Ga 135 Ga 135 Ga 135 Ga 135 Ga	10ther	User James Lake Microel Spotting Deryf Snaw Llony Boomberg Mike Maple	1014 120 1 118 1 110 1 98 M 97 M
Synghity Maps 2002 # Spyte 2 Maps 2002 # Spyte 2 Maps 2 Cality 2 Cality			ctured Unumber 11 Ga 129 Ga 134 Ga 134 Ga 133 Ga 133 Ga 135 Ga 136 Ga 7 Ga 3.8 Ga	10ther	User James Lake Microel Spotting Deryf Snaw Llony Boomberg Mike Maple	1014 120 1 118 1 110 1 98 M 97 M
Conclose Anno Anno Anno Anno Anno Anno Anno Ann			ctured Unumber 11 GB 129 GB 134 GB 104 GB 103 GB 103 GB 103 GB 105 GB 10	10ther	User James Lake Microel Spotting Deryf Snaw Llony Boomberg Mike Maple	1014 120 1 118 1 110 1 98 M 97 M
Concloses Concl			ctured Characteres 11 GB 129 GB 134 GB 104 GB 103 GB 103 GB 103 GB 105 G	10ther	User James Lake Microel Spotting Deryf Snaw Llony Boomberg Mike Maple	1014 120 1 118 1 110 1 98 M 97 M
Condition Condi			ctured Unumber 11 GB 129 GB 134 GB 104 GB 103 GB 103 GB 103 GB 105 GB 10	10ther	User James Lake Microel Spotting Deryf Snaw Llony Boomberg Mike Maple	1014 120 1 118 1 110 1 98 M 97 M

- Data and IP Leakage
- Malicious insiders
- Shadow IT
- Unsecure Devices



MICROSOFT SOLUTIONS

Microsoft's Security Architecture





Azure Active Directory (AAD)

- Single sign-on simplifies access to your apps from anywhere
- A single identity platform lets you engage with internal and external users more securely
- Gartner recognised access management leader in 2020 ^





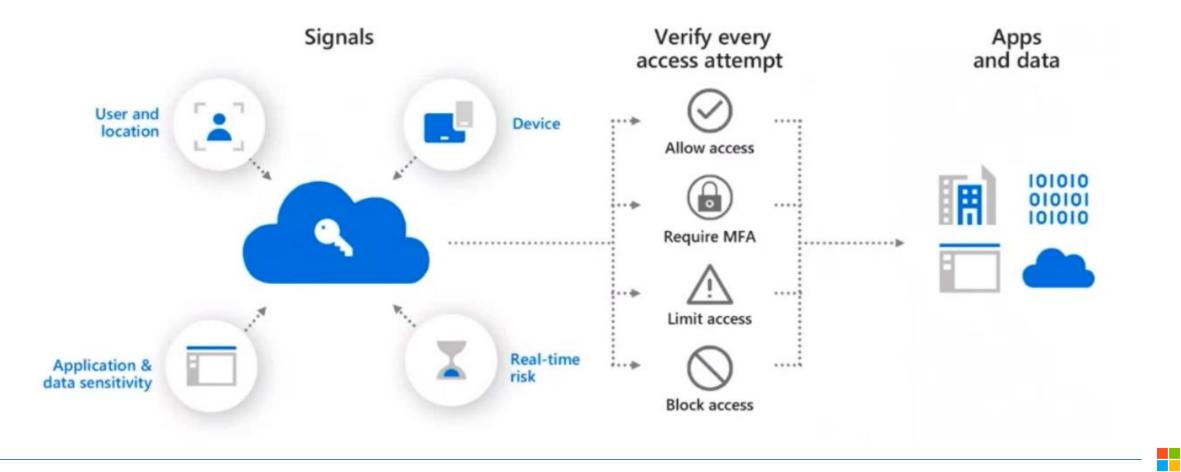
Multi Factor Authentication



- Remove the insecurities of outdated password management processes.
- MFA (or 2FA) secured accounts are 99.9% less likely to be compromised. ^
- Protect access to resources using three key principles



Conditional Access





Microsoft Endpoint Manager

Formerly known as Intune

- Centrally manage your fleet of workstations and mobile devices regardless of their locations
- Extend on-premises Configuration Manager capabilities to the cloud
- Provision new corporate devices from anywhere
- Introduce a BYOD strategy securely

	$\leftarrow \rightarrow$	O A https:	//endpoint.mic	rosoft.co	m/#@sccmavenge	r.com	n/dashboard/	private/4e	9f850d-bc15-433d-80
	Microsoft Er	in center							
	A Home	*	Dashboard 🕥	+ New	dashboard 🕴 Upload	* 0	Download 🧷 Ei	dit 🥜 Full si	creen 🖒 Clone 🔋 Delet
Dashboard		Device enrollment		Device compliance		Device configuration		Welcome to the Microso	
() 11:51 @ @ ₱ •			OK No Intune enro failures last 7 d		devices not in compliance		OK All devices are configured	e	Microsoft Endpoint Manag management capabilities f your device types, includin Manager you can: Enroll and configure yo Upload and distribute y
Microsoft APPS DEVICES SUPPORT		Client apps		App protection policy user status Status iOS users				Protect your organization Cloud-enable computer Monitor and troublesho Tutorials and articles	
Feetured Appe			3 🔺		Policy assigned	1		0	Learn about Microsoft End
Featured Apps VIEW ALL		apps have installation failures		No policy 0			10 Get st	Get your device enrolled Get started with cloud-bas Set up Intune Data Wareho	
Athena.Andro Microsoft (Inter			Intune enrolled LAST UPDATED 4/28				Device comp	liance status	Devices
Axis To Go Microsoft (Inter	and the second se		Windows		10		Compliant		8
Microsoft (inter	nar)		Android		8		In grace perio	d	3 🔺
EDDA Mobile			iOS		6		Not evaluated		2
Microsoft (Inter	mal)		macOS	1			Not compliant	:	11 0
			Windows Mobil	e 0			Total		24
X Excel			Total	25					



Exchange Online Protection

- Reputation Filtering
- Spam and Spoof protection
- Anti-Malware
- Content Filtering
- Zero Hour Auto-purge





Microsoft Defender for Office 365 (MDO)

Formerly Office 365 Advanced Threat Detection (0365 ATP)

Vertice de la congrande Vertice Naris Aaris Aaris Casabidation Roardista shouldy allow Maris Casabidation Roardista shouldy allow Maris Aaris Casabidation Roardista shouldy allow Maris Casabidation Roardista shouldy allow Maris Casabidation Roardista shouldy allow Maris Casabidation Casabidation <			
None Arets Arets Remissions Cassification Cassification Cassifi		once sos security a comp	younge V V V V
Nome Actrs Permissions Permissions Cassification Cassification <th></th> <th></th> <th>Vser reported as compromised (Preview) - DEBRAB@MT</th>			Vser reported as compromised (Preview) - DEBRAB@MT
Acts Permissions Cassification Cassification Old loss prevention Cassification Records management Sepervision Internation governance Sepervision Mail flow Data privacy Search Concorry Search Concorry Search Concorry Concorry <t< th=""><th></th><th>Home</th><th>Investigation #0e7dB5 is Pending Action Oct 28, 2019 539:42 PM End Time End Time 215:53:44 Pending Action</th></t<>		Home	Investigation #0e7dB5 is Pending Action Oct 28, 2019 539:42 PM End Time End Time 215:53:44 Pending Action
Permission: Data loss provention Records: management Information governance Supervision: Threat management Supervision: Threat management Supervision: Entit investigated (63) Park ISC Records: management Supervision: Entit investigated (13) Park ISC Reports Sercice assurance Utars investigated (1) Mail flow Construction: Reports Sercice assurance Utars investigated (1) Mail flow Construction:		Alerts	Total Pending Time
Data loss prevention	ै	Permissions	
Records management Information governance Supervision Threat management Mail forw Data privacy Search Sciench Reports Service assurance User investigated (1) Mail forwaring failer four (1) Threat four (10) Threat f		Classification	
Nection instalgement Supervision Threat management Mail flow Mail flow Data privacy Search Search Bebriss Service assurance Uters investigated (1) Mail forwation (10) Treats found (10) Treats found (10)		Data loss prevention	
Supervision Threat management Mail forw Mail forward Search Reports Service assurance Uters investigated (1) Mail forwarding faile found (1) Threat found (1) T		Records management	Suppicious email sending patterns detacted (1)
Tureat management Paus 1820 Paus 18		Information governance	
Thread management Mail flow Mail flow Data privacy Search eDitcovery Reports Service assurance Users investigated (1) Mail forwarding flate found (1) Thread flate found (1)		Supervision	Emails investigated (403)
Mail flow Data privacy Search Reports Service assurance Users investigated (1) Mail forwarding flate found (1) These		Threat management	Phich (402)
Search C C C C C C C C C C C C C C C C C C C		Mail flow	
eDiscovery Reports Service assurance Uters investigated (1) Reports Uters investigated (1) Reports Uters investigated (1) Reports Example a subscription of (10) Example a subscription of		Data privacy	
Reports V Service assurance Users investigated (1) Reports found (10) Mail forwarding Fuller Found (1) Mail forwarding Fuller Found (1)		Search	
Service assurance Users investigated (1) Mail forwarding Rule Found (1) Invests found (10)		eDiscovery	×
Mail Forwarding Fulle Found (1) Mail Forwarding Fulle Found (1)		Reports	×
mentor weining nue round (1) Bhith		Service assurance	and and an
			main of water young (1)
Composition of our France and provide Composition of the Composition o			Article from informant country (1) MaliciousUH

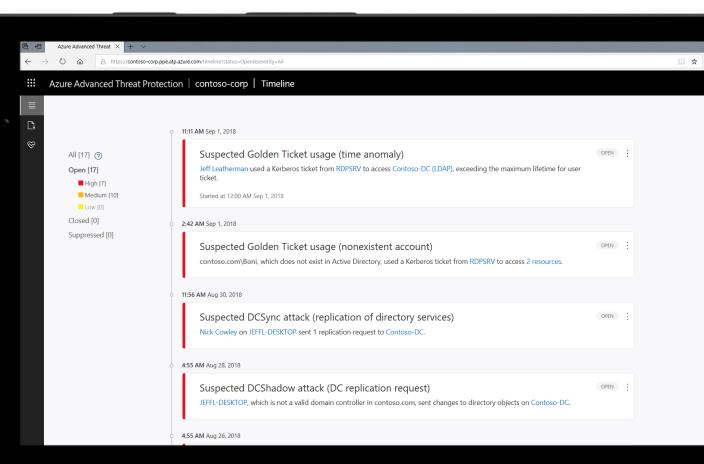
- Exchange Online Protection features.
- Zero Day attack defence.
- Content Filtering and Anti-Malware for Teams, SharePoint, and OneDrive.
- Email and Password Attack Simulation.



Microsoft Defender for Identity (MDI)

Formerly Azure Advanced Threat Detection (Azure ATP)

- Protect against identity compromise
- Prioritised information to focus on real threats
- Identify vulnerabilities before attacks happen





Microsoft Defender for Endpoint (MDE)

Formerly Windows Defender Advanced Threat Detection (Windows ATP)

Threat & Vulnerability Management	dashboard			Top security recommendations 4/51
Organization exposure score	Organization configurati	on score	Machine exposure distribution	Based on highest organizational exposure impa
Exposure score This score reflects the current exposure associated with machines in your organization ©	Configuration 292 / 578 This score reflects the collect configuration posture of you Application. Network, Accourt	ive security r machines across OS,	Exposure distribution Exposed machines are easy targets for cybersecurity attacks. Ensure that these machines can receive security updates, have critical security controls, and are properly configured.	Update Chrome 2 Exposed machines * 25.20 Software patch
0 100	Controls (1)	13 / 63		Update Windows 10 1 Exposed machines + 24.00 Software patch
36/100 Low 0-29 Medium 30-69 High 70-100	OS Network	45 / 175 32 / 62	2 Total	Turn on PUA protection
	Accounts Security controls	7 / 12 195 / 266		
Exposure score over time A 36 Last 30 days	Configuration score over ti	me i 12	📕 Low 📕 Medium 🔳 High	Turn on Attack Surface Reduction rul 2 Exposed machines * 3.00 + 9.00 Configuration change
100	300			Show more Show exceptions

- Endpoint detection and response
- Threat and vulnerability management
- Automated investigation and remediation
- Next generation protection and attack surface reduction



Microsoft Cloud App Security (CAS)

📕 Dashboard - Microsoft + 🗙 🕂 🗸				– 0 ×
⊖ A https://mcastest9.portal.cloudappsecur	ity.com/#/dashboard			☆ ☆ & છ ▦ …
Cloud App Security	م			© ? @ 8
	Get started with Cloud App Security	Create a Cloud Discovery report 🛛 🙆 Connect apps	s 🔞 Create policies 🗄 Learn more	×
! General dashboard →	General dashboard		0,700	
View dashboard for a specific app Microsoft 365 admin center Microsoft Azure Information Protection	 G 5K+ activities monitored SO3 discovered apps (last 30 days) 	5.5K files monitored 72 governance actions taken	 709 accounts monitored 94 user notifications sent 	
Microsoft Skype for Business Microsoft Support - General Microsoft Word Online - General Office 365	910 Open alerts New over the last month + RECENT ALERTS		BY SEVERITY BY ALER)9 Custom
Microsoft Cloud App SecurityMicrosoft Azure	I Alert on new API token creation Mike Microsoft Cloud App Security	36 minutes ago	High	Built-in
 Microsoft OneDrive for Business Microsoft SharePoint Online 	Alert on new API token creation Mike Microsoft Cloud App Security	36 minutes ago	Top 3 alert types 24 Access policy alert	
Microsoft Exchange Online Amazon Web Services - US	Impossible travel activity Super Admin (mcas-test9) 3 services	4 hours ago	23 Activity policy alert	
Box - USSalesforce - US	View all alerts in the last month		System alert Cloud Discovery automatic log upload	error
Microsoft Power BI				
 Microsoft Teams Microsoft Cloud App Security G Suite - US 	1,177 Activity matches New over the last month -	224	432 Content matches New over the last month -	<u>0</u> 1
Vammer	420 Potential ransomware activity		1 Malware detection	

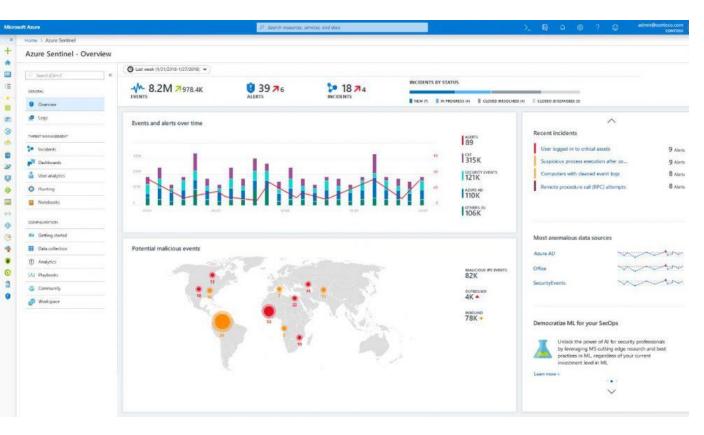
- Centralize and control cloud app activity
- Discover Shadow IT and enforce policies to manage cloud usage.
- Protect your sensitive information anywhere in the cloud.
- Assess the compliance of your cloud apps.



Microsoft Sentinel

Security Event and Incident Management (SEIM) and Security Orchestration and Response (SOAR)

- Gathers security events across
 multiple platforms
- Related events are collated into incidents for review and correction
- Uses configured policies and machine learning to automate corrective action





JASCO OFFERINGS



Jasco's Flexible Approach

- Not every Business is the same
- Tiered offerings to address customers of multiple profiles
- Consultancy and Tailoring!!!





Tier 1 – Security Essentials

Providing visibility for Identities, Users, and Devices without borders



Objectives

- Protect against common external threats.
- Ruin Attacker's Return on Investment (AROI).
- Provide visibility of your security standing and security events.

Components

- Modern Authentication Multi Factor Authentication and Conditional Access
- Device management and security Windows Defender, Log Analytics, Endpoint Manager
- Spam, Phishing, and Malware protection
 Exchange Online Protection
- Office 365 Access Control and Reporting

 Conditional Access App Enforced
 Restrictions



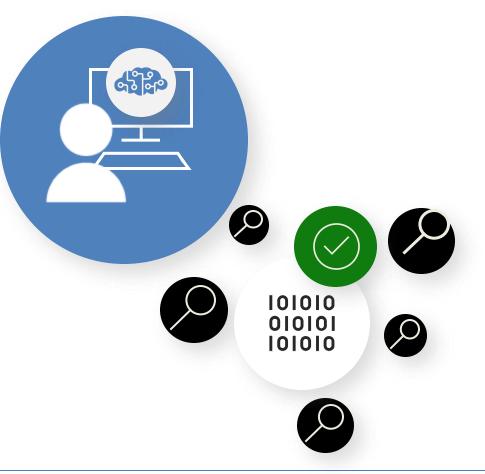
Tier 2 – Security Enhanced

Adding enhanced Visibility, Protection, and Insider Risk Management

Objectives

In addition to Security Essentials:

- Protect email against zero-day attacks and educate staff on how to identify phishing attempts – Microsoft Defender for Office 365
- Track and understand non-standard behaviours using Heuristics and Machine Learning – Microsoft Defender for Identity
- Track, Isolate, and Automate compromise remediation – Microsoft Defender for Endpoint
- Remove Shadow IT risks Microsoft Cloud App Security





Thank You