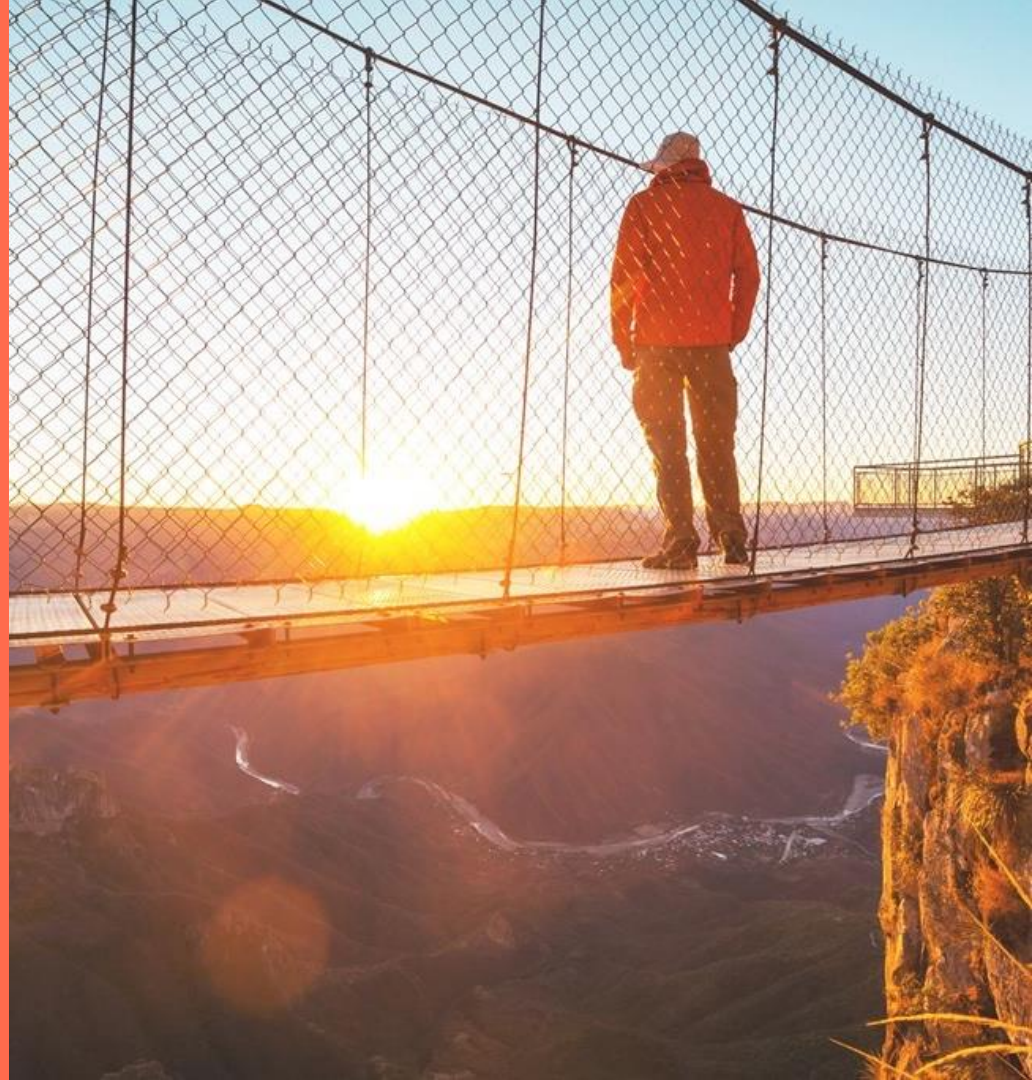
rhipe

A Crayon company

Securing Australian Businesses

Why is cybersecurity increasingly crucial in 2023 and the future?



Bad Security Posture Leads to Incidents

Safe digitalisation requires scalable ways to implement and maintain good security posture

60%

Of data breaches involve **unpatched vulnerabilities**

80%

Of incidents could be addressed through modern approaches

Source:
IDC
Microsoft Digital Defense Report 2022

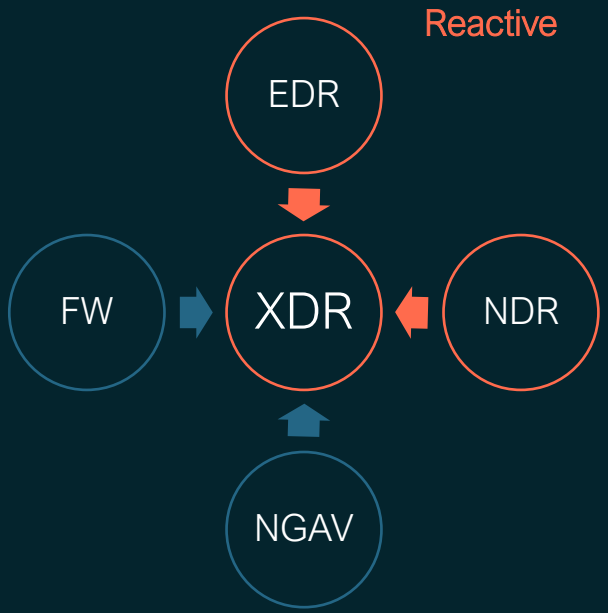
Crayon

Technology Requirements for a Modern Security Posture

- Capability to **Prevent**, Detect, React by **cross-leveraging** security tools and
  - Systems
  - Endpoints
  - Processes
- Policy-driven technical security architecture
- Single pane of glass for operations
- Quality
- Development pace

Crayon

Security Operations in 2020-2023



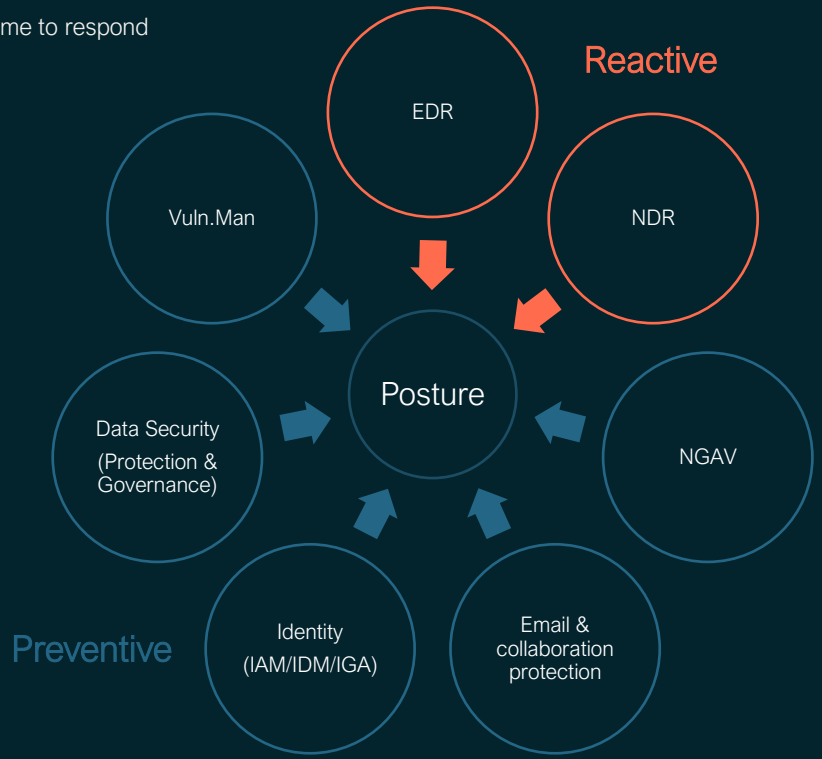
Minimized time to detect a breach

Fastest time to respond

Scalable security architecture: Controls, hardening, policies, guardrails across domains

Minimized time to detect a breach

Fastest time to respond



Crayon

NAVIGATING IN THE NEW SECURITY LANDSCAPE

Defense Priorities

Baseline: Security controls, policies and configurations for (mostly) all users, devices and other end-user services.

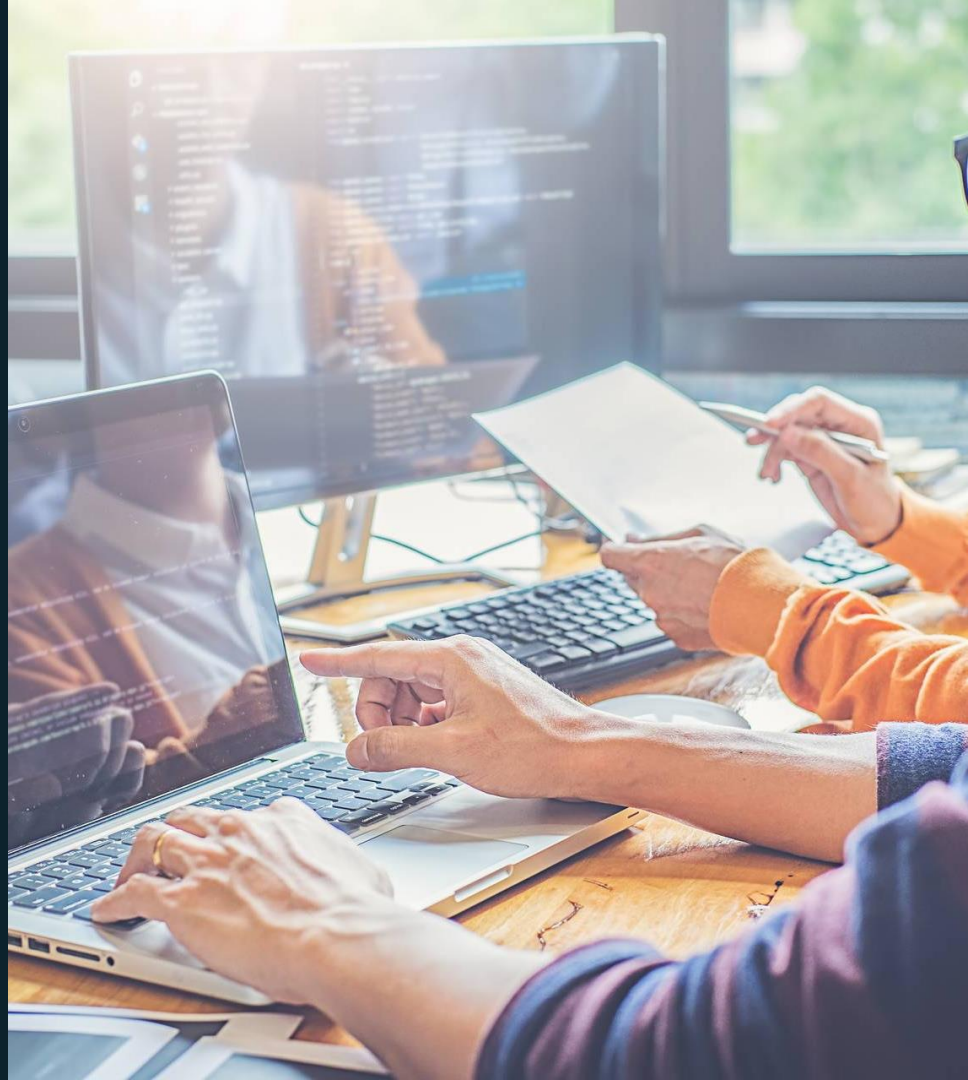
Guardrails: Identification, alerting and addressing deviations from the intended baseline/state that may cause weaknesses.

Cloud Security Posture Management: Automated identification & remediation of security risks across cloud environments

*Source: Microsoft Digital Defense Report 2022

rhipe
A Crayon company

ASD 8 / Cyber attack chain



CYBERSECURITY FRAMEWORKS

Australia Cyber Security Centre - Essential 8

Application Control

Patch Applications

Configure MS Office Macro Settings

User Application Hardening

Restrict Administrative Privileges

Patch Operating Systems

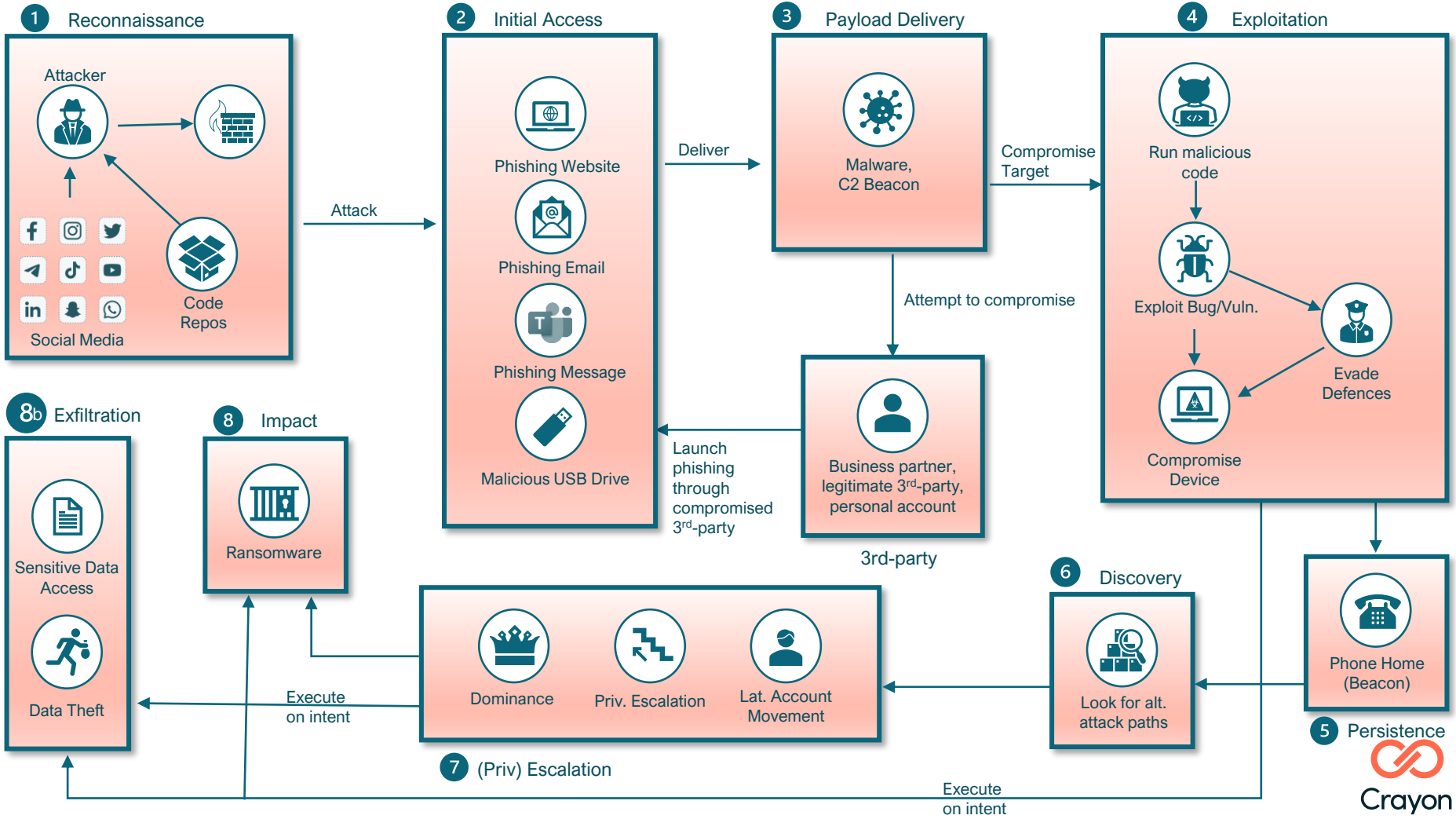
Multi-Factor Authentication

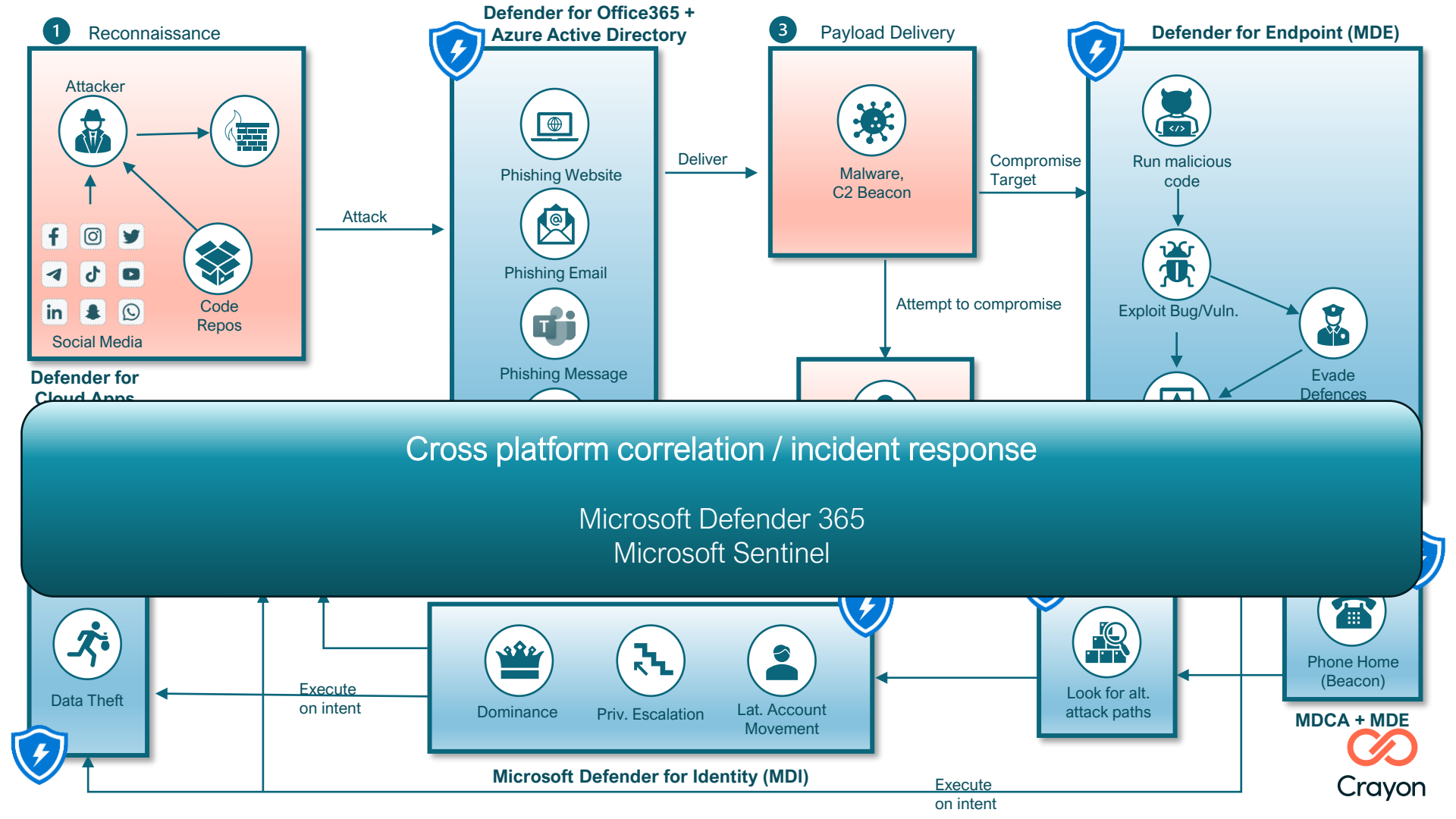
Regular Backups

Crayon

A typical attack chain for perspective….

Crayon


1 Reconnaissance
Attacker
Social Media
Code Repos
Attack
2 Initial Access
Phishing Website
Phishing Email
Phishing Message
Malicious USB Drive
Deliver
3 Payload Delivery
Malware, C2 Beacon
Compromise Target
4 Exploitation
Run malicious code
Exploit Bug/Vuln.
Evade Defences
Compromise Device
Attempt to compromise
Business partner, legitimate 3rd-party, personal account
3rd-party
Launch phishing through compromised 3rd-party
8b Exfiltration
Sensitive Data Access
Data Theft
8 Impact
Ransomware
Execute on intent
Dominance
Priv. Escalation
Lat. Account Movement
7 (Priv) Escalation
6 Discovery
Look for alt. attack paths
Phone Home (Beacon)
5 Persistence
Execute on intent
Crayon

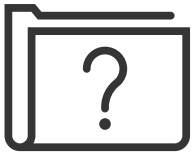

1 Reconnaissance
Attacker
Social Media
Code Repos
Defender for Cloud Apps
Attack
Defender for Office365 + Azure Active Directory
Phishing Website
Phishing Email
Phishing Message
Deliver
3 Payload Delivery
Malware, C2 Beacon
Compromise Target
Attempt to compromise
Defender for Endpoint (MDE)
Run malicious code
Exploit Bug/Vuln.
Evade Defences
Cross platform correlation / incident response
Microsoft Defender 365
Microsoft Sentinel
Data Theft
Execute on intent
Dominance
Priv. Escalation
Lat. Account Movement
Microsoft Defender for Identity (MDI)
Look for alt. attack paths
Phone Home (Beacon)
MDCA + MDE
Execute on intent
Crayon

Cyber kill chain Microsoft M365 BP or E5(Security)

- Single vendor across attack chain
- Telemetry from many sources is automatically correlated
- Incident Response is automated across email, device, identity, web security

Identity Security

Device security



Data Security

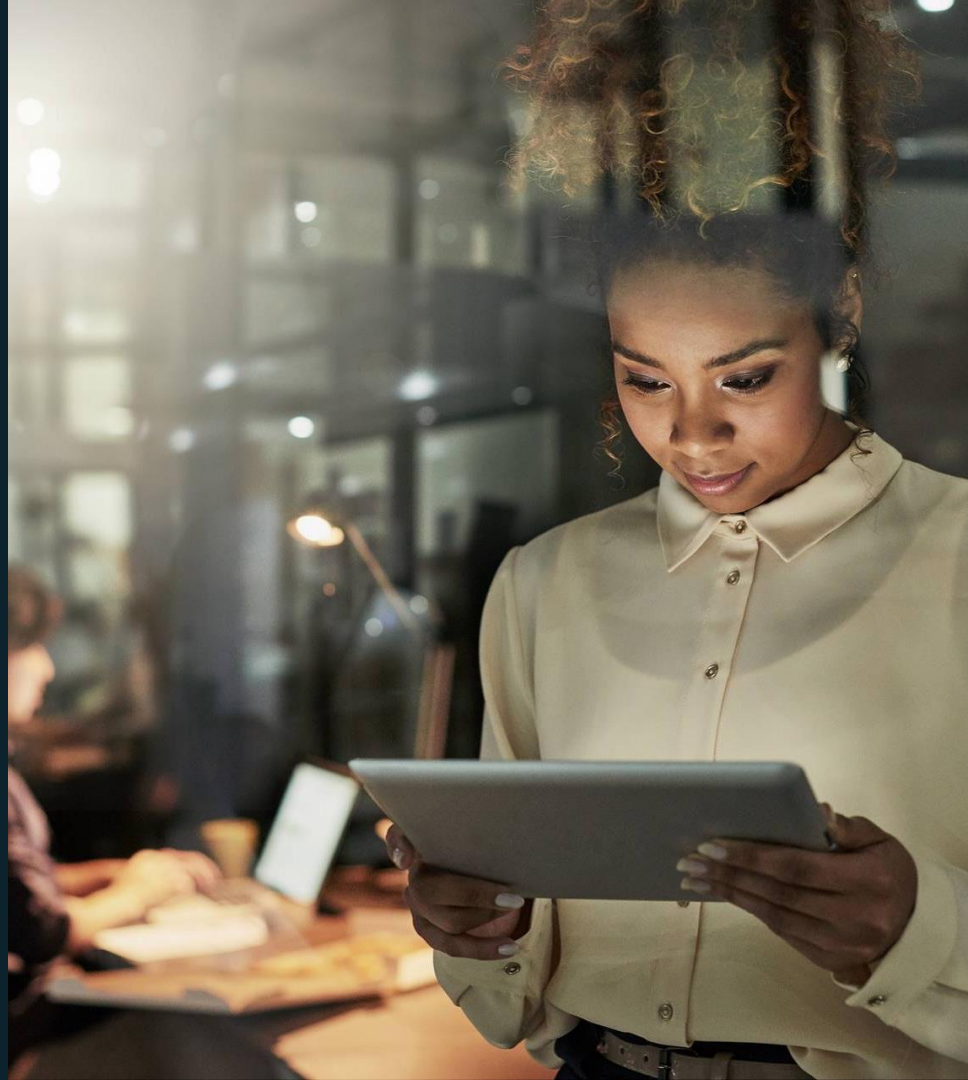
Cloud security

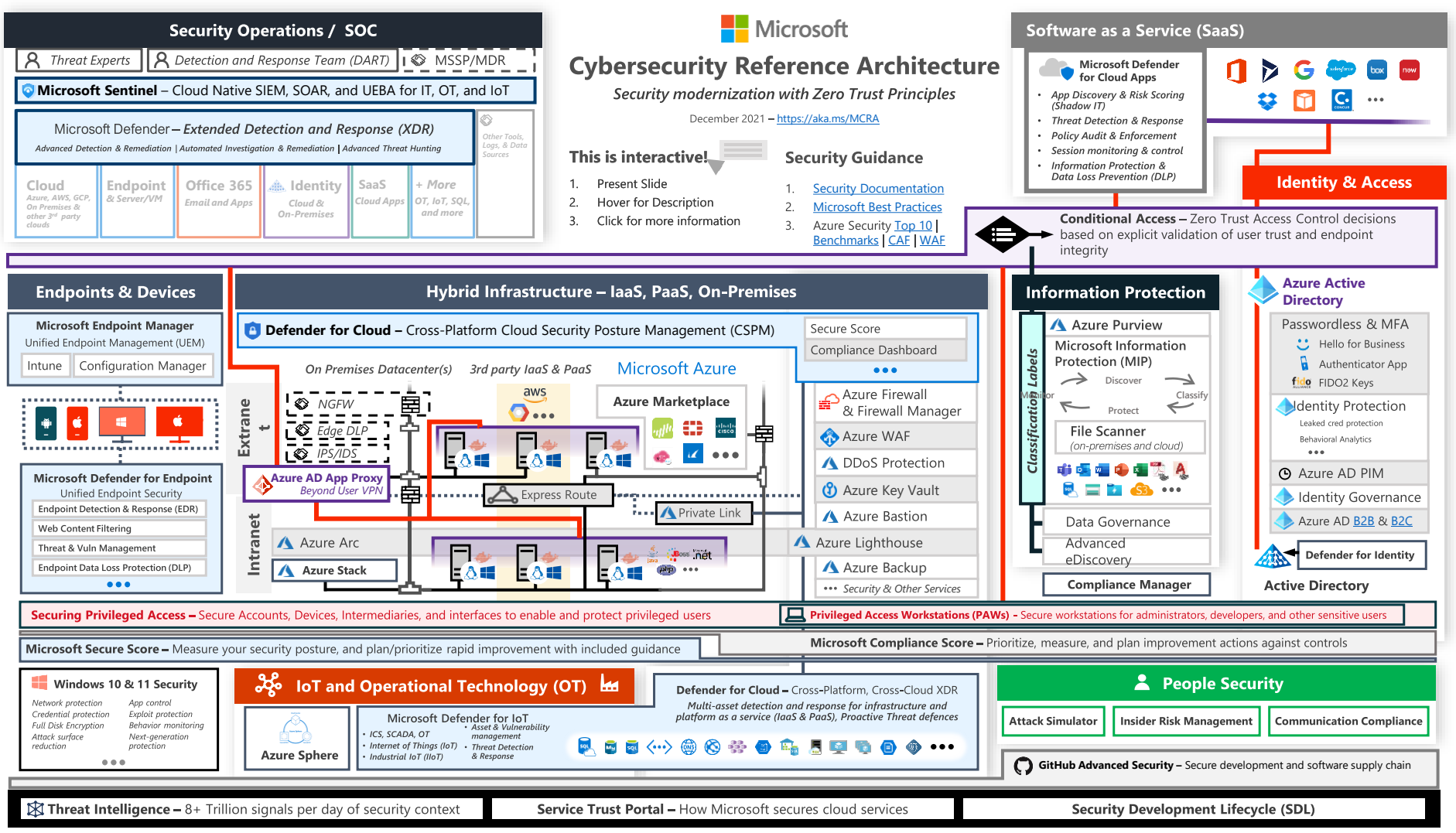
Collaboration (email, SharePoint, Teams

Crayon

rhipe
A Crayon company

What is the Microsoft Security Platform?




Security Operations / SOC
Threat Experts
Detection and Response Team (DART)
MSSP/MDR
Microsoft Sentinel – Cloud Native SIEM, SOAR, and UEBA for IT, OT, and IoT
Microsoft Defender – Extended Detection and Response (XDR)
Advanced Detection & Remediation | Automated Investigation & Remediation | Advanced Threat Hunting
Other Tools, Logs, & Data Sources
Cloud
Azure, AWS, GCP, On Premises & other 3rd party clouds
Endpoint
& Server/VM
Office 365
Email and Apps
Identity
Cloud & On-Premises
SaaS
Cloud Apps
+ More
OT, IoT, SQL, and more
Microsoft
Cybersecurity Reference Architecture
Security modernization with Zero Trust Principles
December 2021 – https://aka.ms/MCRA
This is interactive!
1. Present Slide
2. Hover for Description
3. Click for more information
Security Guidance
1. Security Documentation
2. Microsoft Best Practices
3. Azure Security Top 10 | Benchmarks | CAF | WAF
Software as a Service (SaaS)
Microsoft Defender for Cloud Apps
App Discovery & Risk Scoring (Shadow IT)
Threat Detection & Response
Policy Audit & Enforcement
Session monitoring & control
Information Protection & Data Loss Prevention (DLP)
Identity & Access
Conditional Access – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity
Endpoints & Devices
Microsoft Endpoint Manager
Unified Endpoint Management (UEM)
Intune
Configuration Manager
Microsoft Defender for Endpoint
Unified Endpoint Security
Endpoint Detection & Response (EDR)
Web Content Filtering
Threat & Vuln Management
Endpoint Data Loss Protection (DLP)
Hybrid Infrastructure – IaaS, PaaS, On-Premises
Defender for Cloud – Cross-Platform Cloud Security Posture Management (CSPM)
Secure Score
Compliance Dashboard
On Premises Datacenter(s)
3rd party IaaS & PaaS
Microsoft Azure
Extranet
NGFW
Edge DLP
IPS/IDS
Azure AD App Proxy
Beyond User VPN
Express Route
Private Link
Intranet
Azure Arc
Azure Stack
aws
Azure Marketplace
Azure Firewall & Firewall Manager
Azure WAF
DDoS Protection
Azure Key Vault
Azure Bastion
Azure Lighthouse
Azure Backup
Security & Other Services
Information Protection
Classification Labels
Azure Purview
Microsoft Information Protection (MIP)
Discover
Classify
Protect
Monitor
File Scanner
(on-premises and cloud)
Data Governance
Advanced eDiscovery
Compliance Manager
Azure Active Directory
Passwordless & MFA
Hello for Business
Authenticator App
FIDO2 Keys
Identity Protection
Leaked cred protection
Behavioral Analytics
Azure AD PIM
Identity Governance
Azure AD B2B & B2C
Defender for Identity
Active Directory
Securing Privileged Access – Secure Accounts, Devices, Intermediaries, and interfaces to enable and protect privileged users
Privileged Access Workstations (PAWs) - Secure workstations for administrators, developers, and other sensitive users
Microsoft Secure Score – Measure your security posture, and plan/prioritize rapid improvement with included guidance
Microsoft Compliance Score – Prioritize, measure, and plan improvement actions against controls
Windows 10 & 11 Security
Network protection
Credential protection
Full Disk Encryption
Attack surface reduction
App control
Exploit protection
Behavior monitoring
Next-generation protection
IoT and Operational Technology (OT)
Azure Sphere
Microsoft Defender for IoT
ICS, SCADA, OT
Internet of Things (IoT)
Industrial IoT (IIoT)
Asset & Vulnerability management
Threat Detection & Response
Defender for Cloud – Cross-Platform, Cross-Cloud XDR
Multi-asset detection and response for infrastructure and platform as a service (IaaS & PaaS), Proactive Threat defences
People Security
Attack Simulator
Insider Risk Management
Communication Compliance
GitHub Advanced Security – Secure development and software supply chain
Threat Intelligence – 8+ Trillion signals per day of security context
Service Trust Portal – How Microsoft secures cloud services
Security Development Lifecycle (SDL)

MICROSOFT SECURITY PLATFORM

Achieve your Security Posture with Microsoft

There are lots of ways to achieve a security posture that will protect your clients systems and data

Microsoft 365 Defender Services

Adopt a Cybersecurity Framework Model in conjunction with Microsoft Security Suite

Take advantage of Azure AD P1 – Multi-Factor Authentication Features

Preventative before reactive security posture

Crayon

FEATURE COMPARISON BASED ON LICENSES

Azure AD Multi-Factor Authentication (MFA)

Feature	Azure AD Free*	Azure AD Free Global Admins only	Office 365	Azure AD P1	Azure AD P2
Protect Azure AD tenant admin accounts with MFA	●	● (Global Admins only)	●	●	●
Mobile app as a second factor	●	●	●	●	●
Phone call as a second factor		●	●	●	●
SMS as a second factor		●	●	●	●
Admin control over verification methods		●	●	●	●
Fraud alert				●	●
MFA Reports				●	●
Custom greetings for phone calls				●	●
Custom caller ID for phone calls				●	●
Trusted IPs				●	●
Remember MFA for trusted devices		●	●	●	●
MFA for on-premises applications				●	●
Conditional access				●	●
Risk-based conditional access					●
Identity Protection (Risky sign-ins, risky users)					●
Access Reviews					●
Entitlements Management					●
Privileged Identity Management (PIM), just-in-time access					●
Lifecycle Workflows (preview)					●

*Free - Security defaults (enabled for all users)

Crayon

Microsoft Defender for Cloud Apps

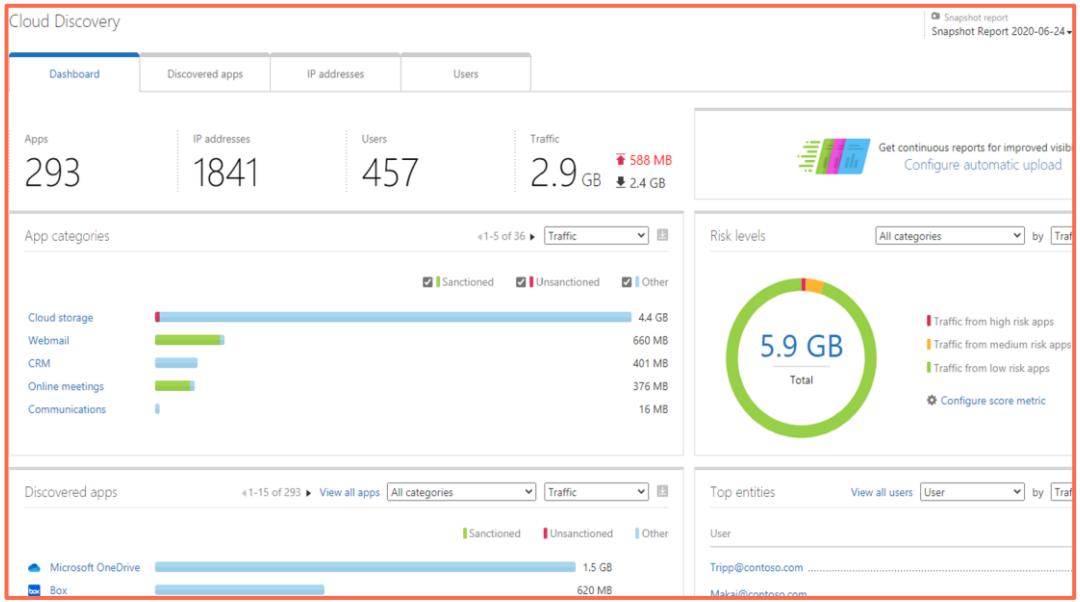
Microsoft Defender for Cloud Apps provides rich visibility to your cloud services, control over data travel, and sophisticated analytics to identify and combat cyber threats across all your Microsoft and third-party cloud services.

The Defender for Cloud Apps Framework

- Discover and control the use of Shadow IT.
- Protect your sensitive information anywhere in the cloud.
- Protect against cyber threats and anomalies.
- Assess your cloud apps' compliance.

Office 365 Cloud App Security

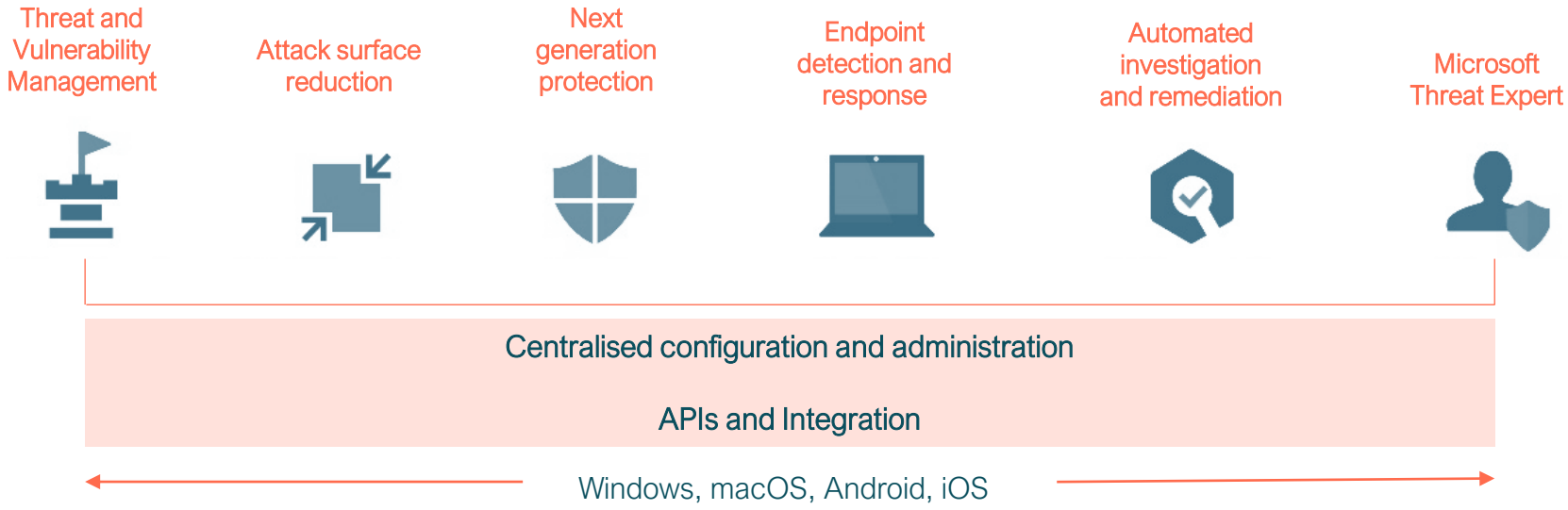
Enhance Cloud App Discovery in Azure Active Directory



Crayon

MICROSOFT DEFENDER SERVICES

Microsoft Defender for Endpoint



Crayon

Microsoft Defender for Office 365

Microsoft Defender for Office 365 covers:

1. Threat protection policies
2. Reports
3. Threat investigation and response capabilities
4. Automated investigation and response capabilities

M365 BUSINESS PREMIUM

Microsoft Defender for **Office 365 Plan 1**

- Safe Attachments
- Safe Links
- Safe Attachments for SharePoint, OneDrive, & Microsoft Teams
- Anti-phishing protection
- Real-time detections

Microsoft Defender for **Office 365 Plan 2**

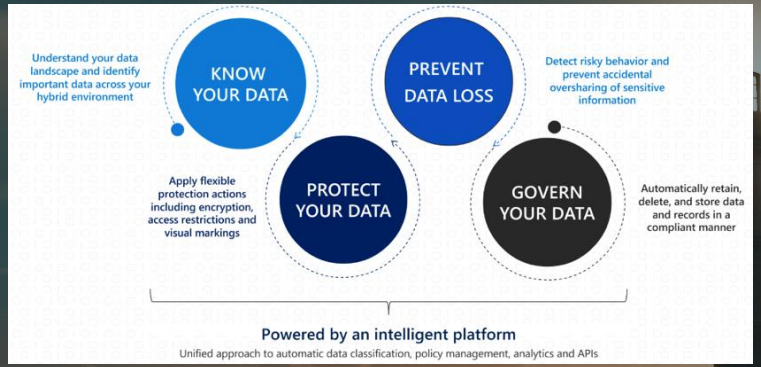
- Threat Trackers & Threat Explorer
- Automated investigation & response (AIR)
- Attack Simulator
- Proactively hunt for threats
- Investigate incidents and alerts

Crayon

DATA LOSS PREVENTION

Purview Information Protection

- Data security across On-premise, endpoints, 3rd party cloud services, SharePoint, Teams, OneDrive
- Automatic Document protection through encryption
- Secure business from Insider risk or malicious employees
- Automatic data classification of data

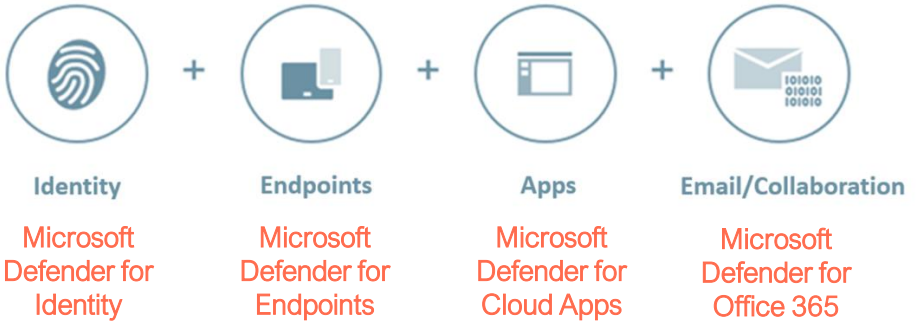


MICROSOFT 365 DEFENDER SERVICES

Microsoft 365 Defender

- Coordinates the detection, prevention, investigation, and response to threats.
- Protects identities, endpoints, apps, and email/collaboration.
- Integrated protection against sophisticated attacks

Integrated Microsoft 365 Defender Experience



Crayon

Defence in Depth

Identity

Device

Application

Data

Network

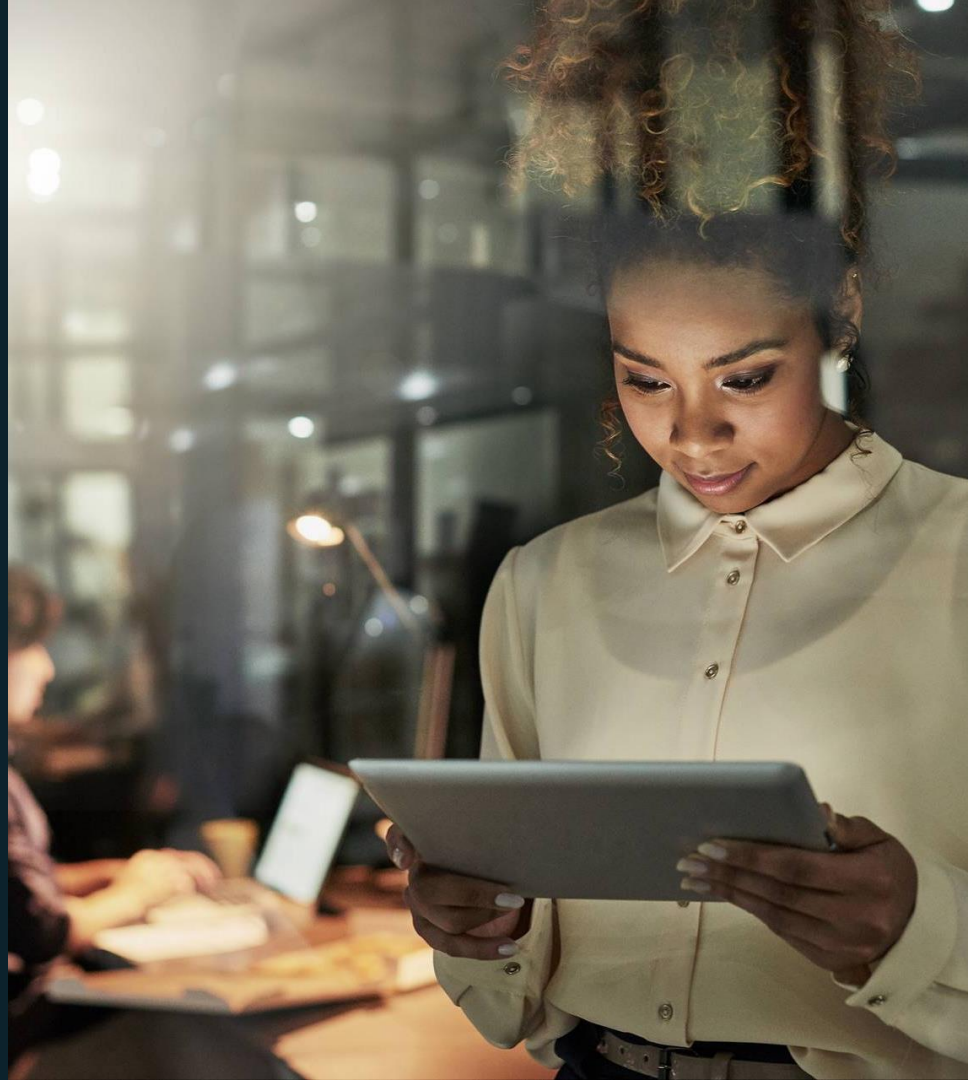
Infrastructure

Cloud Native

Azure Active Directory, Intune, Defender for Business, Defender for Office 365, Defender for Cloud Apps, Purview Information Protection

rhipe
A Crayon company

Mapping Microsoft to ASD 8



ACSC – Essential 8

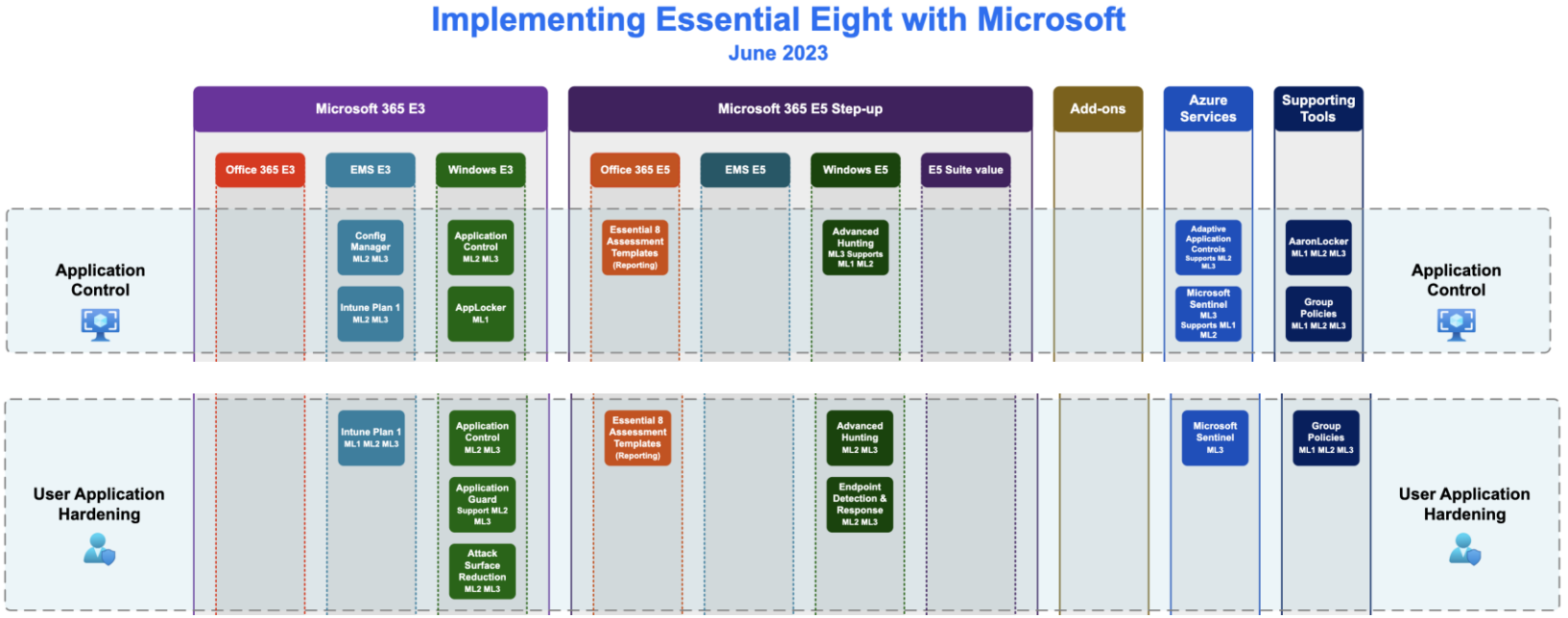
- The Australian Cyber Security Centre (ACSC) leads the Australian Government's efforts to improve cybersecurity
- The ACSC recommends that all Australian organisations implement the Essential Eight mitigation strategies

ACSC Essential 8 – Mitigation Strategy	Microsoft Solution
1) Application Control	Microsoft Defender for Endpoint & Applocker
2) Patch Applications	Microsoft Intune & Microsoft Defender for Endpoint
3) Configure Microsoft Office Macro Settings	Microsoft Intune & Microsoft Defender for Endpoint
4) User Application Hardening	Microsoft Intune & Microsoft Defender for Endpoint
5) Restrict Administrative Privileges	Microsoft Intune & Azure Active Directory Premium P1/P2
6) Patching Operating Systems	Microsoft Intune & Microsoft Defender for Endpoint
7) Multi-factor Authentication	Azure Active Directory – Premium P1/P2
8) Regular Backups	Azure Backup & Crayon Cloud Backup (M365 Data)

Service Trust Portal
Resources for Australia

Crayon

ASD 8 Journey



- Https://m365.com/files/Essential-8.htm

Crayon

Resources

- https://www.agilient.com.au/resources/ - Great framework excel
- https://servicetrust.microsoft.com/ViewPage/RegionalAustralia– ASD 8 detail + other service detail
- Check out Github for Automation (open source, proceed with caution)
- ASD 8: Https://m365.com/files/Essential-8.htm
- Https://learn.microsoft.com/en-us/compliance/essential-eight/e8-overview
- Https://m365.com/files/Essential-8.htm

Crayon

rhipe

A Crayon company

Thank you