
INGRAM MICRO CLOUD
More as a Service
May 16 2023
Microsoft Defender for Business
Diego Lens
Ingram Micro Cloud BeNeLux
Start : 9h15
More as a Service

1


INGRAM MICRO CLOUD
More as a Service
MAY 16, 2023
Microsoft Defender for Business
Diego Lens
Ingram Micro Cloud BeNeLux
More as a Service

2

Diego Lens

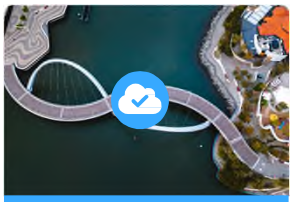
- 20 Years working in Distribution
- Cloud Enablement
- Technical Trainings
- Microsoft Azure
- Microsoft 365
- Azure Virtual Desktop

- diego.lens@ingrammicro.com
- **linkedin.com/in/diegolens**

3

Growth Solutions

INGRAM MICRO CLOUD
More as a Service

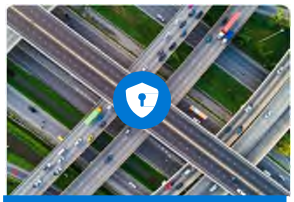


Modern Cloud Platforms

Transform Into the New Norm

Go boldly into the future with innovative infrastructure and platform solutions built for driving profitability and growth through key app modernization, data & insights, and cloud strategies.

- **App Modernization**
  DevOps, Containers, Microservices
  + Infrastructure
- **Data & Insights**
  DB (PaaS), Analytics, Warehousing, AI/ML
  + Infrastructure



Seamless Security

Build your Business with True Peace of Mind

Move forward towards a bright business future with total asset and data protection including seamless sign-on, endpoint security, identity security, and complete security operations management.

- **Endpoint**
  Modern Endpoint, MDR/XDR, Server Security
- **Identity**
  Authentication, Identity & Access Management
- **Security operations**
  Vulnerability Mng, Tier 2 SOC Analytics, SIEM

Connected Workplace

Together We Achieve More

Work together, work smarter and stay productive, from anywhere with our comprehensive suite of collaboration apps, digital experiences, and virtual desktops, designed to help you do more.

- **Collaboration Apps**
  Productivity Suits, conferencing
- **Virtual Desktops**
  Remote Work, Desktop Virtualization, OS
- **Employee Experience**
  Workflow insights, resources, learning

Business Performance

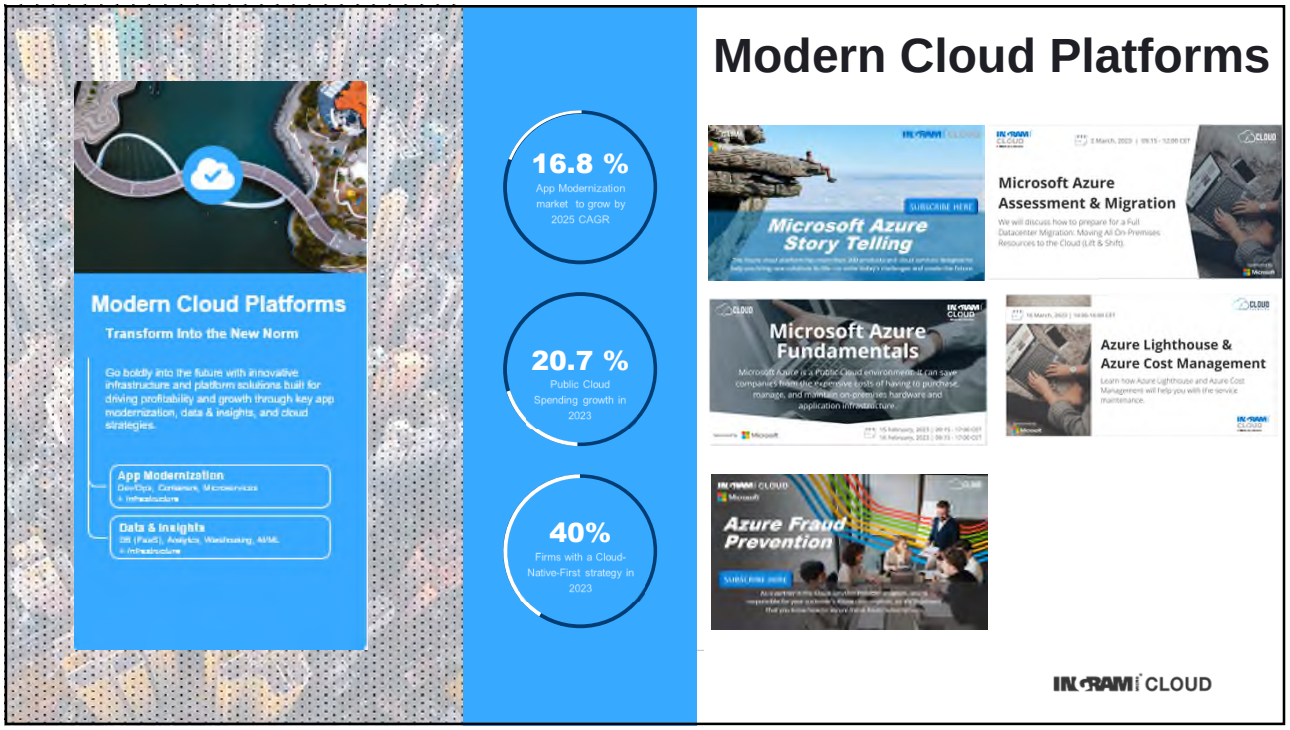
Work at the Speed of Modern Business

Build a fine-tuned business engine to power your performance with our tailor-made technological approach to equip your teams with CRM, ERP software, and imaginative workforce automation.

- **CRM**
  Customer Relationship Management
- **ERP**
  Enterprise Resource Planning
- **Workforce Automation**
  No/low Code, Power Automate

http://bit.ly/ingramcloud https://ingram.cloudchampion.nl https://ingram.cloudchampion.be

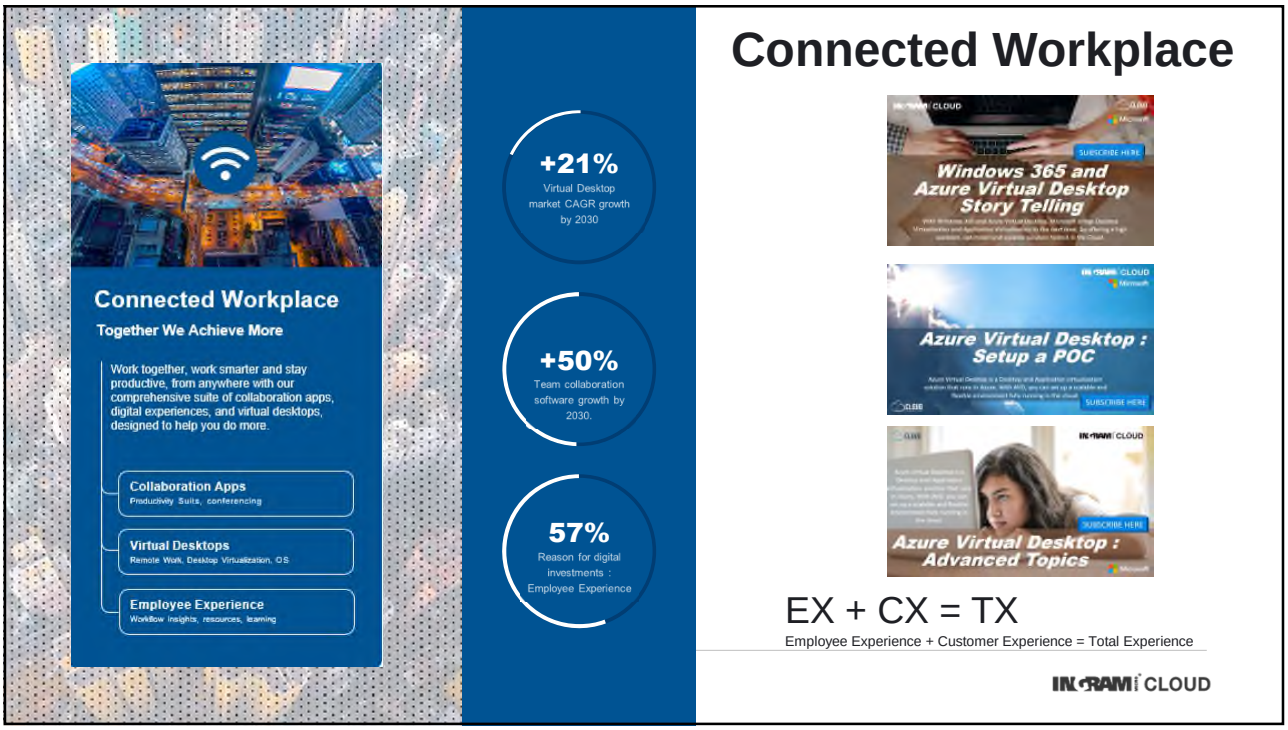
4


Modern Cloud Platforms
Transform Into the New Norm
Go boldly into the future with innovative infrastructure and platform solutions built for driving profitability and growth through key app modernization, data & insights, and cloud strategies.
App Modernization
Data & Insights
16.8 %
App Modernization market to grow by 2025 CAGR
20.7 %
Public Cloud Spending growth in 2023
40%
Firms with a Cloud-Native-First strategy in 2023
Modern Cloud Platforms
Microsoft Azure Story Telling
Microsoft Azure Assessment & Migration
Microsoft Azure Fundamentals
Azure Lighthouse & Azure Cost Management
Azure Fraud Prevention
INGRAM CLOUD

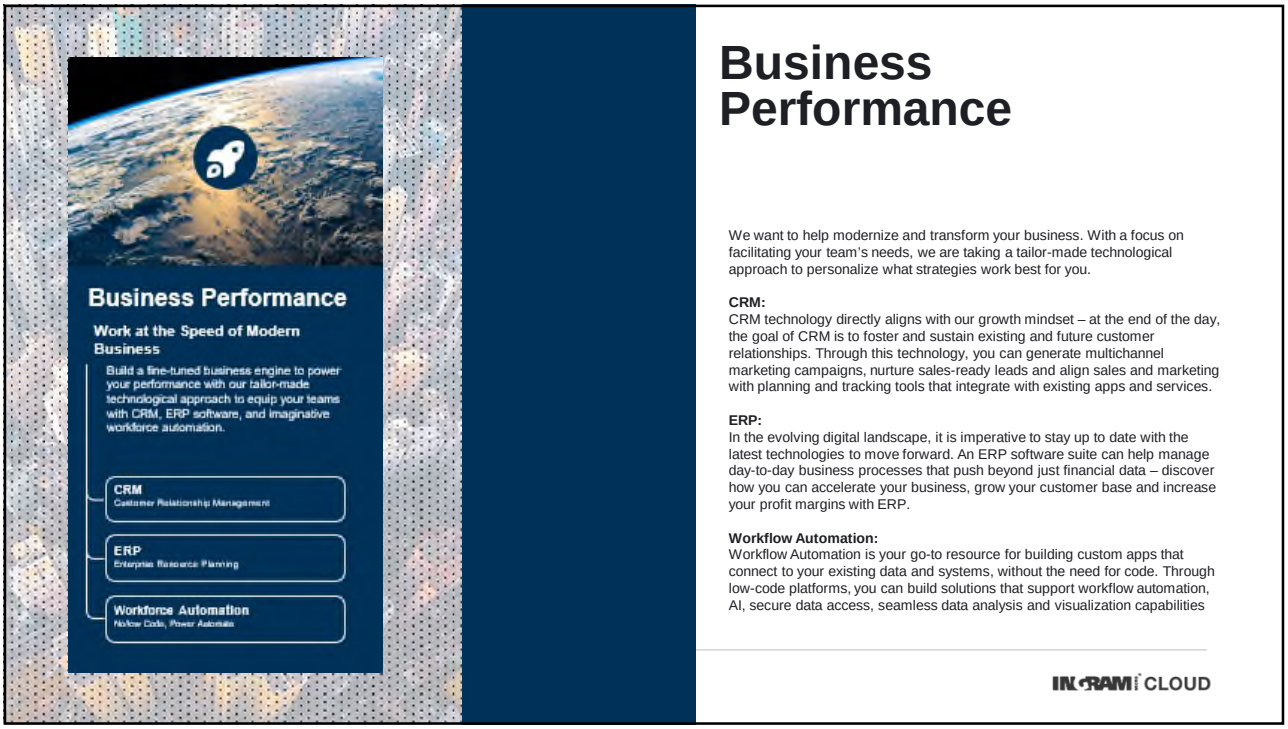
5


Seamless Security
Build your Business with True Peace of Mind
Move forward towards a bright business future with total asset and data protection including seamless sign-on, endpoint security, identity security, and complete security operations management.
Endpoint
Identity
Security operations
$129B
Cybersecurity Public Cloud Services Spend by 2025 Globally
+50%
organizations will be using MDR by 2025.
60%
security deployments are in the Public Cloud
Seamless Security
Microsoft 365 Security Story Telling
Microsoft 365 Defender for Business
Microsoft Entra
Microsoft Intune
Microsoft 365 Defender Suite
Microsoft Purview Information Protection
INGRAM CLOUD

6


Connected Workplace
Together We Achieve More
Work together, work smarter and stay productive, from anywhere with our comprehensive suite of collaboration apps, digital experiences, and virtual desktops, designed to help you do more.
Collaboration Apps
Productivity Suits, conferencing
Virtual Desktops
Remote Work, Desktop Virtualization, OS
Employee Experience
Workflow insights, resources, learning
+21%
Virtual Desktop market CAGR growth by 2030
+50%
Team collaboration software growth by 2030.
57%
Reason for digital investments : Employee Experience
Connected Workplace
Windows 365 and Azure Virtual Desktop Story Telling
Azure Virtual Desktop : Setup a POC
Azure Virtual Desktop : Advanced Topics
EX + CX = TX
Employee Experience + Customer Experience = Total Experience
INGRAM CLOUD

7


Business Performance
Work at the Speed of Modern Business
Build a fine-tuned business engine to power your performance with our tailor-made technological approach to equip your teams with CRM, ERP software, and imaginative workforce automation.
CRM
Customer Relationship Management
ERP
Enterprise Resource Planning
Workforce Automation
No/low Code, Power Automate
Business Performance
We want to help modernize and transform your business. With a focus on facilitating your team's needs, we are taking a tailor-made technological approach to personalize what strategies work best for you.
CRM:
CRM technology directly aligns with our growth mindset – at the end of the day, the goal of CRM is to foster and sustain existing and future customer relationships. Through this technology, you can generate multichannel marketing campaigns, nurture sales-ready leads and align sales and marketing with planning and tracking tools that integrate with existing apps and services.
ERP:
In the evolving digital landscape, it is imperative to stay up to date with the latest technologies to move forward. An ERP software suite can help manage day-to-day business processes that push beyond just financial data – discover how you can accelerate your business, grow your customer base and increase your profit margins with ERP.
Workflow Automation:
Workflow Automation is your go-to resource for building custom apps that connect to your existing data and systems, without the need for code. Through low-code platforms, you can build solutions that support workflow automation, AI, secure data access, seamless data analysis and visualization capabilities
INGRAM CLOUD

8

Ingram Micro Cloud Enablement 2023

Enablement
http://bit.ly/ingramcloud

Cloud Champion
https://ingram.cloudchampion.be
https://ingram.cloudchampion.nl

Newsletter
http://bit.ly/imc-email

INGRAM MICRO CLOUD More as a Service

9

9

Agenda

- Introduction MDB
- Cyber Security Frameworks
- Microsoft Defender for Business : Setup
- Endpoint Detection & Response (EDR)
- Automated Investigation (AIR)
- Advanced Features
- Threat Vulnerability Management (TVM)

INGRAM MICRO CLOUD

10

10

11

SMBs are increasingly a target of cyberattacks like ransomware

COVID-19 exploited by malicious cyber actors

"...groups and cybercriminals are targeting individuals, small and medium enterprises, and large organizations with COVID-19-related scams and phishing emails."

Department of Homeland Security, April 8, 2020, CISA Alert (AA20-099A)

Increase in ransomware attacks

"... small businesses comprise approximately one-half to three-quarters of the victims of ransomware," he said. Overall, ransomware attacks have been up almost 300% in the past year, he said. "

Homeland Security Secretary Alejandro Mayorkas, 06 May 2021 ABC report

1/3rd of all cyberattacks are targeted at small businesses.[1]

of small businesses that experienced a recent cyberattack were not able to operate.[2]

average cost of a SMB data breach.[3]

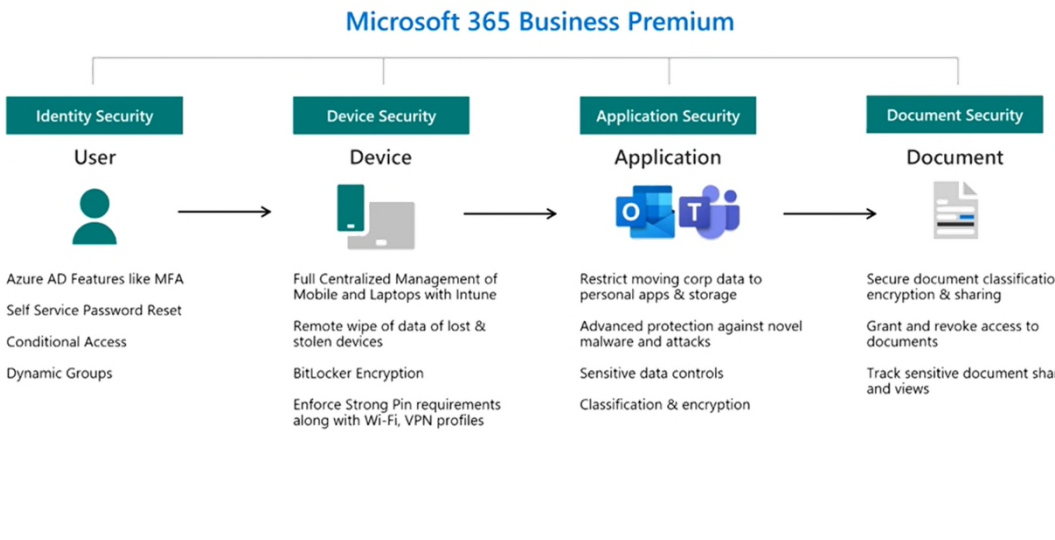
INGRAM MICRO CLOUD More as a Service

Source: 1 Introduction to the 2020 DBIR | Verizon Enterprise Solutions, 2 Microsoft commissioned Forrester Research, 2020, 3 Kaspersky Global Corporate IT Security Risks Survey, 2019

12

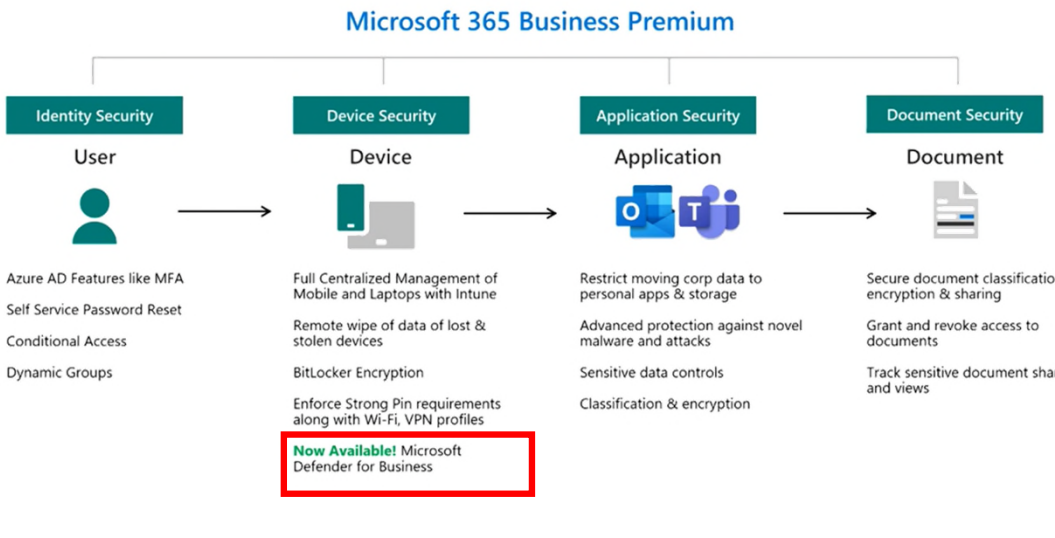
12

Sophisticated Attacks = Layered Security



13

Sophisticated Attacks = Layered Security



14

Device Security during the years

- Anti Virus (AV)
- Endpoint Protection Platform (EPP)
- Endpoint Detection and Response (EDR)

AV	EPP	EDR
Signature Based Protection	Machine Learning Based Protection	Endpoint Security Layer
Great for Known Threats	Prevents Known and Unknown Threats (Reactive)	Alert Triage & Remediation (Proactive)
Higher Resource Usage	Low Resource Usage	Contain – Investigate - Respond

Device Security Evolution

Windows Defender | Microsoft Defender for Endpoints Plan 2 (M365E5)

INGRAM MICRO CLOUD More as a Service

15

15

Microsoft Defender for Business

Now in Microsoft 365 Business Premium!

Elevate your security

Elevate your security with enterprise-grade endpoint protection specially built for businesses with up to 300 employees.

Enterprise-grade protection

Security for all your devices with next-gen protection, endpoint detection and response, and threat and vulnerability management.

Easy to use

Streamline onboarding with wizard-driven set up and recommended security policies activated out-of-the-box to quickly secure devices.

Cost-effective

Endpoint security that keeps you productive and works with your IT without compromising budget.

Microsoft Defender for Business now generally available in Microsoft 365 Business Premium. https://aka.ms/SMBsecurityFebBlog
Standalone available later this year.

INGRAM MICRO CLOUD More as a Service

16

16

How to purchase Microsoft Defender for Business

Available since MARCH, 1st 2022

Microsoft 365 Business Premium ($22pupm)[1]
Comprehensive productivity and security solution
Per user license

- Microsoft 365 Business Standard ($12.50)[1] Office apps and services, Teams
- \+
- Microsoft Defender for Business — New
- Microsoft Defender for Office 365 Plan 1
- Intune
- Azure AD Premium Plan 1
- Azure Information Protection Premium P1
- Exchange Online Archiving
- Autopilot
- Azure Virtual Desktop license
- Windows 10/11 Business
- Shared Computer Activation

Available since MAY, 2nd 2022

Microsoft Defender Business ($3pupm)[1,2]
Enterprise-grade endpoint security
Per user license

- ✓ Next generation protection
- ✓ Cross Platform support (iOS, Android, Windows, MacOS)[4]
- ✓ Endpoint Detection and Response
- ✓ Threat and Vulnerability Management
- ✓ ...and more

[1]price is subject to change based on subscription term, currency and region
[4]iOS, and Android requires Microsoft Endpoint Manager. Please see Documentation for more detail.

[2] Standalone General availability later this calendar year
[3]MDB is now rolling out to Business Premium customers

17

MDB brings many E5 capabilities to SMB

Cross platform and enterprise grade protection with next-gen protection, endpoint detection and response, and threat and vulnerability management

Available as a standalone offering and as part of Microsoft 365 Business Premium

Standalone offering will serve non-Microsoft 365 customers. **No licensing prerequisites**

Supports multi-customer viewing of security incidents with **Microsoft 365 Lighthouse** for partners in preview

Customer size	< 300 seats	> 300 seats	
Endpoint capabilities\SKU	Microsoft Defender for Business	Microsoft Defender for Endpoint Plan 1	Microsoft Defender for Endpoint Plan 2
Centralized management	✓	✓	✓
Simplified client configuration	✓		
Threat and Vulnerability Management	✓		✓
Attack Surface Reduction	✓	✓	✓
Next-Gen Protection	✓	✓	✓
Endpoint Detection and Response	✓[2]		✓
Automated Investigation and Response	✓[2]		✓
Threat Hunting and 6-months data retention			✓
Threat Analytics	✓[2]		✓
Cross platform support for Windows, MacOS, iOS, and Android	✓	✓	✓
Microsoft Threat Experts			✓
Partner APIs	✓	✓	✓
Microsoft 365 Lighthouse for viewing security incidents across customers	✓[3]		

[1]Limited. [2]Optimized for SMB. [3]Additional capabilities planned

INGRAM MICRO CLOUD More as a Service

18

MDB brings many E5 capabilities to SMB

Cross platform and enterprise grade protection with next-gen protection, endpoint detection and response, and threat and vulnerability management	Available as a standalone offering and as part of Microsoft 365 Business Premium	Standalone offering will serve non-Microsoft 365 customers. No licensing prerequisites	Supports multi-customer viewing of security incidents with Microsoft 365 Lighthouse for partners in preview

Customer size	< 300 seats	> 300 seats	
Endpoint capabilities\SKU	Microsoft Defender for Business	Microsoft Defender for Endpoint Plan 1	Microsoft Defender for Endpoint Plan 2
Centralized management	✓	✓	✓
Simplified client configuration	✓		
Threat and Vulnerability Management	✓		✓
Attack Surface Reduction	✓	✓	✓
Next-Gen Protection	✓	✓	✓
Endpoint Detection and Response	✓[2]		✓
Automated Investigation and Response	✓[2]		✓
Threat Hunting and 6-months data retention			✓
Threat Analytics	✓[2]		✓
Cross platform support for Windows, MacOS, iOS, and Android	✓	✓	✓
Microsoft Threat Experts			✓
Partner APIs	✓	✓	✓
Microsoft 365 Lighthouse for viewing security incidents across customers	✓[3]		

Optimized for SMB

[1]Limited. [2]Optimized for SMB. [3]Additional capabilities planned

INGRAM MICRO CLOUD More as a Service

19

Microsoft Defender for Business Servers

- Announced on July 13, 2022
- At this moment in Preview
- Endpoint Security for :
  - Windows Servers
  - Linux Servers

NEW

Throughout the duration of the preview, server protection can be activated within the Microsoft 365 Defender security admin portal at no cost. The preview will end when general availability is announced. At that time, a Microsoft Defender for Business servers license must be purchased for each onboarded server, or those servers can be offboarded.

- At GA : Microsoft Defender for Business Servers Add-On : $3/Server

https://techcommunity.microsoft.com/t5/small-and-medium-business-blog/server-protection-for-small-business-now-in-preview-with/ba-p/3571185

INGRAM MICRO CLOUD More as a Service

20

20

Microsoft Defender for Business

Elevate your security

- Threat & Vulnerability Management
- Attack Surface Reduction
- Next Generation Protection
- Endpoint Detection & Response
- Auto Investigation & Remediation

Simplified Onboarding and Administration

APIs and Integration

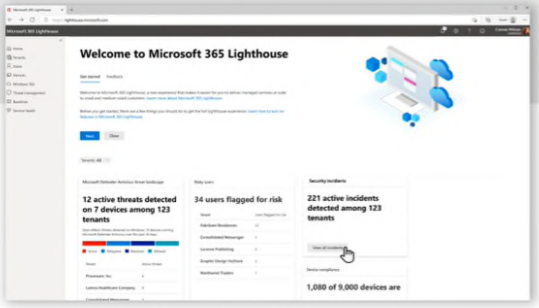
INGRAM MICRO CLOUD More as a Service

21

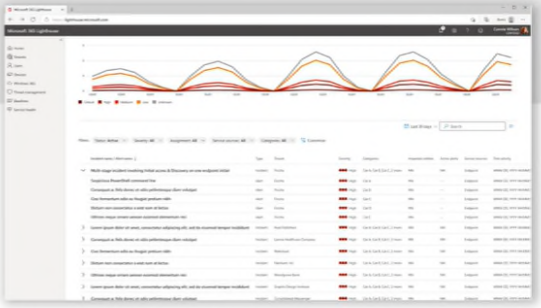
21

Microsoft 365 Lighthouse and MDB

View security incidents and alerts from Defender for Business in the dashboard and get the detail from the Incidents queue. Additional security management capabilities are planned on the roadmap.



Security incident summary on the Home dashboard



Incident queue highlighting security incidents and alert details

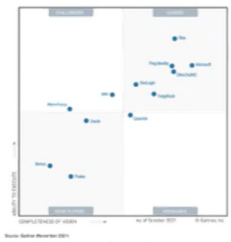
INGRAM MICRO CLOUD More as a Service

22

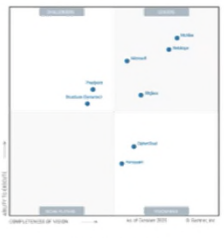
22

Gartner

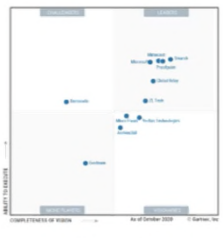
Microsoft Security— a Leader in 5 Gartner Magic Quadrant reports



Access Management

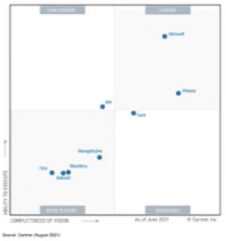


Cloud Access Security Brokers



Enterprise Information Archiving

Endpoint Protection Platforms



Unified Endpoint Management

"Gartner "Magic Quadrant for Access Management," by Henrique Teixeira, Abhyuday Data, Michael Kelley, November 2021
"Gartner " Magic Quadrant for Cloud Access Security Brokers," by Craig Lawson, Steve Riley, October 2020
"Gartner " Magic Quadrant for Enterprise Information Archiving," by Michael Hoech, Jeff Vogel, October 2020
"Gartner "Magic Quadrant for Endpoint Protection Platforms," by Paul Webber, Rob Smith, Prateek Bhajanka, Mark Harris, Peter Firstbrook, May 2021
"Gartner "Magic Quadrant for Unified Endpoint Management," by Dan Wilson, Chris Silva, Tom Cipolla, August 2021

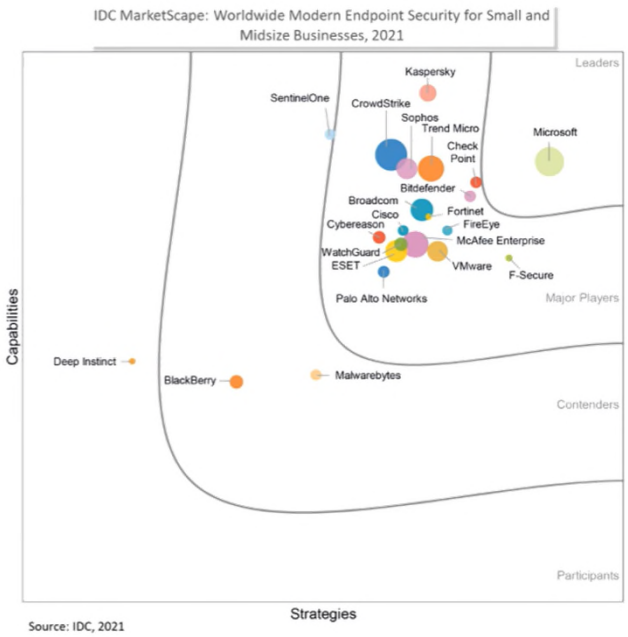
These graphics were published by Gartner, Inc. as part of larger research documents and should be evaluated in the context of the entire documents. The Gartner documents are available upon request from Microsoft. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

INGRAM MICRO CLOUD More as a Service

23

23

Microsoft named a Leader in IDC MarketScape for Modern Endpoint Security for Enterprise and Small and Midsize Businesses



Source: IDC, 2021

IDC MarketScape: Worldwide Modern Endpoint Security for Small and Midsize Businesses
2021 Vendor Assessment https://idcdocserv.com/US48304721
IDC MarketScape vendor analysis model is designed to provide an overview of the competitive fitness of information and communication technology (ICT) suppliers in a given market. The research methodology utilizes a rigorous scoring methodology based on both qualitative and quantitative criteria that results in a single graphical illustration of each vendor's position within a given market. The Capabilities score measures vendor product, go-to-market, and business execution in the short term. The Strategy score measures alignment of vendor strategies with customer requirements in a three to five-year timeframe. Vendor market share is represented by the size of the icons.

Microsoft named a Leader in IDC MarketScape for Modern Endpoint Security for Enterprise and Small and Midsize Businesses - Microsoft Security Blog

INGRAM MICRO CLOUD More as a Service

24

24


Microsoft
Defender for
Business
LAB 0:
Create a Windows 10 virtual
Test PC
INGRAM MICRO CLOUD
25

25


INGRAM MICRO CLOUD
More as a Service
Zero Trust Security Model
&
Cyber Security Frameworks
More as a Service™

26

Zero Trust Security Model

https://docs.microsoft.com/en-us/security/zero-trust/

27

27

Principles of Zero Trust

Instead of assuming everything behind the corporate firewall is safe, Zero Trust assumes *an open environment where trust must be validated*

Assume breach – Assume that attackers will succeed (partially or fully) and design accordingly

Verify explicitly – Validate trust of users, devices, applications, and more using data/telemetry

Use least privileged access – to limit the impact of any given compromise

28

28

Zero Trust Components

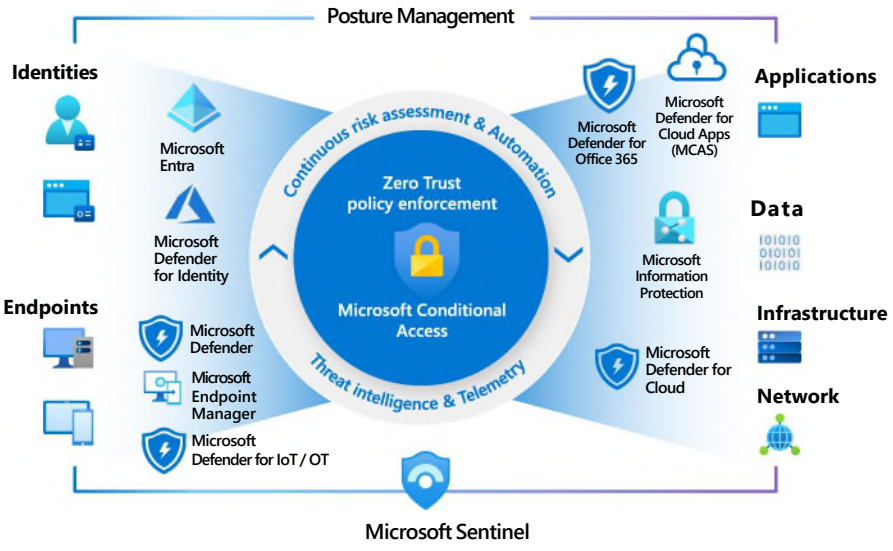
- Identities
- Endpoints
- Applications
- Data
- Infrastructure
- Network

INGRAM MICRO CLOUD More as a Service

29

29

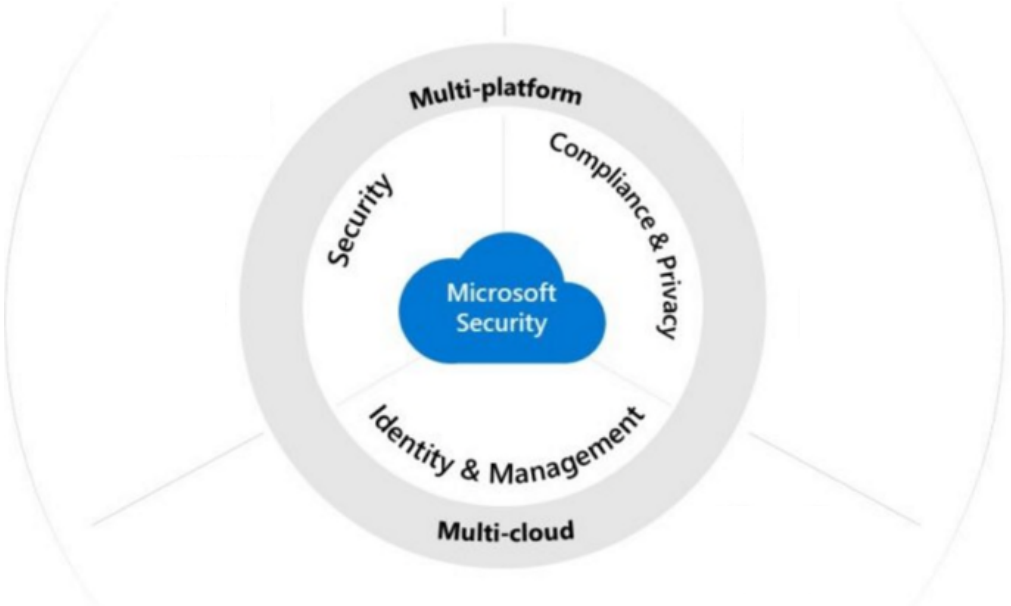
Microsoft Zero Trust Capabilities



INGRAM MICRO CLOUD

30

Six Security Product Families

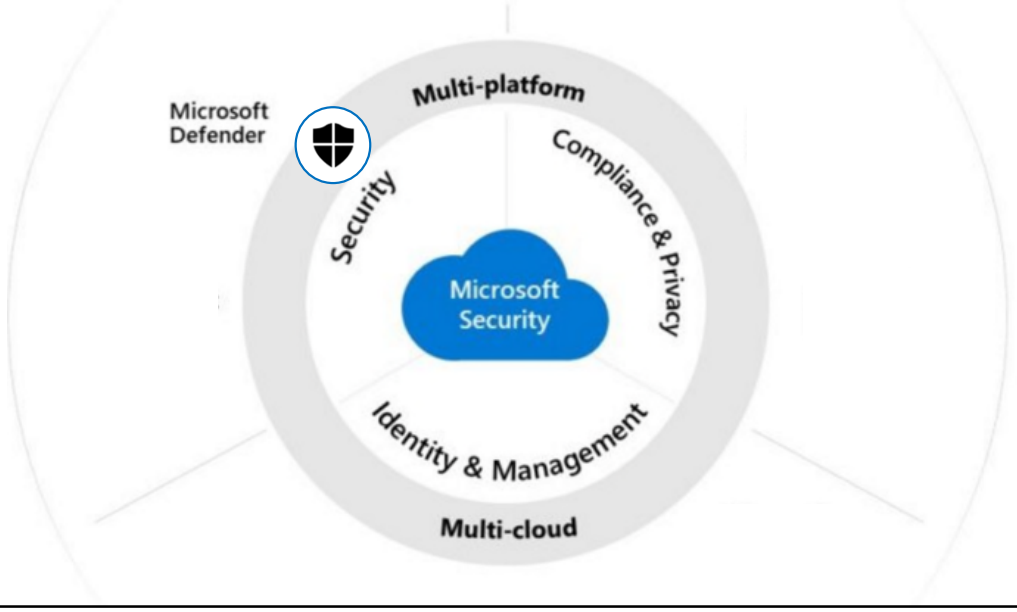


INGRAM MICRO CLOUD More as a Service

31

31

Microsoft Defender

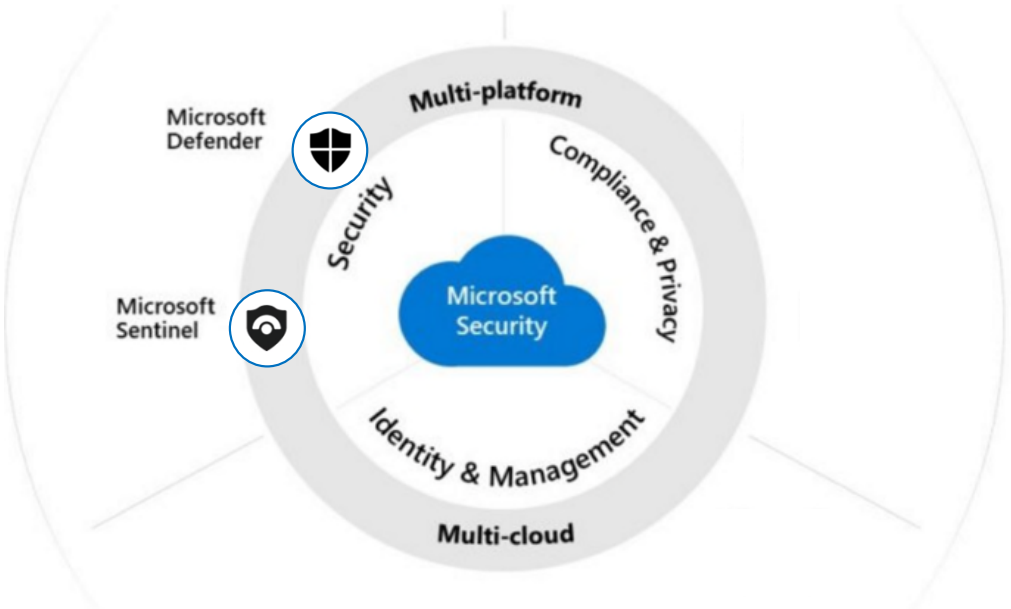


INGRAM MICRO CLOUD More as a Service

32

32

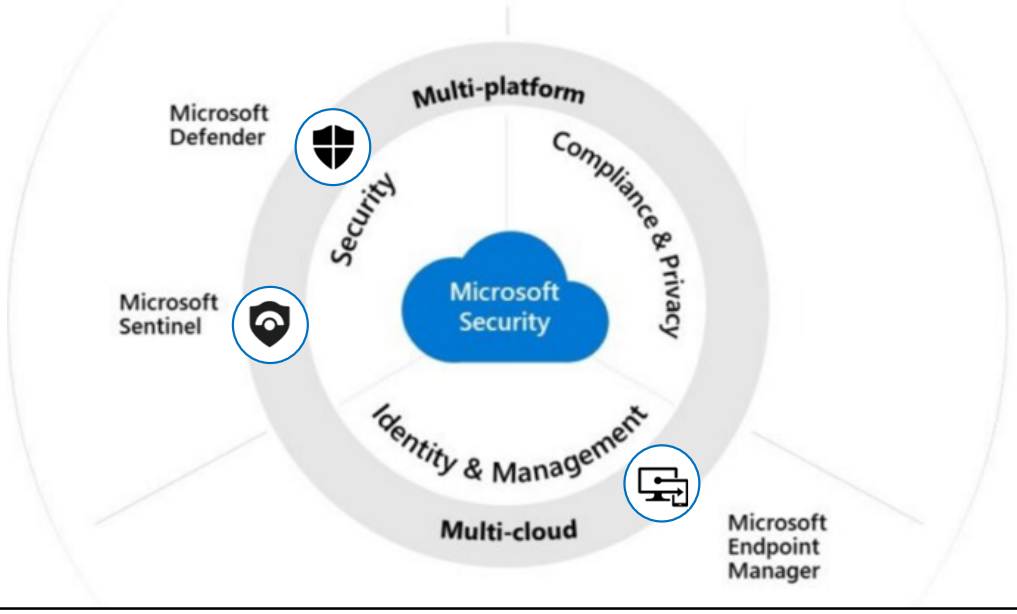
Microsoft Sentinel



33

33

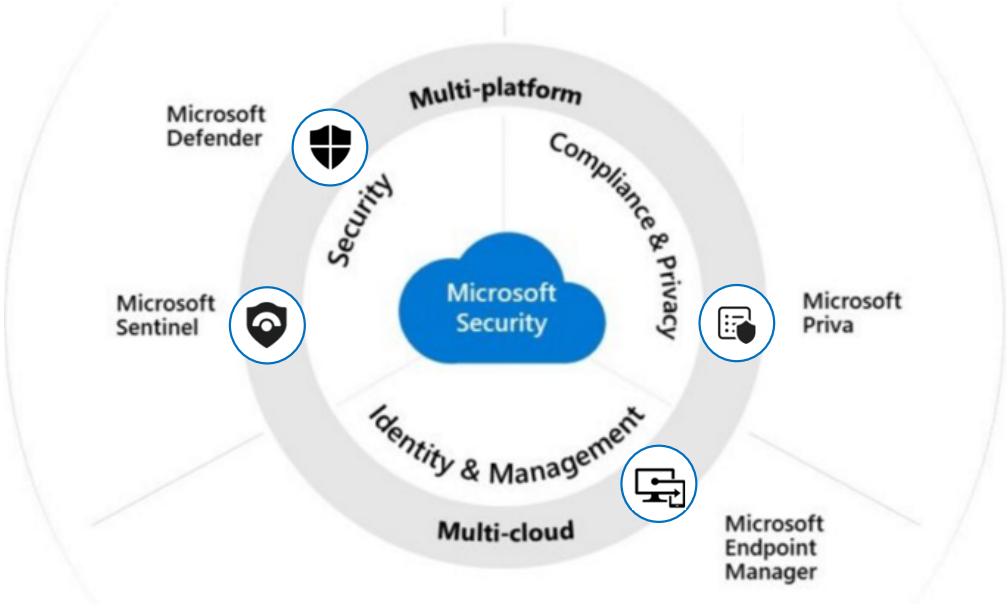
Microsoft Endpoint Manager



34

34

Microsoft Priva



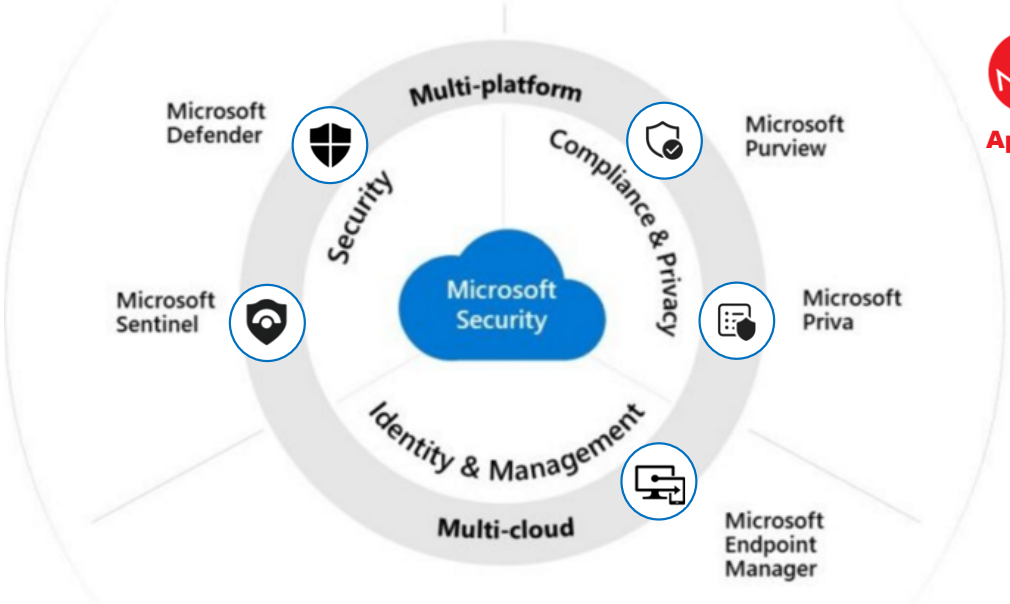
NEW
Jan '22

INGRAM MICRO CLOUD More as a Service

35

35

Microsoft Purview



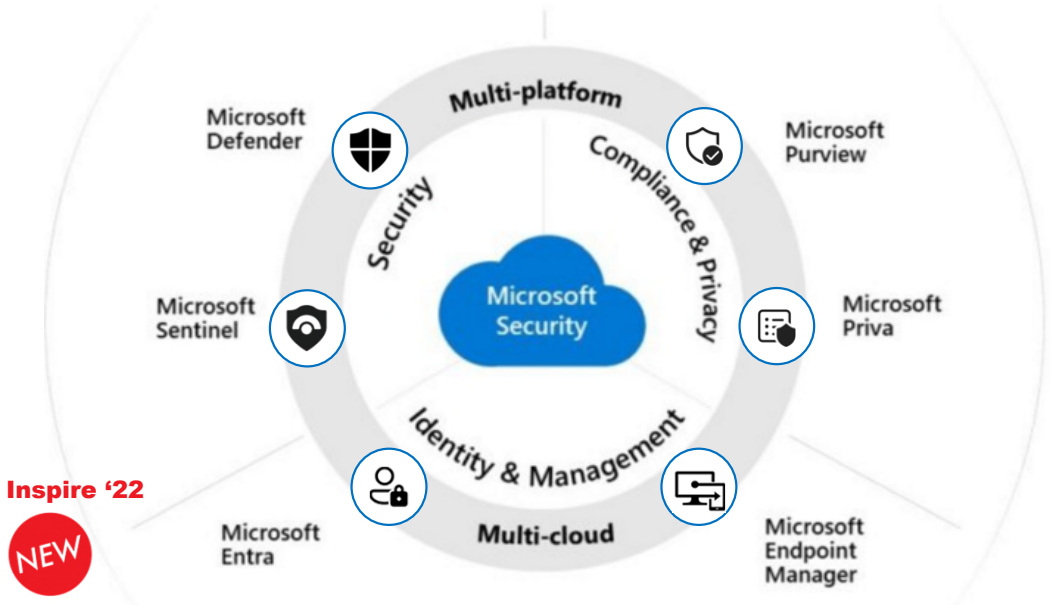
NEW
Apr '22

INGRAM MICRO CLOUD More as a Service

36

36

Microsoft Entra



Inspire '22

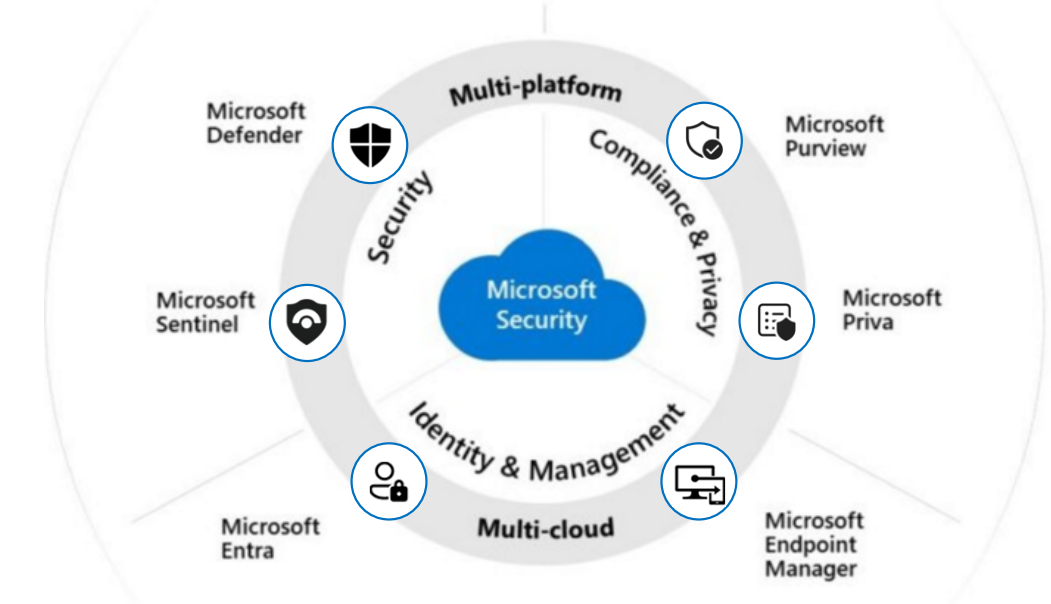
NEW

INGRAM MICRO CLOUD More as a Service

37

37

Six Security Product Families



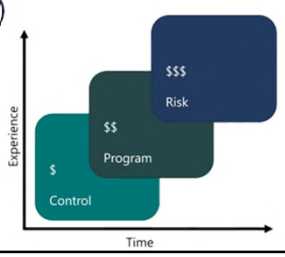
INGRAM MICRO CLOUD More as a Service

38

38

What is a Cybersecurity Framework

- A methodology to protect your digital assets
- A system of standards, guidelines and best practices
- A way to comply with industry regulations
- Three types of Frameworks
  - Control Frameworks (baseline set of controls)
  - Program Frameworks (comprehensive security program)
  - Risk Frameworks (risk management)



INGRAM MICRO CLOUD More as a Service

39

39

Cyber Security Frameworks

- CIS Top 18 Controls

CIS Center for Internet Security

Controls

- NIST CSF
- ISO 27001

Program

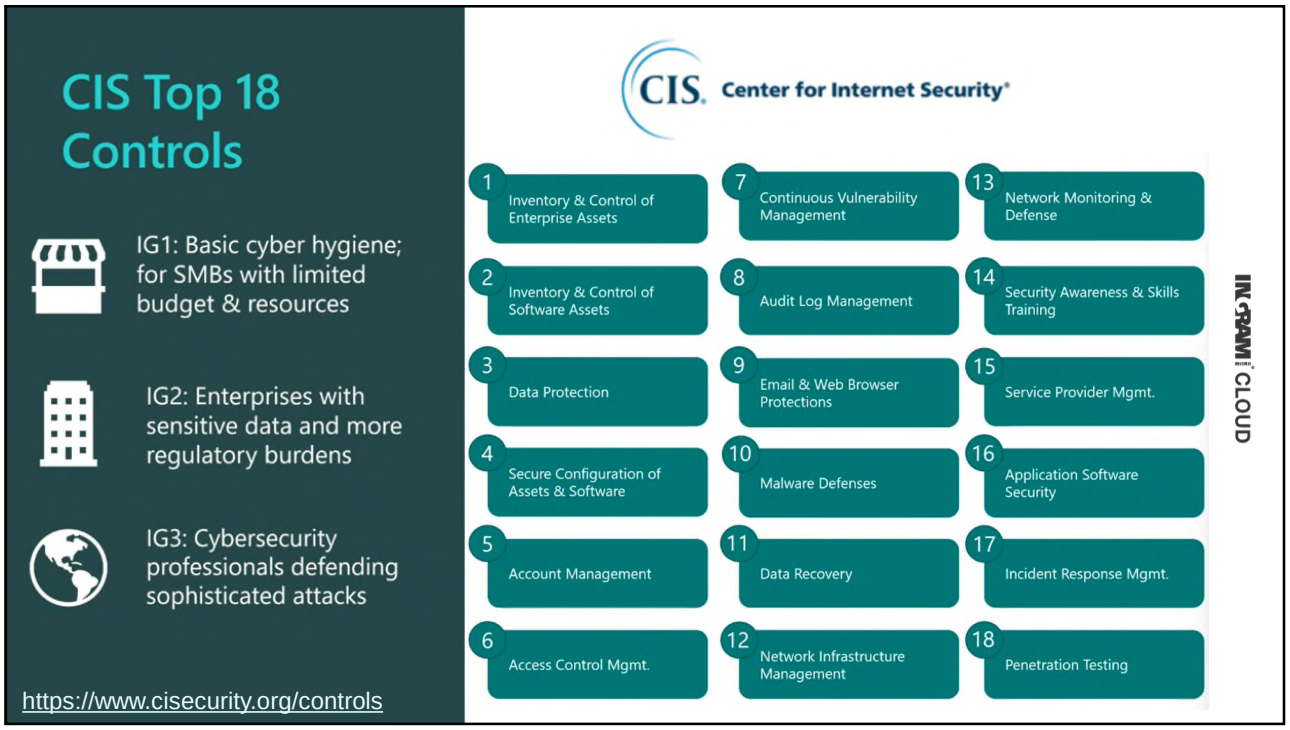
- CIS RAM
- ISO 27005

Risk

INGRAM MICRO CLOUD More as a Service

40

40


CIS Top 18 Controls
IG1: Basic cyber hygiene; for SMBs with limited budget & resources
IG2: Enterprises with sensitive data and more regulatory burdens
IG3: Cybersecurity professionals defending sophisticated attacks
https://www.cisecurity.org/controls
CIS Center for Internet Security
1 Inventory & Control of Enterprise Assets
2 Inventory & Control of Software Assets
3 Data Protection
4 Secure Configuration of Assets & Software
5 Account Management
6 Access Control Mgmt.
7 Continuous Vulnerability Management
8 Audit Log Management
9 Email & Web Browser Protections
10 Malware Defenses
11 Data Recovery
12 Network Infrastructure Management
13 Network Monitoring & Defense
14 Security Awareness & Skills Training
15 Service Provider Mgmt.
16 Application Software Security
17 Incident Response Mgmt.
18 Penetration Testing
INGRAM MICRO CLOUD

41


Check Categories
1. Tenant Setup
2. Identity Protection
3. Email Protection
4. Information Governance
5. Teams Security
6. Manage Devices
7. Endpoint Protection
8. Secure Remote Access
INGRAM MICRO CLOUD
More as a Service
42

42

Tenant Setup

	CIS Controls reference	Recommend settings	Recommended settings *High risk*
Decide between hybrid & cloud-only identity	N/A	Hybrid, Azure AD Connect	Hybrid, Azure AD Connect
Azure AD Connect - sign-in method	5.6, 6.7	Password Hash Sync	Password Hash Sync
Azure AD Connect - single sign-on	5.6, 6.7	Enabled	Enabled
Azure AD Connect - On-premises attribute for Azure AD username	5.6, 6.7	userPrincipalName	userPrincipalName
Azure AD Connect - Password writeback	N/A	Enabled	Enabled
Decide on email migration strategy	N/A	Hybrid Agent	Hybrid Agent
Configure DNS domains	N/A	List	List

INGRAM MICRO CLOUD More as a Service

43

43

Identity Protection

	CIS Controls reference	Recommend settings	Recommended settings *High risk*
Plan for administrative access	5.4	Required	Required
Configure dedicated admin accounts	5.4	Recommended	*Required*
Multi-factor authentication (MFA) for admins*	6.5	Required; Security defaults	Required; *Conditional Access*
Multi-factor authentication (MFA) for users*	6.3	Required; Security defaults	Required; *Conditional Access*
Self-service password reset (SSPR)	N/A	Enabled-All	Enabled-All
Block legacy authentication*	6.3	Enabled; Security defaults	Enabled; *Conditional Access*

INGRAM MICRO CLOUD More as a Service

44

44

Email Protection

	CIS Controls reference	Recommend Settings	Recommended Settings *High Risk*
Enable Defender for Office 365 Preset policies (Exchange Online Protection, Anti-phishing, Safe Links, and Safe Attachments)	9.7	Standard	Strict
Enable transport rule for attachments with Office macro extension	9.6	Warn	*Block*
Block auto-forwarded email	N/A	All Users	All Users
Enable Sender Policy Framework (SPF)	9.5	All domains	All domains
Enable DomainKeys Identified Mail (DKIM) signing	9.5	All domains	All domains
Enable DMARC policy	9.5	Enabled, quarantine	Enabled, *reject*
Enable Common Attachment Types filter	9.6	Preset, standard	Preset, *strict*
Enable safe attachments for SharePoint, OneDrive and Microsoft Teams	9.7	Preset, built-in	Preset, built-in

INGRAM MICRO CLOUD More as a Service

45

45

Information Governance

	CIS Controls reference	Recommend Settings	Recommended Settings *High Risk*
Set up Data Loss Prevention (DLP)	3.13	Recommended, using default policy	*Enabled for sensitive data types (GLBA, HIPAA, etc.)*
Enable email encryption	3.10	Office 365 Message Encryption	*Sensitivity Labels*
Enable retention policies	3.4	Optional	*Enabled with automatic deletion*
Enable sensitivity labels	3.7	Optional	*Required, Unified labels*

INGRAM MICRO CLOUD More as a Service

46

46

Teams Security

	CIS Controls reference	Recommend Settings	Recommended Settings *High Risk*
Allow users to create teams	3.3, 6.1	Default behavior	Restrict groups settings
Guest access	5.1, 6.1	Enabled	Enabled
External chat	N/A	Allowed (Default)	Restricted
3rd party cloud storage	3.2	Defaults	Off
Meeting policy and settings	N/A	Defaults	Block anonymous
Messaging policy	N/A	Defaults	Defaults
OneDrive for Business sharing	3.3	Anyone	Require login
Migrate files to Teams & OneDrive for Business	3.2	Required	Required
Teams app permission policy	2.1, 2.3	Default policy (Allow all apps)	Allow only specific apps

INGRAM MICRO CLOUD More as a Service

47

47

Manage Devices

	CIS Controls reference	Recommend Settings	Recommended Settings *High Risk*
Onboard existing Active Directory joined PCs	1.1, 4.11	Hybrid Azure AD Join	Hybrid Azure AD Join
Provision new/refreshed company PCs	1.1, 4.11	Azure AD join with Autopilot	Azure AD join With Autopilot
Onboard iOS and Android devices	1.1, 4.11, 4.12	Company Portal app	Apple Business Manager, Android zero-touch and Company Portal
Deploy Microsoft 365 apps	N/A	Required-all users on Windows, iOS, macOS, and Android	Required-all users on Windows, iOS, macOS, and Android
Enable enterprise state roaming	N/A	All-Users	All-Users
Configure app protection policies for company owned PCs	4.11	Enabled, encrypt data only	Enabled, encrypt data + block relocation
Block/Allow access from employee-owned mobile devices	4.11, 4.12	Allowed, default app protection policy	Block client app access, block web downloads
Block/Allow access from employee-owned PCs	4.11, 4.12	Block client app access, block web downloads	Block client app access, block web downloads
Enable device configuration profiles	4.1, 4.3, 4.6, 4.10	Basic config profile	Endpoint security profiles
Enable device compliance policies	1.2, 4.6	Optional	Enforced, Conditional Access

INGRAM MICRO CLOUD More as a Service

48

48

Endpoint Protection

	CIS Controls reference	Recommend Settings	Recommended Settings *High Risk*
Windows Defender firewall policy	4.5	Default policy	Default policy
Windows Defender Next-gen protection policy	10.1	Default policy, Block mode	Default policy, Block mode
Email notifications	13.11	Alerts & vulnerabilities	Microsoft Sentinel
Automated investigation & response	10.7, 13.7	On	On
Compliance policy	10.7	Devices must have Low risk score, enforced with Conditional Access	Devices must have Clear risk score, enforced with Conditional Access
Attack surface reduction rules	10.5	Audit	Block
App and browser isolation	10.5	Off	Enabled – Windows network isolation for approved IP addresses and cloud resources
Device Control	10.3	Off	Block removable storage
Application Control	2.5-2.7	Audit	Enforce Components, Store Apps, and SmartLocker

INGRAM MICRO CLOUD More as a Service

49

49

Secure Remote Access

	CIS Controls reference	Recommend Settings	Recommended Settings High Risk
Access on-premises desktop apps & data	12.7, 13.5	Split-tunnel VPN	Azure Virtual Desktop
Secure access to 3rd party cloud apps	5.6, 6.3, 6.6., 6.7	Azure AD Single sign-on (SSO)	Azure AD Single sign-on (SSO)
Secure access to on-premises web apps	12.3	Azure AD App proxy	Azure AD App proxy

https://techcommunity.microsoft.com/t5/small-and-medium-business-blog/guide-to-implementing-cis-controls-with-microsoft-365-business/ba-p/1610358

INGRAM MICRO CLOUD More as a Service

50

50

CIS Microsoft 365 Foundation Benchmarks

INGRAM MICRO CLOUD More as a Service

51

51

Remediation Settings

1. Select `Admin Centers` and `Exchange`.
2. Click on the `Classic Exchange admin center` at the bottom.
3. Select `permissions` from the Exchange navigation pane.
4. Select `user roles`.
5. De-Select `My Custom Apps` `My Marketplace Apps` and `My ReadWriteMailboxApps`.

To prohibit users installing Outlook add-ins, use the Microsoft Online PowerShell Module:

1. Connect to Microsoft Online service using `Connect-MSOLService`.
2. Run the following Microsoft Online PowerShell command:

```
$newPolicyName = "Role Assignment Policy - Prevent Add-ins"
$revisedRoles = "MyTeamMailboxes", "MyTextMessaging", "MyDistributionGroups",
"MyMailSubscriptions", "MyBaseOptions", "MyVoiceMail",
"MyProfileInformation", "MyContactInformation", "MyRetentionPolicies",
"MyDistributionGroupMembership"

New-RoleAssignmentPolicy -Name $newPolicyName -Roles $revisedRoles
Set-RoleAssignmentPolicy -id $newPolicyName -IsDefault
Get-Mailbox -ResultSize Unlimited | Set-Mailbox -RoleAssignmentPolicy
$newPolicyName
```

If you have other Role Assignment Policies modify the last line to filter out your custom policies

Default Value:

UI - `My Custom Apps` is `Checked`, `My Marketplace Apps` is `Checked`, and `My ReadWriteMailboxApps` is `Checked`

PowerShell - `My Custom Apps` `My Marketplace Apps` and `My ReadWriteMailboxApps` are `Present`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.1 Establish and Maintain a Software Inventory Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	●	●	●
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

https://downloads.cisecurity.org/#/

INGRAM MICRO CLOUD More as a Service

52

52

NIS2 Directives

- NIS : Network and Information Security (EU)
- NIS2 Strengthens security requirements in the EU
- High common level of cybersecurity across the European Union
- Supersedes the first NIS

53

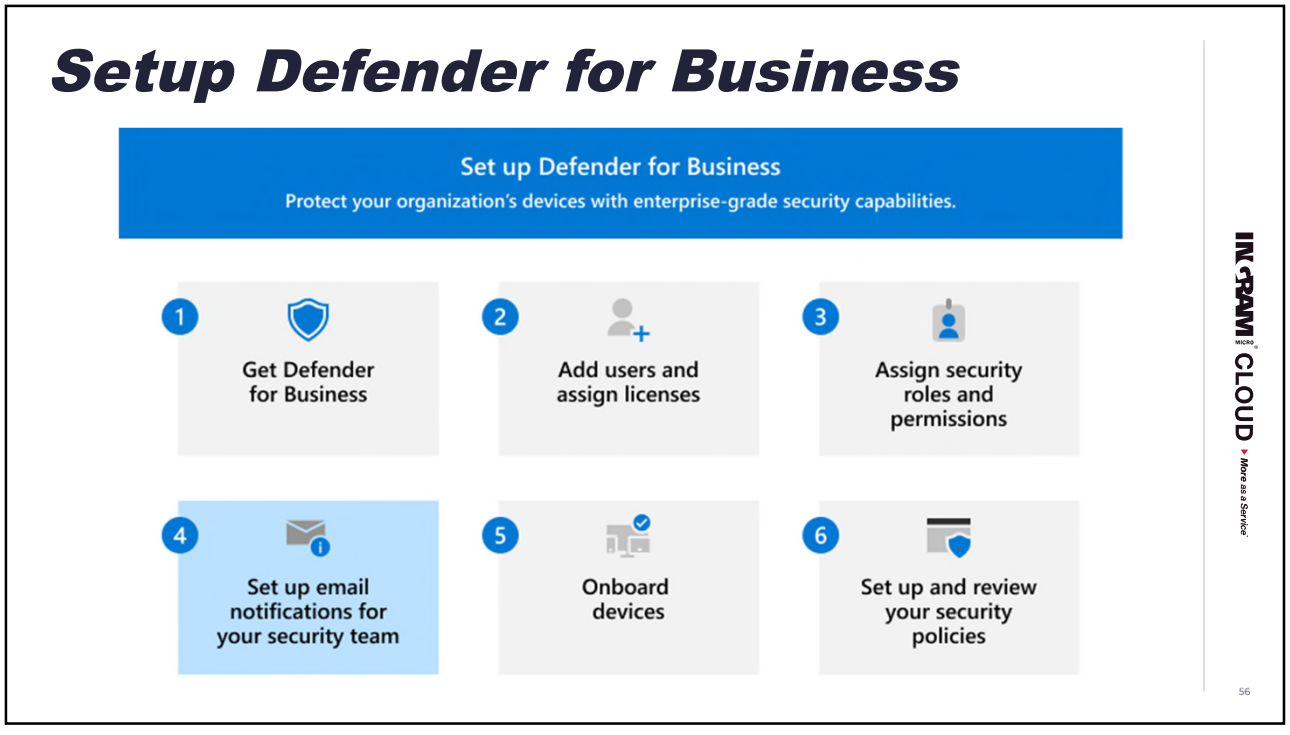
53

54

54


INGRAM MICRO CLOUD
More as a Service
Microsoft Defender for Business:
Setup
More as a Service™

55


Setup Defender for Business
Set up Defender for Business
Protect your organization's devices with enterprise-grade security capabilities.
1
Get Defender for Business
2
Add users and assign licenses
3
Assign security roles and permissions
4
Set up email notifications for your security team
5
Onboard devices
6
Set up and review your security policies
INGRAM MICRO CLOUD
More as a Service
56

56

1. Prerequisites

- Subscription
  - Microsoft 365 Business Premium

  or
  - Microsoft Defender for Business (standalone)
- Datacenter locations
  - European Union, United Kingdom, United States
- User & Permissions
  - To Sign up : Global Admin
  - To Access M365 Defender Portal : Security Admin or Security Reader
- Managed Devices : W10 Business, Professional, Enterprise, MACOS

  *(*Servers later this year)*

https://docs.microsoft.com/en-us/microsoft-365/security/defender-business/mdb-onboard-devices?view=o365-worldwide&tabs=WindowsClientDevices

57

57

2. Assign Roles

- https://security.microsoft.com

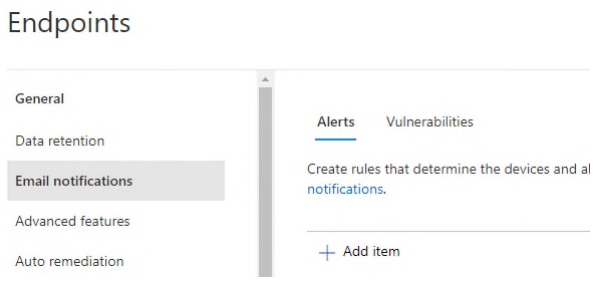
Permission level	Description
Global administrators (also referred to as global admins) *As a best practice, limit the number of global admins.*	Global admins can perform all kinds of tasks. The person who signed up your company for Microsoft 365 or for Microsoft Defender for Business is a global administrator by default. Global admins are able to access/change settings across all Microsoft 365 portals, such as: - The Microsoft 365 admin center (https://admin.microsoft.com) - Microsoft 365 Defender portal (https://security.microsoft.com)
Security administrators (also referred to as security admins)	Security admins can perform the following tasks: - View and manage security policies - View and manage security threats and alerts (these activities include taking response actions on endpoints) - View security information and reports
Security reader	Security readers can perform the following tasks: - View security policies - View security threats and alerts - View security information and reports

58

58

3. Security Notifications

- When new exploits or vulnerabilities are detected
- Email notifications is ONE of the notification options
- Change Notification Settings :
  - https://security.microsoft.com > Settings > Endpoints > General > Email

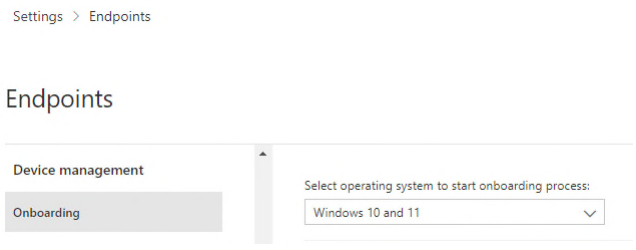


59

59

4. Onboard Devices to MDB

- Local Script
- Group Policy
- Microsoft Intune (only of subscription is M365 Business Premium)
- Automatic enrollment

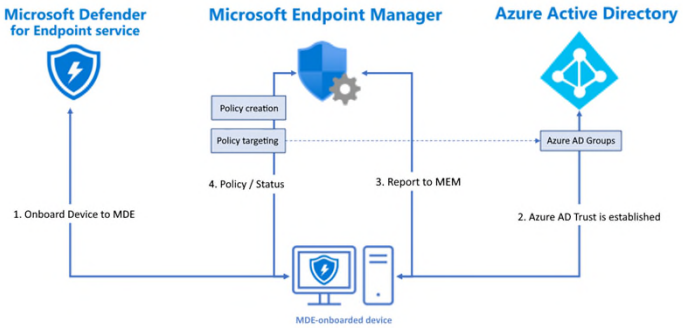


60

60

5a. Configure Security Policies

- Choose where to manage security policies
  - Microsoft 365 Defender portal
  - Microsoft Endpoint Manager Admin Center



61

61

5b. Next-Generation Protection Policy

Device configuration > Next-generation protection > NGP Windows default policy

Next-generation protection includes antivirus and antimalware protection to protect your devices. Review and configure your next-generation protection settings. Keep your default settings or change them to suit your organization's needs. Learn more about Next-generation protection settings.

Reset to default

Real-time protection

Turn on real time protection
Enforce monitoring and prevent users from disabling real-time protection. Real-time protection locates and stops malware from running on devices.
On

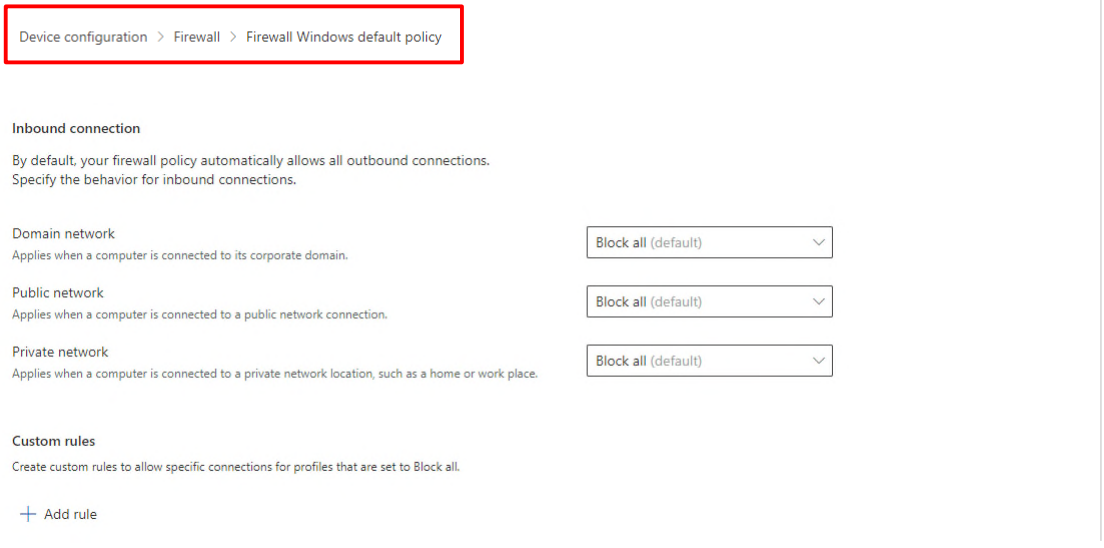
Block at first sight
Detects and blocks malware within seconds. Increases your sample submission timeout to 50 seconds and sets your detection level to High.
On

Turn on network protection
Prevent users from disabling network protection. Protects against phishing scams, exploit-hosting sites, and malicious content on the Internet.
Block mode (default)

62

62

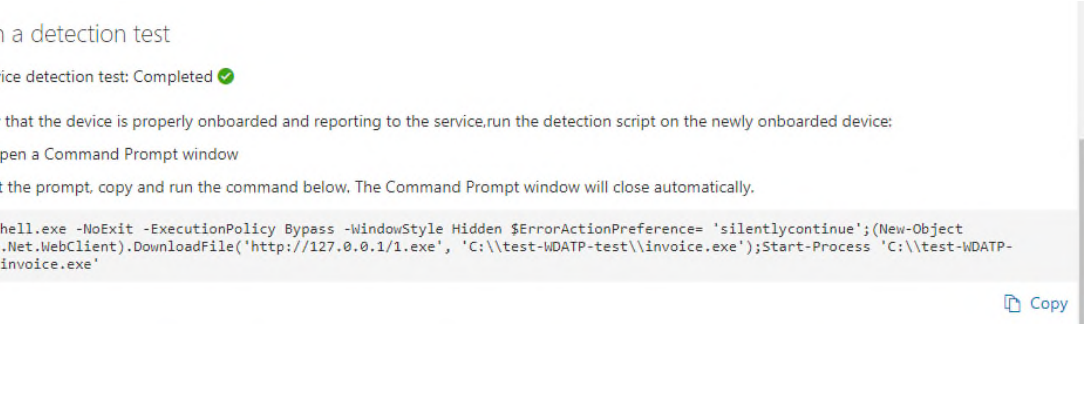
5c. Firewall Policy & Custom Rules



63

63

Run a detection test

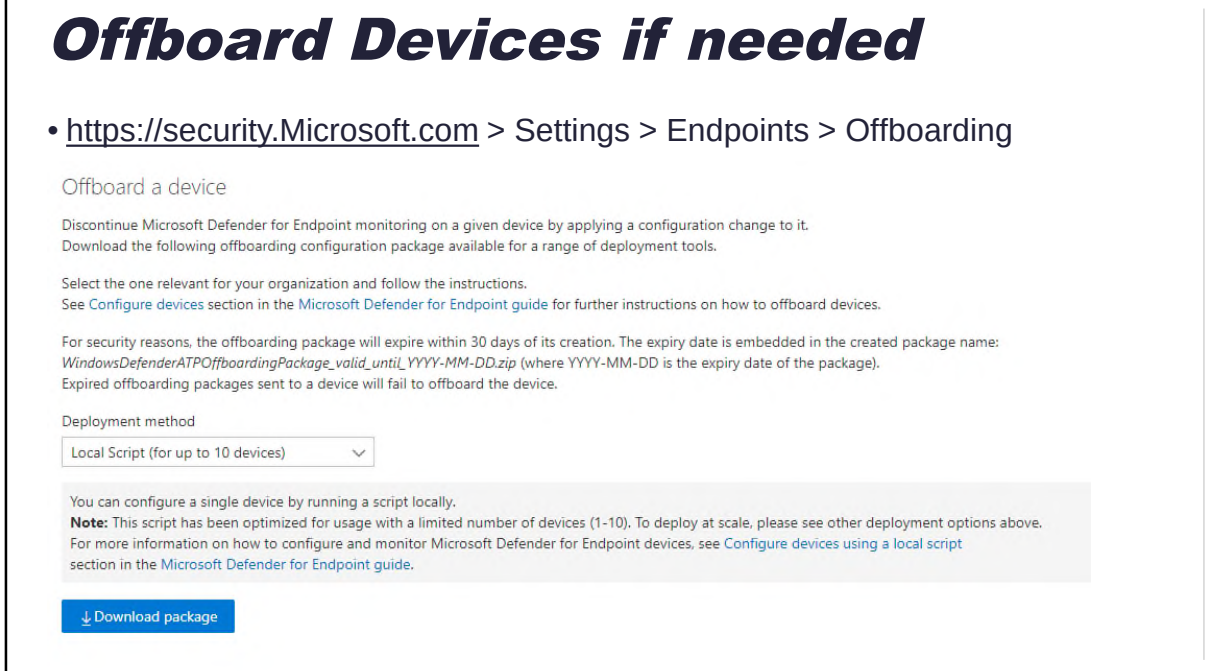


64

64

Offboard Devices if needed

- https://security.Microsoft.com > Settings > Endpoints > Offboarding



65

65

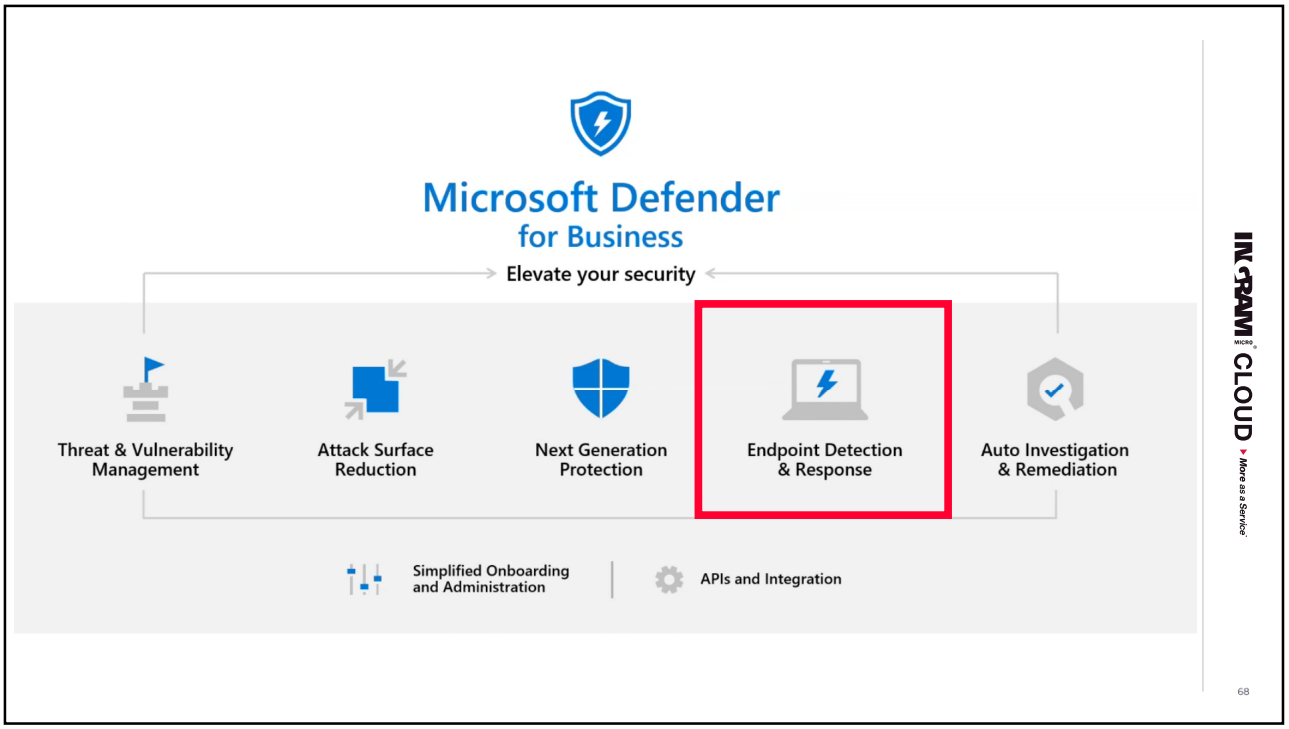
LAB 2:
Getting started with Microsoft Defender for Business

66

66


INGRAM MICRO CLOUD
More as a Service
Endpoint Detection & Response (EDR)
More as a Service™

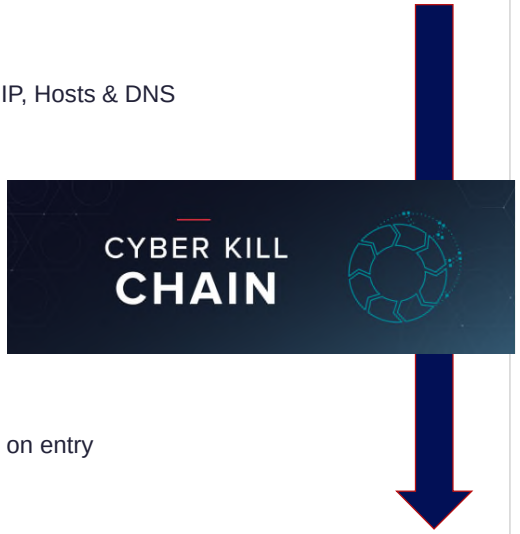
67


Microsoft Defender
for Business
Elevate your security
Threat & Vulnerability Management
Attack Surface Reduction
Next Generation Protection
Endpoint Detection & Response
Auto Investigation & Remediation
Simplified Onboarding and Administration
APIs and Integration
INGRAM MICRO CLOUD
More as a Service
68

68

Cyber Kill Chain

- Reconnaissance
  - Gather information about the environment, Users & IP, Hosts & DNS
- Compromised Credential
  - Brute force attempts, Suspicious VPN Connections
- Lateral Movement
  - Spread the attack and gain elevation
- Domain Dominance
  - Gain control over your environment / multiple points on entry

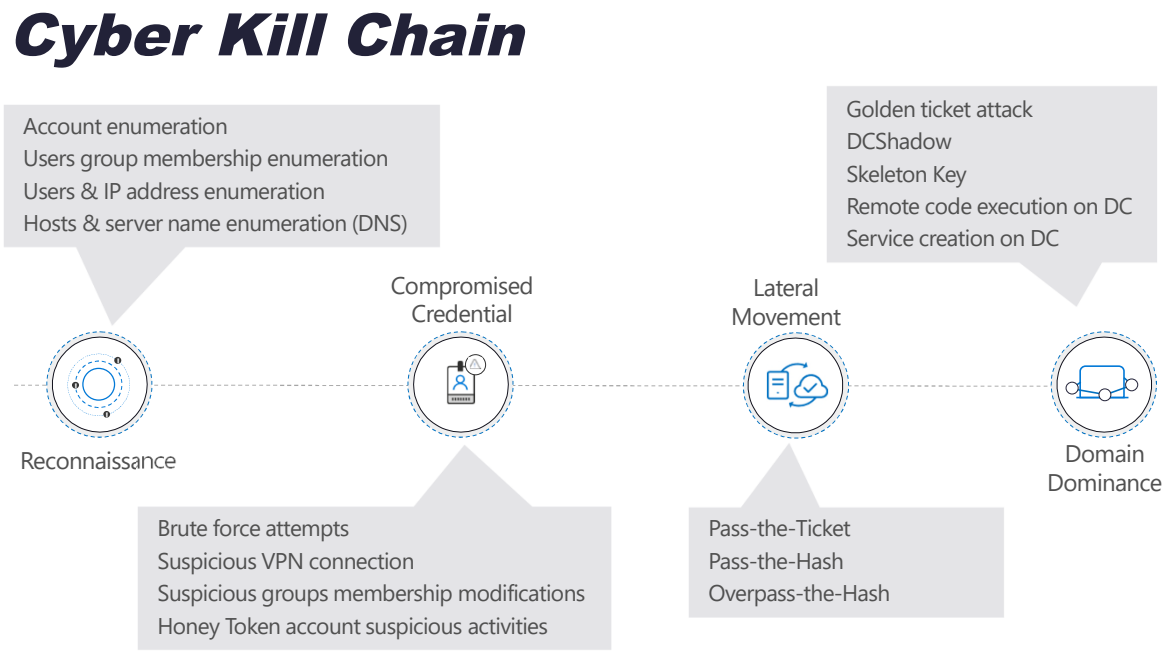


INGRAM MICRO CLOUD More as a Service

69

69

Cyber Kill Chain

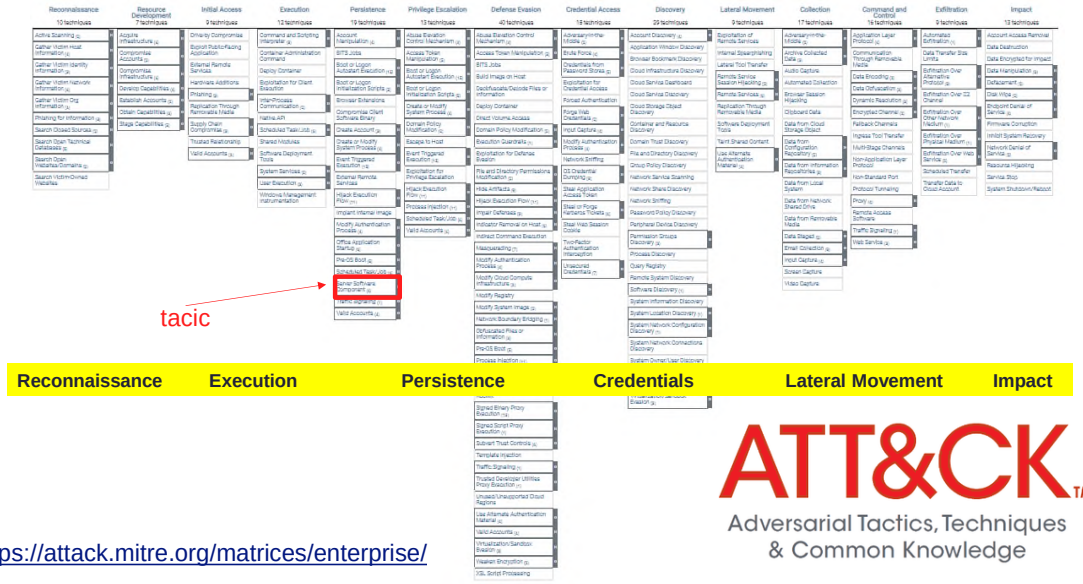


INGRAM MICRO CLOUD

70

70

MITRE ATT&CK tactics



ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

https://attack.mitre.org/matrices/enterprise/

71

71

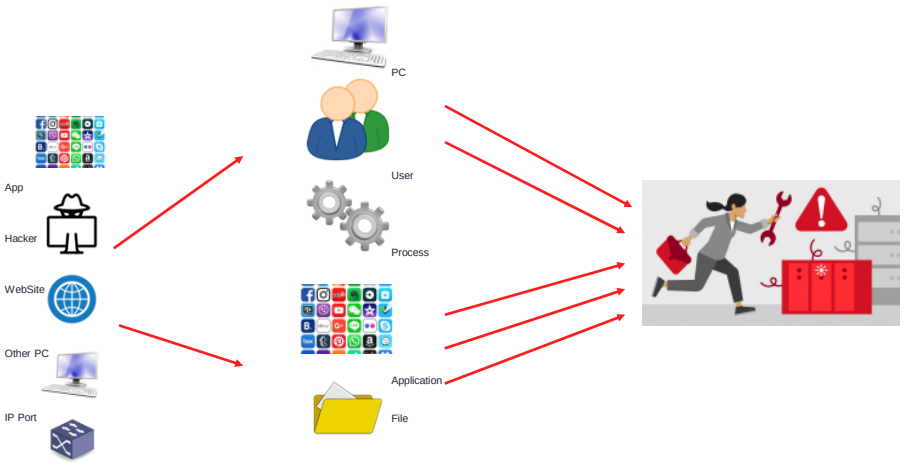
Endpoint Detection and Response

- Behavior-based detection and response
- Identify and remove Persistent threats
- Manual and Live response
  - Run antivirus scan
  - Isolate device
  - Stop and quarantine a file
  - Add an indicator to block or allow a file

72

72

Threats – Alerts - Incidents



Source Threat Node Alert Incident

INGRAM MICRO CLOUD More as a Service

73

73

Incident Summary

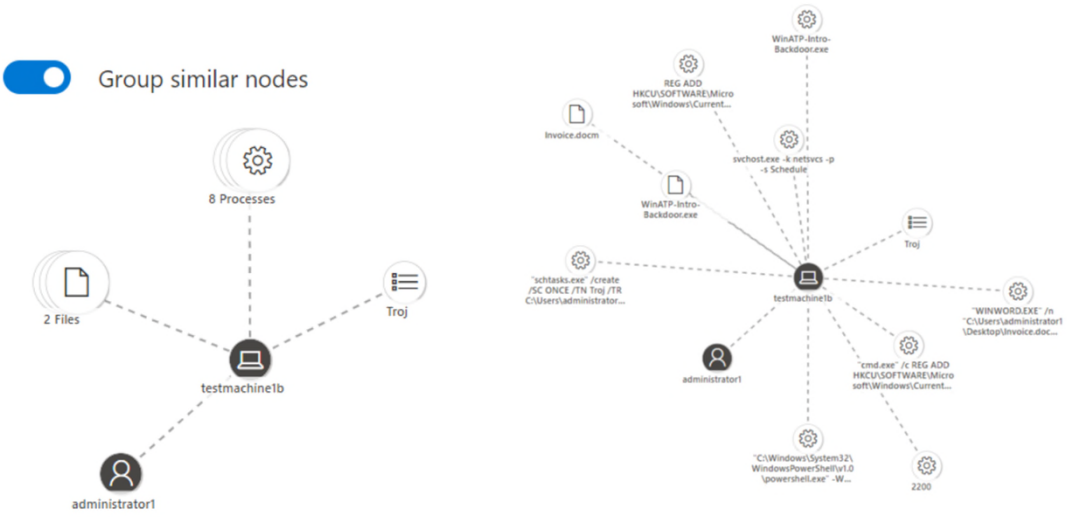
- Incident Analysis based on MITRE ATT&CK tactics

INGRAM MICRO CLOUD More as a Service

74

74

Incident Analysis & Graph

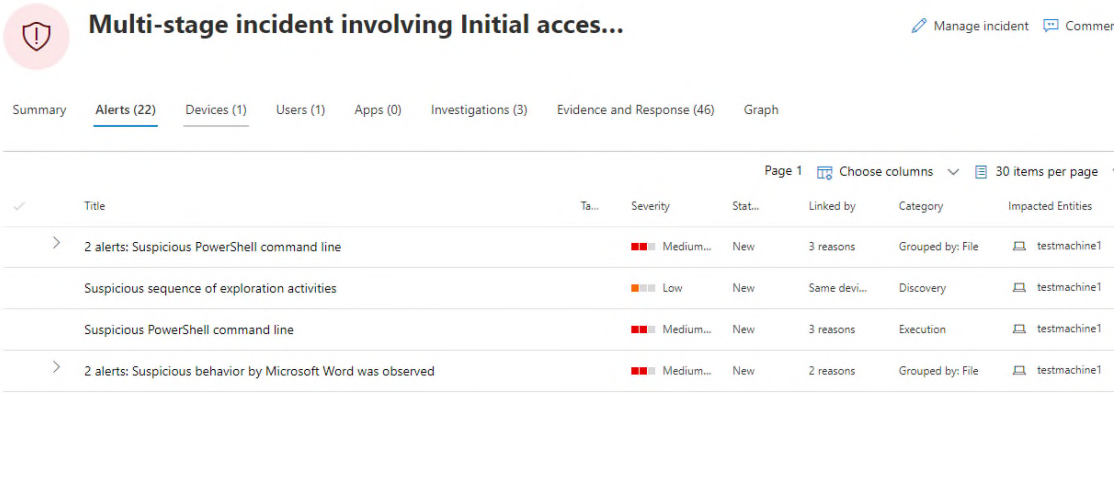


INGRAM MICRO CLOUD More as a Service

75

75

Incident Overview

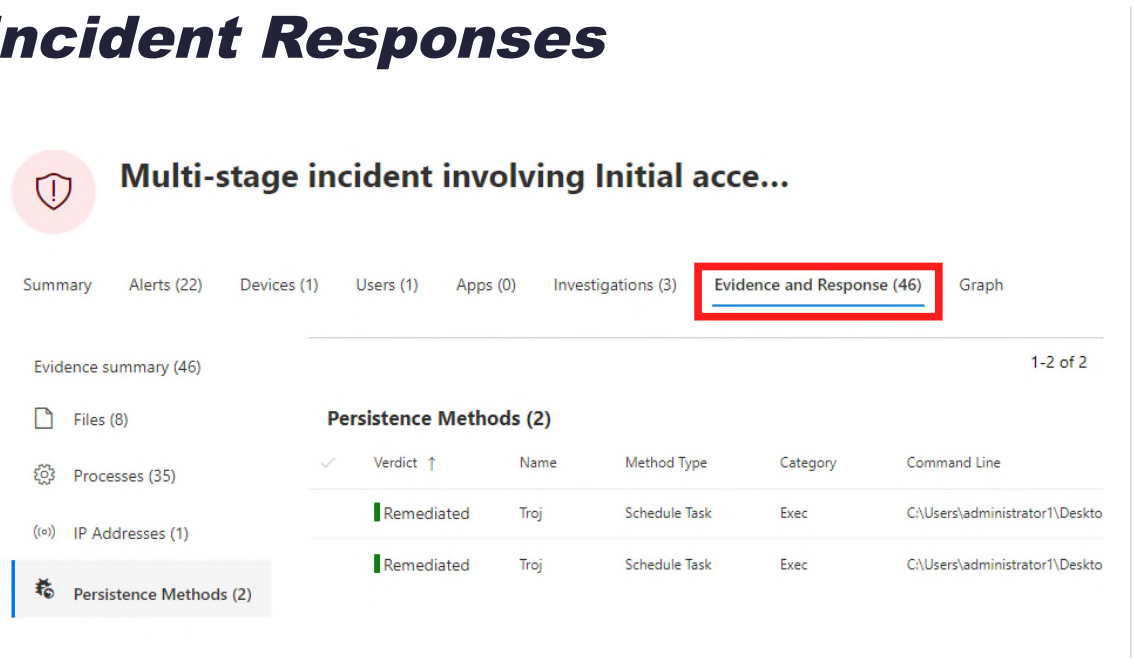


INGRAM MICRO CLOUD More as a Service

76

76

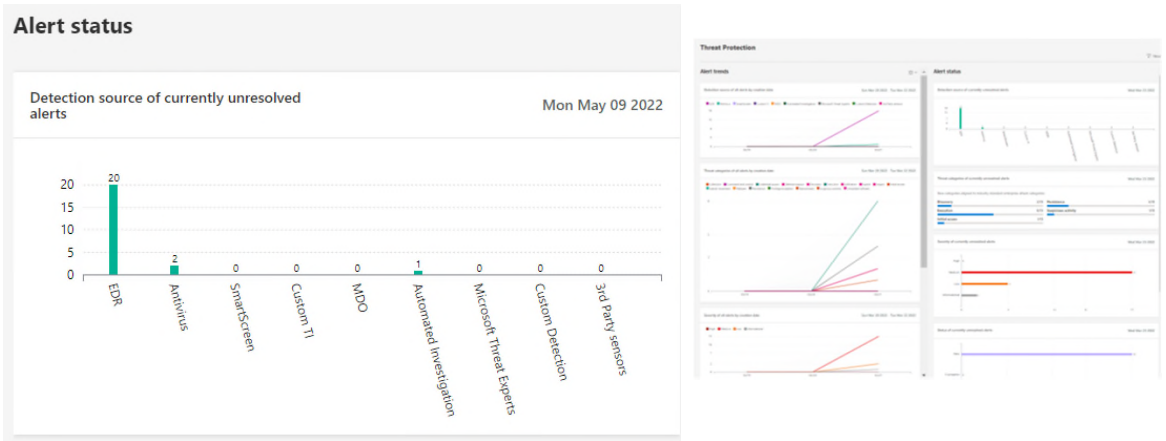
Incident Responses



77

77

Threat Protection Reports

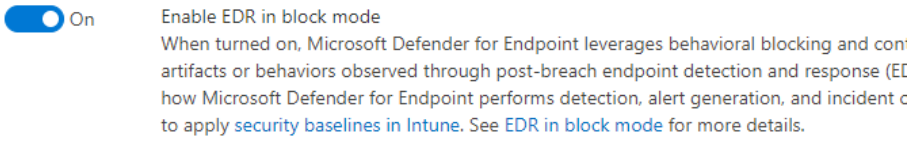


78

78

Enabling EDR Block Mode

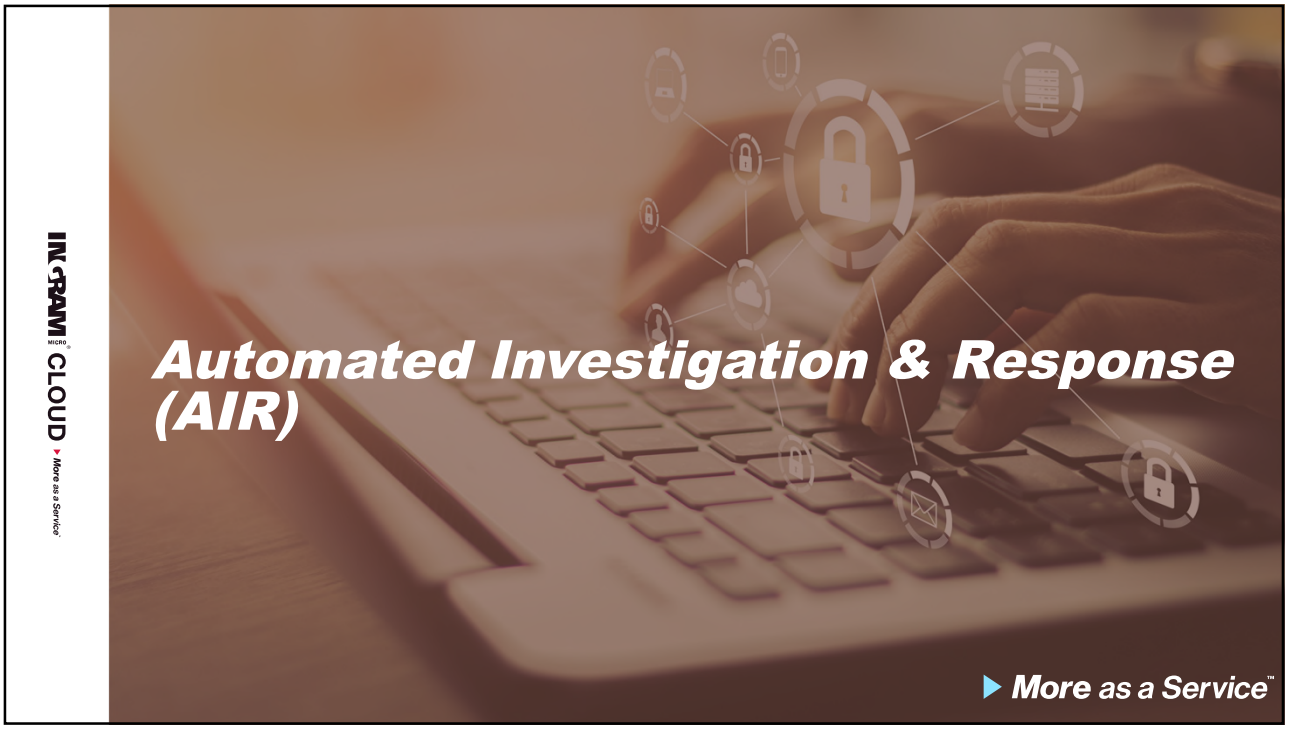
- When malicious artifact is detected
  - MDB blocks and remediates the artifact
- You can enable this mode for Groups of Devices in Intune
- https://security.microsoft.com > Settings > Endpoints > Advanced Features



INGRAM MICRO CLOUD More as a Service

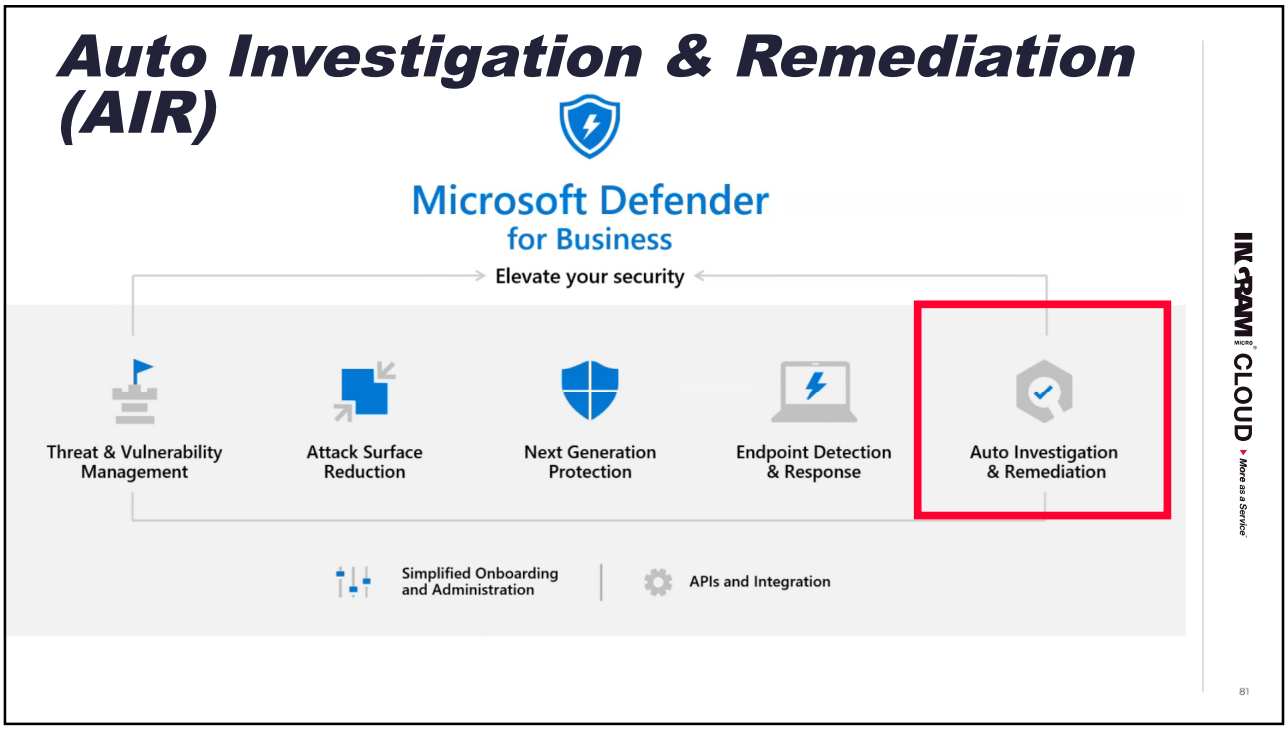
79

79



80

Auto Investigation & Remediation (AIR)

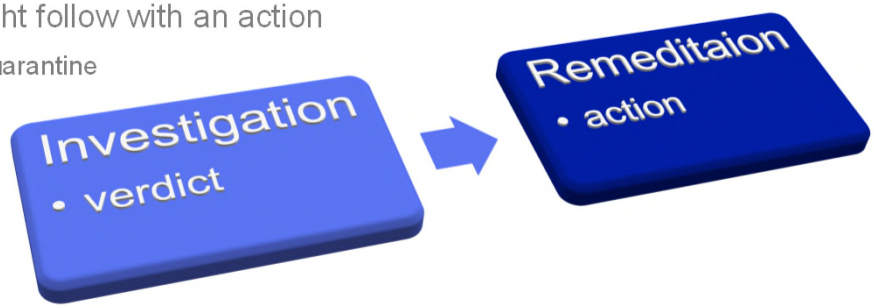


81

81

Investigation & Remediation

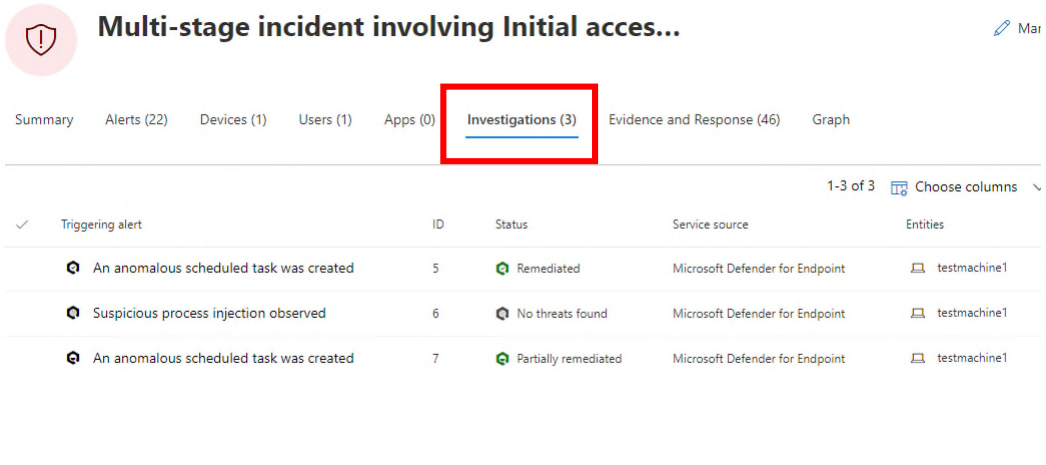
- Some incidents can start an Automated Investigation
  - A verdict will follow after the investigation
  - Malicious
  - Suspicious
  - No threats found
- Remediation might follow with an action
  - Sending file in quarantine
  - Stop Process
  - Isolate Device
  - Blocking URL
  - Other Action



82

82

Investigations & Remediations

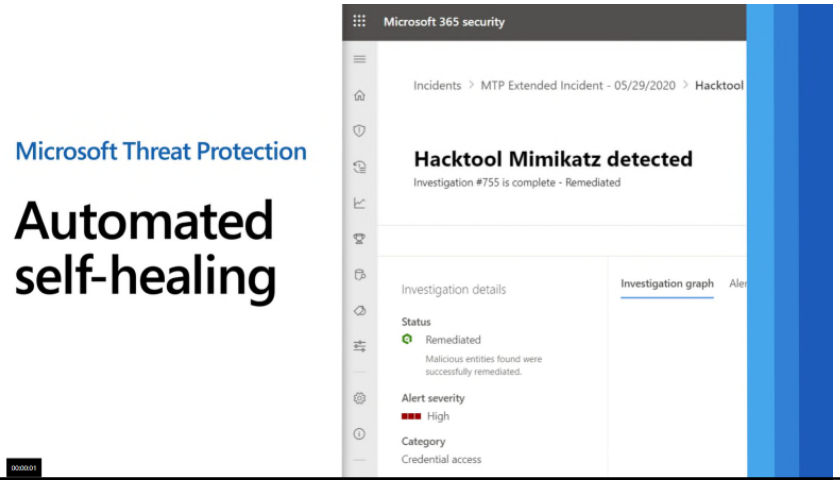


83

83

Why Auto Investigation & Remediation ?

- https://www.microsoft.com/en-us/videoplayer/embed/RE4BzwB

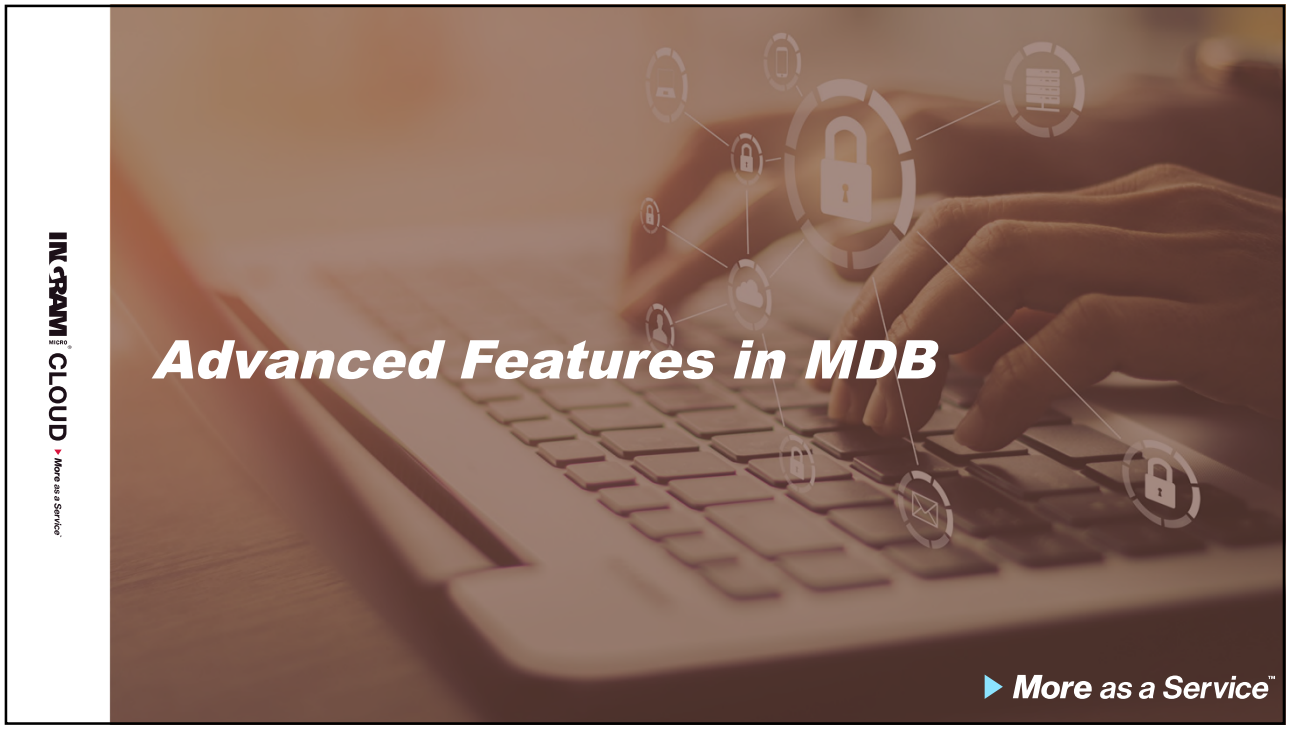


84

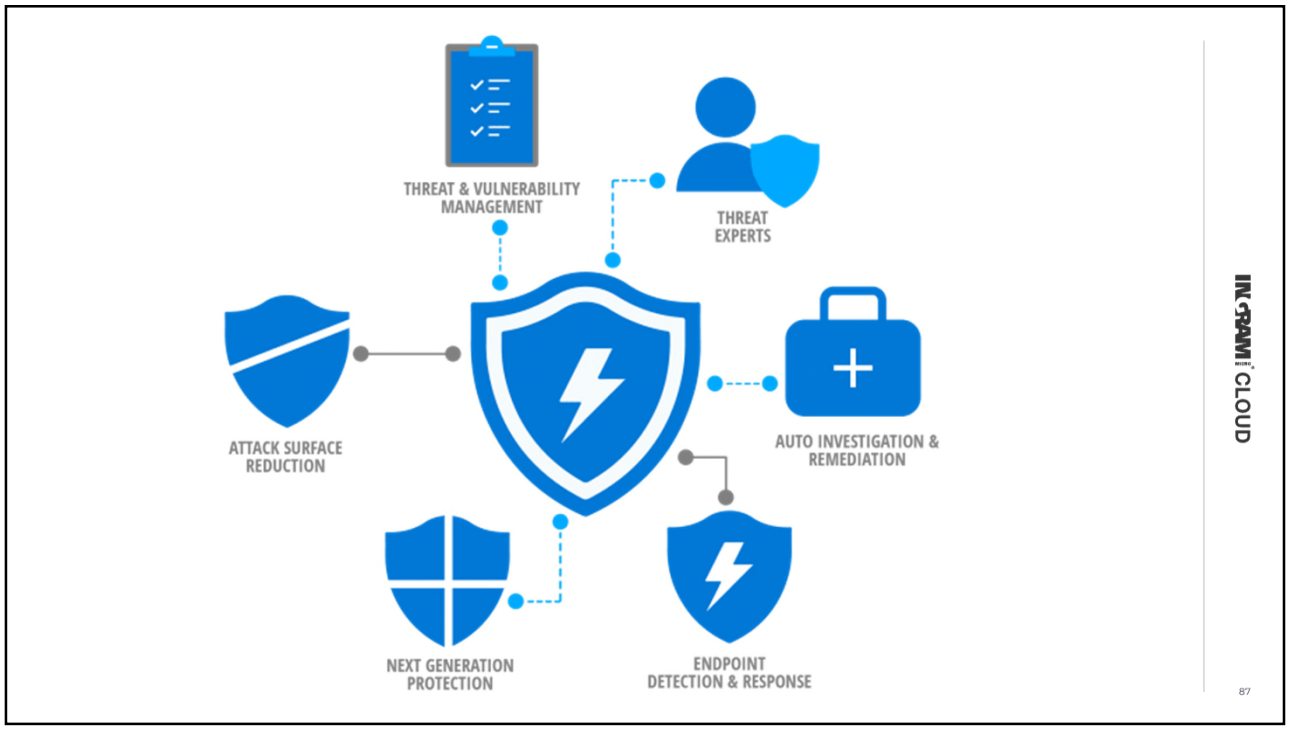
84


Microsoft
Defender for
Business
LAB 3:
Endpoint Detection & Response
INGRAM MICRO CLOUD
85

85


INGRAM MICRO CLOUD
More as a Service
Advanced Features in MDB
More as a Service™

86


THREAT & VULNERABILITY MANAGEMENT
THREAT EXPERTS
ATTACK SURFACE REDUCTION
AUTO INVESTIGATION & REMEDIATION
NEXT GENERATION PROTECTION
ENDPOINT DETECTION & RESPONSE
INGRAM CLOUD
87

87


Attack Surface Reduction (ASR)
INGRAM CLOUD
88

88

Attack Surface Reduction (ASR)

Hardware-based isolation

Network protection

Application control

Web protection

Ransomware protection

Exploit protection

Controlled folder access

Device control

Attack Surface Reduction Rules

INGRAM MICRO CLOUD More as a Service

89

89

Attack Surface Reduction Tools

- Hardware based isolation
  - Isolates untrusted websites in a separate container (sandbox)
  - Microsoft Defender Application Guard
- Application control
  - Prevent applications from running by allowing only Trusted Applications
  - Microsoft Defender Application Control
- Controlled folder access
  - Specified folders where only trusted applications can write files
- Network protection
  - Similar protection as Controlled folder access for network connections
- Exploit protection
  - Windows Defender Exploit Guard

ATTACK SURFACE REDUCTION

INGRAM MICRO CLOUD More as a Service

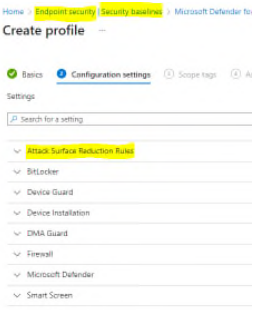
90

90

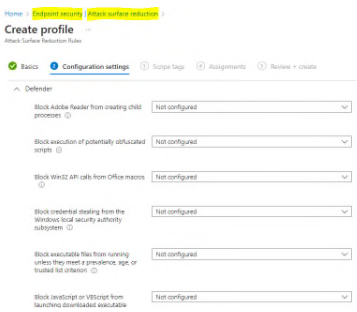
Attack Surface Reduction Rules

- Use Microsoft Intune or Group Policies to enable ASR Rules

Endpoint Security Baselines



Attack Surface Reduction Profile



https://learn.microsoft.com/nl-nl/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-deployment

91

91

Tamper Protection

92

92

Tamper Protection

- During cyber attacks, bad actors try to disable security features, such as intivirus protection
- Tamper protection prevents malicious applications for
  - Disabling virus or threat protection
  - Disabling real-time protection
  - Removing security updates
  - Disabling automatic actions
  - Disabling scanning files & folders

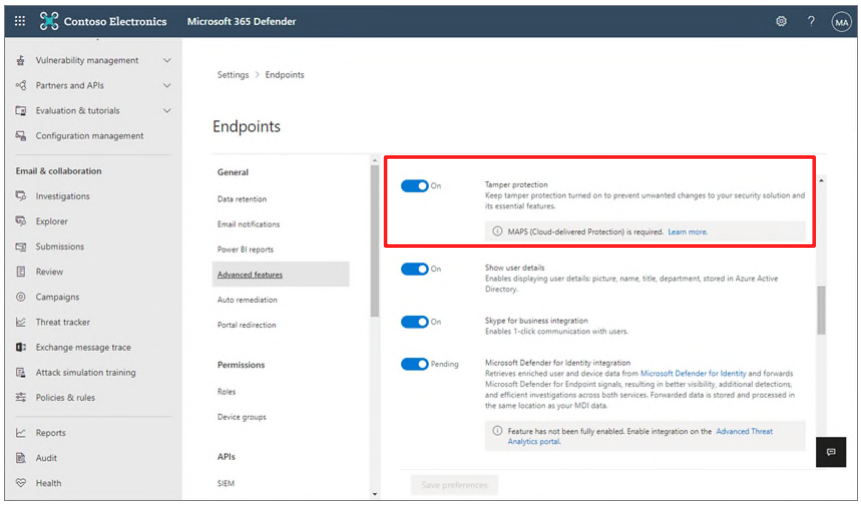
INGRAM MICRO CLOUD More as a Service

93

93

Enable Tamper Protection

- Microsoft 365 Defender portal



INGRAM MICRO CLOUD More as a Service

94

94

Manual Response

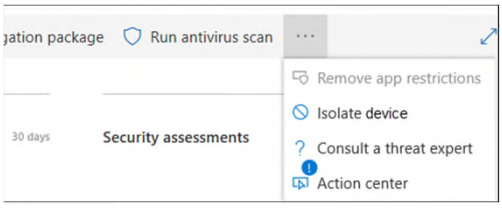
INGRAM MICRO CLOUD

95

95

Manual Response Actions

- Microsoft Defender for Business includes response actions :
  - Run antivirus scan
  - Isolate device
  - Stop and quarantine a file
  - Add an indicator to block or allow a file
- Only available for Windows 10/ Windows 11



INGRAM MICRO CLOUD More as a Service

96

96

Live Response

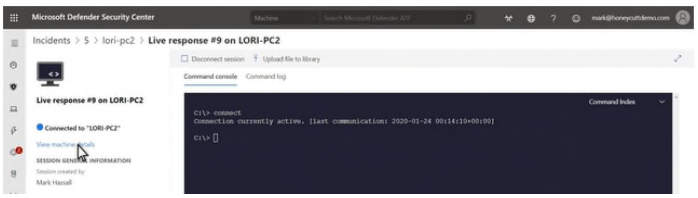
INGRAM MICRO CLOUD

97

97

Live Response Session

- Instantaneous access to a device using remote shall
- Do in-depth investigative work
- Take immediate response
  - Basic and Advanced commands
  - Download Files
  - Upload PowerShell script
  - Run the script
  - Take/Undo remediations



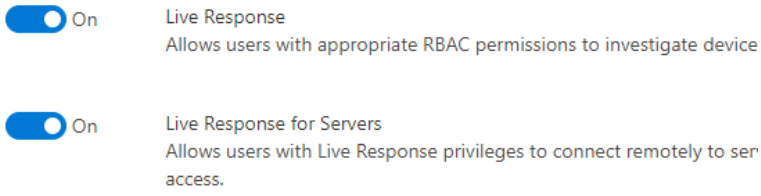
INGRAM MICRO CLOUD More as a Service

98

98

Enable Live Response

- https://security.Microsoft.com > settings > Advanced Features



INGRAM MICRO CLOUD More as a Service

99

99

Live Response Commands

- Windows
- macOS
- Linux

Command	Description	Windows and Windows Server	macOS	Linux
cd	Changes the current directory.	Y	Y	Y
cls	Clears the console screen.	Y	Y	Y
connect	Initiates a live response session to the device.	Y	Y	Y
connections	Shows all the active connections.	Y	N	N
dir	Shows a list of files and subdirectories in a directory.	Y	Y	Y
drivers	Shows all drivers installed on the device.	Y	N	N
fg `<command ID>`	Place the specified job in the foreground, making it the current job. NOTE: fg takes a 'command ID' available from jobs, not a PID	Y	Y	Y
fileinfo	Get information about a file.	Y	Y	Y
findfile	Locates files by a given name on the device.	Y	Y	Y
getfile <file_path>	Downloads a file.	Y	Y	Y
help	Provides help information for live response commands.	Y	Y	Y
jobs	Shows currently running jobs, their ID and status.	Y	Y	Y
persistence	Shows all known persistence methods on the device.	Y	N	N
processes	Shows all processes running on the device.	Y	Y	Y
registry	Shows registry values.	Y	N	N
scheduledtasks	Shows all scheduled tasks on the device.	Y	N	N
services	Shows all services on the device.	Y	N	N
startupfolders	Shows all known files in startup folders on the device.	Y	N	N
status	Shows the status and output of specific command.	Y	N	N
trace	Sets the terminal's logging mode to debug.	Y	Y	Y

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide

INGRAM MICRO CLOUD More as a Service

100

100

Incidents Queue

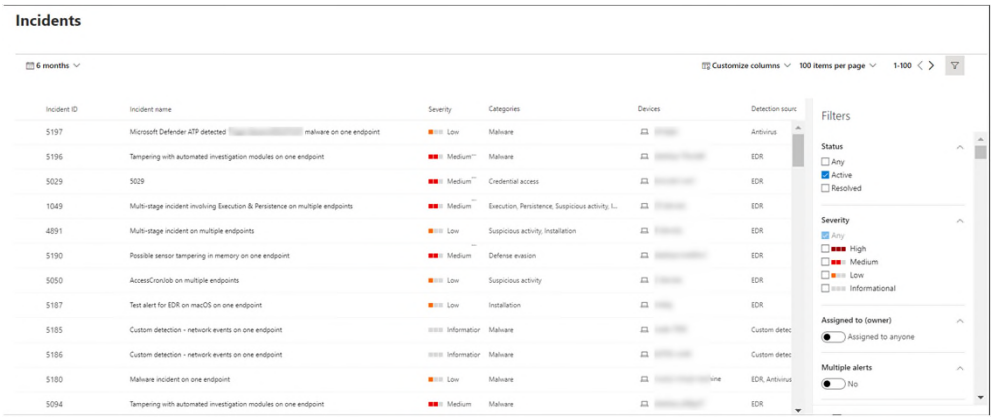
INGRAM MICRO CLOUD

101

101

Incidents Queue

- Shows a collection of incidents



INGRAM MICRO CLOUD More as a Service

102

102

Incident Severity Level

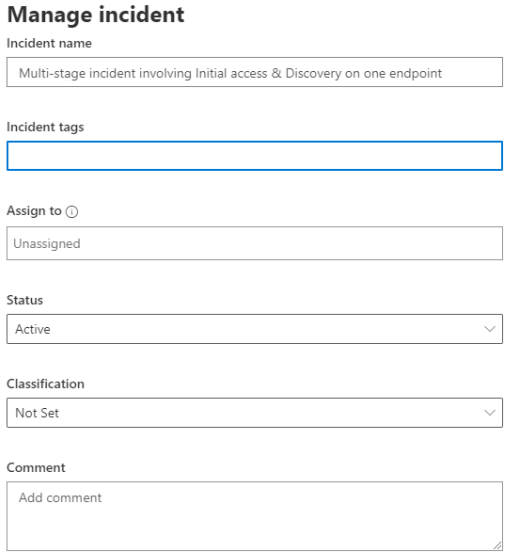
Severity

Incident severity	Description
High (Red)	Threats often associated with advanced persistent threats (APT). These incidents indicate a high risk due to the severity of damage they can inflict on devices.
Medium (Orange)	Threats rarely observed in the organization, such as anomalous registry change, execution of suspicious files, and observed behaviors typical of attack stages.
Low (Yellow)	Threats associated with prevalent malware and hack-tools that do not necessarily indicate an advanced threat targeting the organization.
Informational (Grey)	Informational incidents might not be considered harmful to the network but might be good to keep track of.

103

Manage Incident

- Assign to a SecAdmin
- Status
  - Active
  - In Progress
  - Resolved
- Manual Classification
  - For Logging



104

Threat Analytics

INGRAM MICRO CLOUD

105

105

What is Threat Analytics ?

- In-Product threat intelligence solution
- Intelligence solution **from Microsoft security researchers**
- Designed to assist the security Team
  - Latest threats
  - High-impact threats
  - Highest exposure threats
- You can create **email notification Rule** on Threat Analytics
  - Ransomware
  - Phising
  - Vulnerability
  - Activity Group

INGRAM MICRO CLOUD More as a Service

106

106


Microsoft
Defender for
Business
LAB 4:
Advanced Features
INGRAM MICRO CLOUD
107

107


INGRAM MICRO CLOUD
More as a Service
Threat & Vulnerability Management
(TVM)
More as a Service™

108

Threat & Vulnerability Management

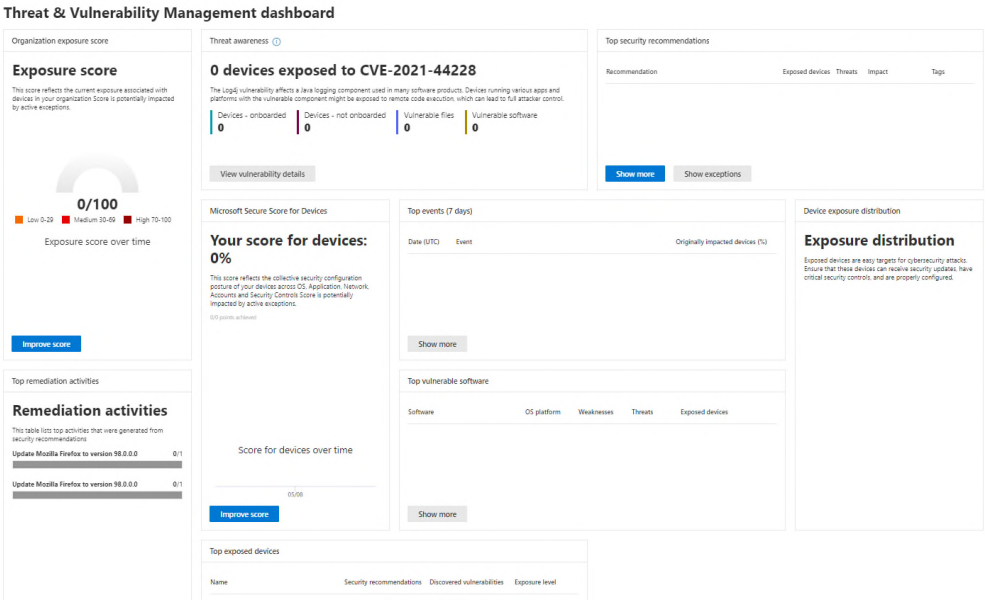
- **Discover** vulnerabilities & misconfigurations
  - Real time / without agent or periodic scans
- **Prioritize** vulnerabilities based on threat landscape
- Built-in **Remediation** process

INGRAM MICRO CLOUD More as a Service

109

109

Threat & Vulnerability Mgmt Dashboard

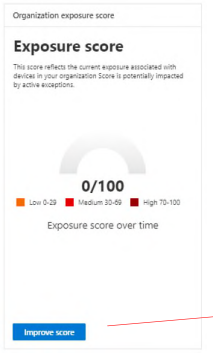


INGRAM MICRO CLOUD More as a Service

110

110

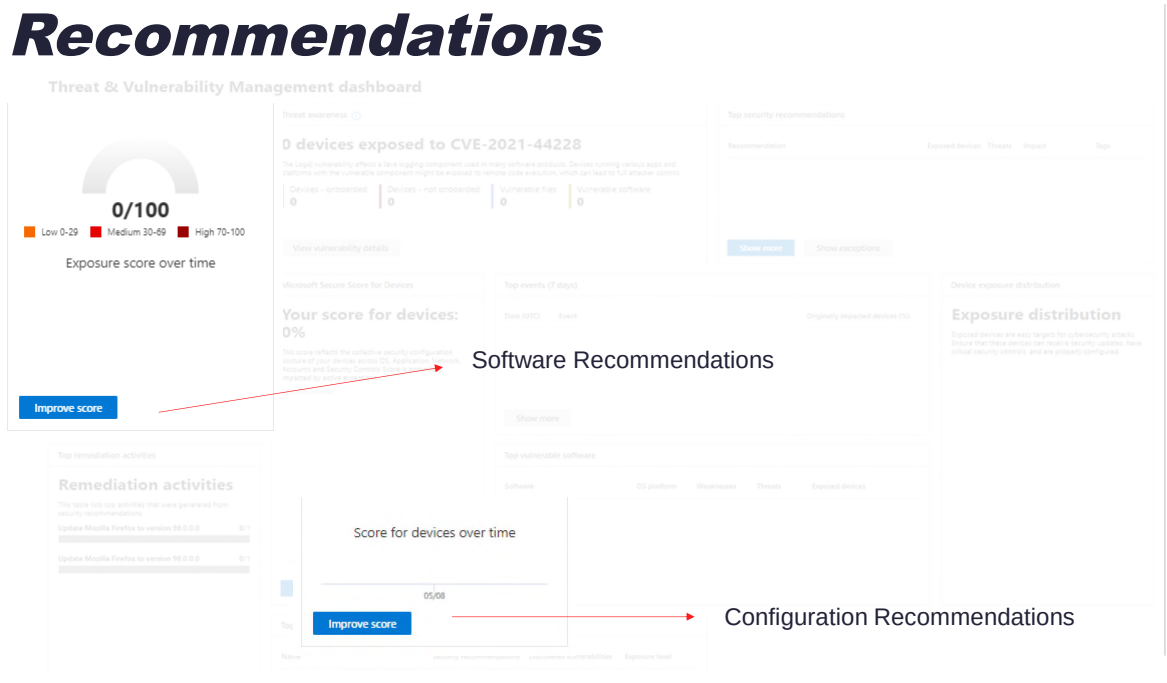
Exposure Score



- Current state of your organizations device exposure to threats and vulnerabilities
- Weaknesses discovered in your devices
- Goal is to LOWER the exposure score
- Improve Score shows software recommendations

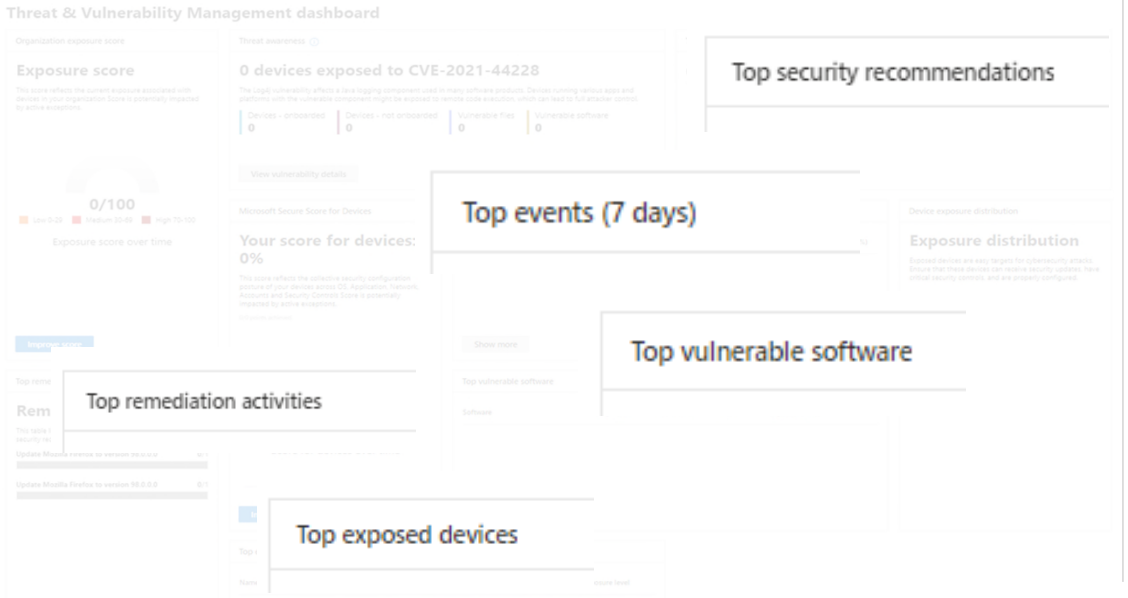
111

Recommendations



112

Top Required Actions & Remediations

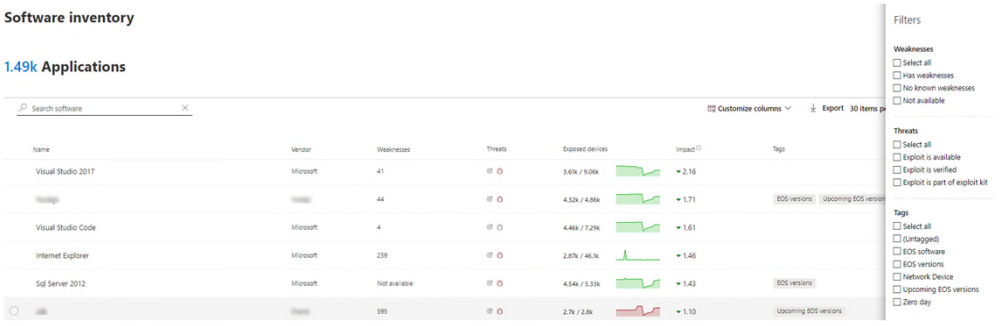


113

113

Sofware Inventories

- Associated threats with know Software versions

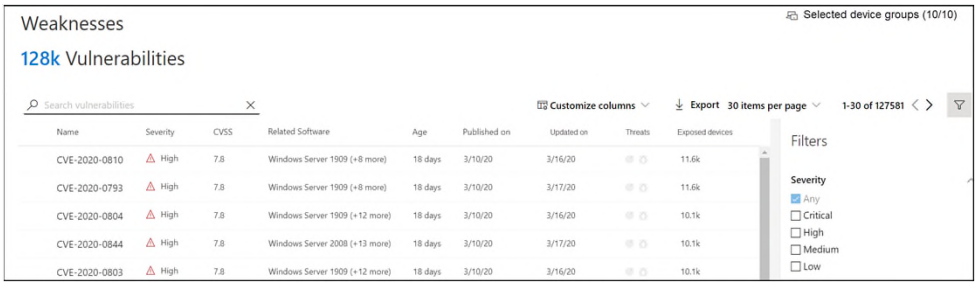


114

114

Common Vulnerabilities and Exposures (CVE)

- Known Weaknesses detected on devices
- Full database of CVE's :
  - https://cve.org



INGRAM MICRO CLOUD More as a Service

115

115

LAB 5: Threat & Vulnerability Management

INGRAM MICRO CLOUD

116

116

Wrap-Up

- Introduction MDB
- Cyber Security Frameworks
- Microsoft Defender for Business : Setup
- Endpoint Detection & Response (EDR)
- Automated Investigation (AIR)
- Advanced Features (ASR + …)
- Threat Vulnerability Management (TVM)

INGRAM MICRO CLOUD

117

117