IBM Security

Reducing Risk and Enhancing Security

with MaaS360 Threat Management

Clint Adams
IBM Security – MaaS360 Product Management

September 2022

IBM

Agenda

MaaS360 Point of View and Strategy

MaaS360 Mobile Threat Management

- History
- What's New?
  - Detections and Responses
  - Security Dashboard and User Risk Management
  - Threat Telemetry Enrichment (Zscaler example)

Mobile Threat and Risk Management Setup and Demo

Enabling the Features

Questions

MaaS360 Strategy Overview

The case for the convergence of Endpoint Management and Security Platforms

In our “work-from-anywhere” world, organizations need to centrally manage endpoints and security, while keeping their IT experts efficient, create frictionless experiences for their end users, reduce the cyberthreats and keep a low TCO.

- Companies are challenged with multiple endpoint security tools or dashboards that limits the ability of SOC analysts and IT Admins to effectively mitigate and deal with threats.
- UEM based Threat Management offers an opportunity to ”de-silo” management and security functions, reducing complexity in the number of endpoint solutions while enhancing integration and aligning risk mitigation approaches.
- MaaS360 Threat Management provides a unified view of device, users, threats and vulnerabilities in one Admin experience that can easily be used by the IT Admin and SOC functions.
- MaaS360 Threat Management provides a frictionless end user experience. Simply configure the Security Policy, publish and deploy. No additional agents to deploy or separate systems to manage.
- With IBM MaaS360 with Watson you will merge efficiency and effectiveness by managing endpoints including mobile devices, laptops, desktops, wearables, ruggedized **and** protect them with **augmented** threat management capabilities that include a new centralized policy, plus new detections and responses such as phishing and insider threats.

Analysts Concur

“While endpoint management and security programs have long operated in silos, complexity and risk are driving new requirements for integration and risk mitigation alignment…”

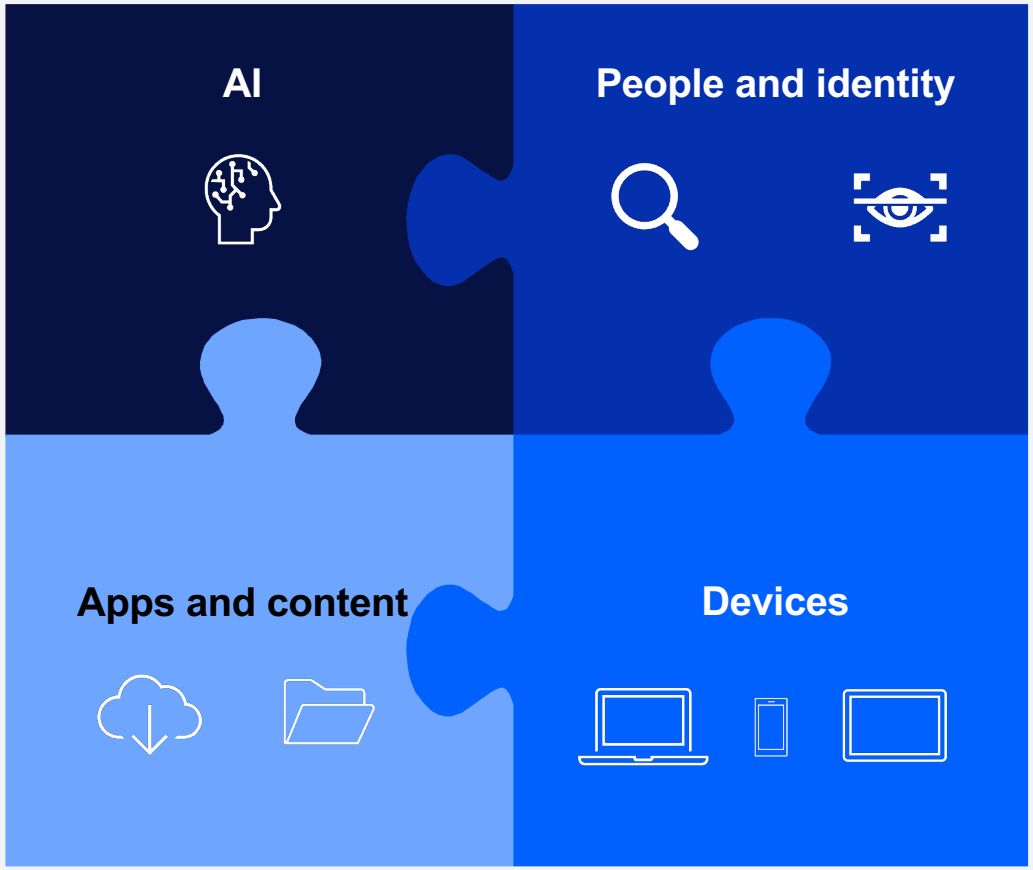
“As adversaries capitalize on newly discovered vulnerabilities, IT and security teams require the ability to rapidly assess risk and align mitigation strategies, enabling faster response..”

“Converging endpoint management and security processes and systems will help drive both efficacy and efficiency, leading to a reduction of risk…”

Source: Enterprise Strategy Group, Unified Endpoint Management and Security in a Work-from-anywhere World Ebook

Offering Strategy IBM Security MaaS360 with Watson

Unifies, secures, and manages devices and users



Unified Endpoint Management

- Provide best in class UEM/Modern Management coverage across all endpoints
- Enable co-existence with traditional endpoints management tools for laptop/desktop management
- Enable support for purpose built and industry focused use cases
- Expand admin and enable end user experience management
- Expand Device, App and end user Analytics and Automation

Zero Trust Endpoint Security

- Expand security detection, prevention and response on mobile endpoints with Threat Management
- Expand Security Analytics to enable response based on User and Device risk posture
- Enable Zero Trust and XDR use cases via integrations with IBM Security stack

Mobile Threat Management Overview

History

MaaS360 Threat Management

Historically has provided a targeted set of detections for Malware, JB/Rooted.

- No centralized policy
- No comprehensive response framework

MaaS360 Threat Management in 2021

- Detections
  - Trusteer Malware Detected
  - Jailbreak/Rooted
  - Insecure WiFi
  - Antivirus status
  - App Compliance State
  - Passcode Status
  - Critical Security Patch
  - Device Encryption Status
  - Device Managed Status
  - Device inactivity
  - OS and MaaS App Version
  - SIM Change
- Responses
  - Compliance rules
  - Risk Rules
- Insights and Analytics
  - User and Device Risk Scoring
  - Organization Risk Scoring

What’s new?

MaaS360 Mobile Threat Management now

Provide a set of detections and responses targeted primarily at Mobile Insider Threat use cases

Evolve Threat Management from a small set of detections (JB/Rooted, Malware, MDM attributes) scattered in various policies (MDM, Compliance Rules) and responses (OOC, Alerting, etc.) by providing additional high value detections and a consolidated policy and response framework

MaaS360 Mobile Threat Management Evolves in 2022

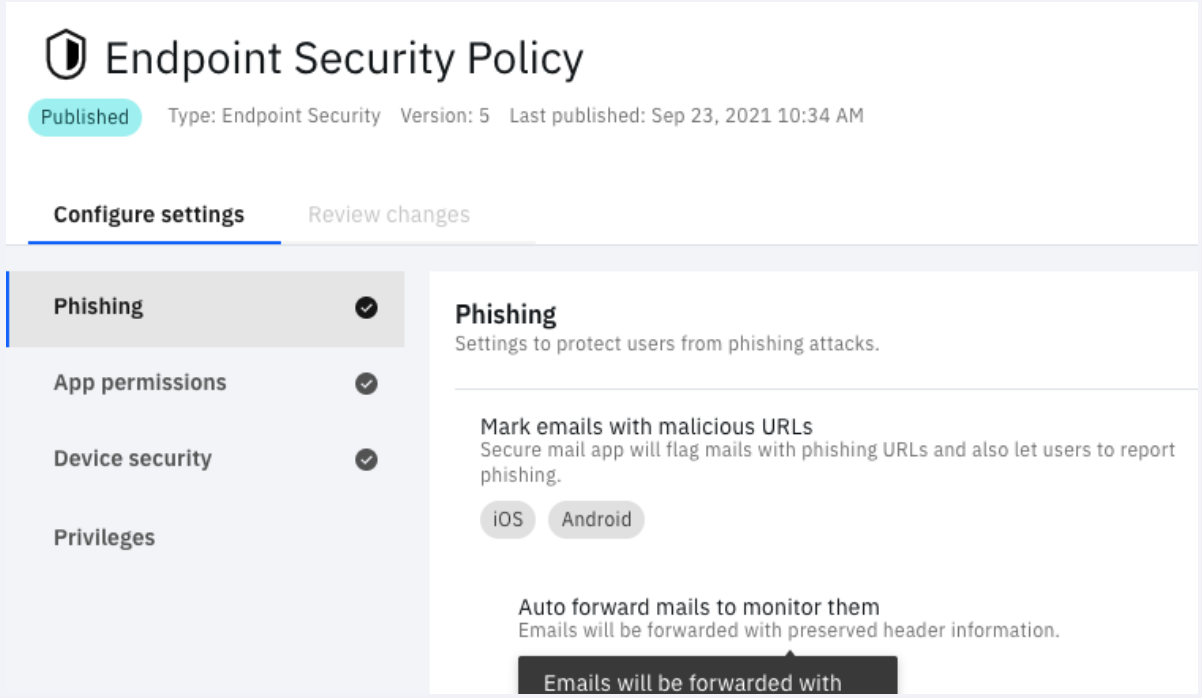
- Add useful, high value insider threat/zero trust detections
- Consolidate policy and response definition in a centralized policy
- Enhance the Risk Dashboard into a full function Security Analytics Dashboard
- Provide API based integration opportunities
- Bring it all together with Risk Based Conditional access to automate response to threats

General Availability

MaaS360 Threat Management evolves in 2022 by providing additional high value detections and a consolidated policy and response framework:

New Detections:	***New Endpoint Security Policy:***	***Enhanced Processing and SEIM/SOAR Support:***	***Mobile Threat Telemetry Integration:***
SMS and Email Phishing, Excess App Permissions (Android), Windows and Mac User/Privilege Detections.	A central policy to control detections and responses.	A new Security API that provides real time threat telemetry to broaden response and runbook processes.	Ingest 3rd party mobile threat telemetry and enrich with UEM device and user context.
	New Security Dashboard /Analytics / Integration:		
	Real time processing and viewing of user and device risk and threat events		

Endpoint Security Policy



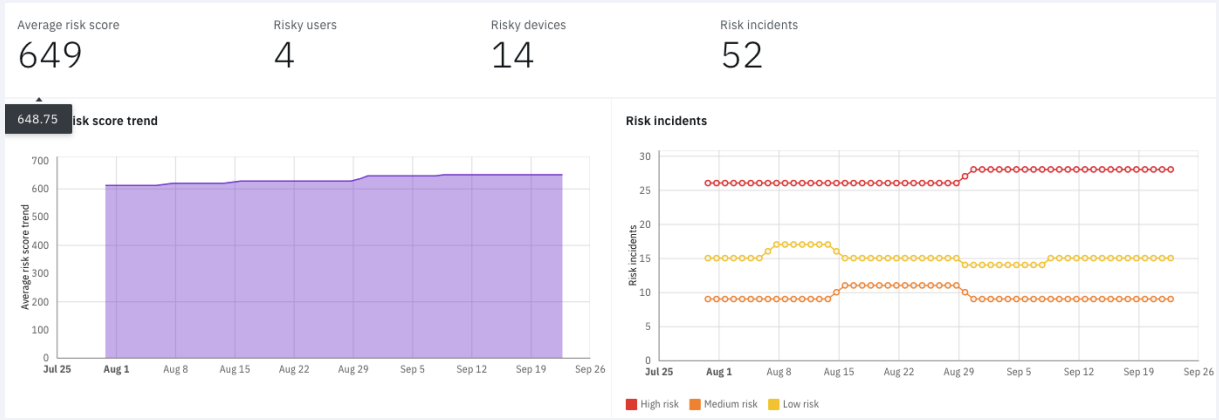
Deployment

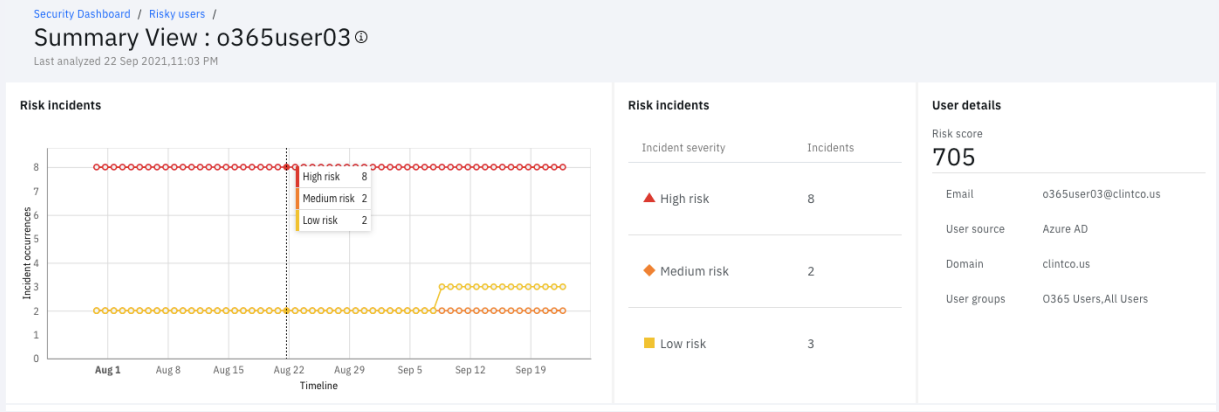
- Requires the MaaS360 agent
- The agent consumes the EPS Policy as configured on the MaaS360 portal

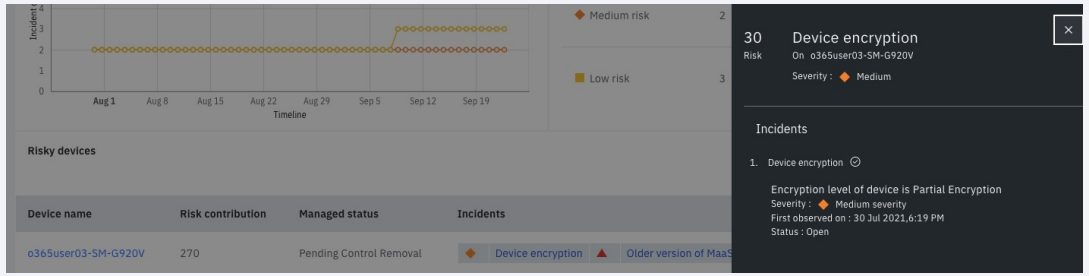
Includes policy for the following use cases:

- Trusteer signature-based JB/Rooted Detection
- X-Force Exchange Phishing Detection (Email and SMS)
- Excessive App Permission Detection
- Trusteer Malware and Insecure Wi-Fi Detection
- Windows and Mac User and Process Privilege Detection

Security Dashboard







- Detections appear on the Security Dashboard as Security Incidents and can be viewed on the MaaS360 Security Dashboard
- Security Incidents are also available via the Security API. This is primary QRadar Integration mechanism.
- Incidents are used to calculate a Risk Score based on Risk Rules. This is primarily for customers that do not use QRadar or QRadar UBA.

IBM MaaS360 Threat Management

Threat Telemetry Enrichment

Threat Telemetry Enrichment Overview – Zscaler Example

Summary of Zscaler

Zscaler is a market leader in Network Threat Detection and Access Control/ZTNA.

They provide:

➢Threat Intelligence

➢Network Threat Detections (Phishing, Anomalies, Data Leak/Exfiltration)

➢Network Gateway and Access Control/ZTNA

➢Threat API and Threat Telemetry feeds

MaaS360 can use Zscaler to augment detections and responses and can enrich and correlate telemetry to allow for greater visibility of insider and mobile threats in the enterprise.

Key Capabilities

- Enhanced Network Based Phishing detection based on Malicious URL detection
- Unified dashboard for threat events happening on a MaaS360 device
- Zscaler events contribute to User Risk rules/scoring data.
- Merge Zscaler and MaaS360 information to provide Device context for all threat events
- Provide this enriched data to upstream systems (SEIM, SOAR, XDR, etc.)

Future

- Add other Zscaler capabilities to support Insider Threat (Data Exfil, Data Leak) and ZTNA Use cases
- Leverage the Architecture and Approach (Threat Feed, Threat Telemetry Enrichment) for other partners (Wandera, etc.).

Mobile Threat and Risk Management Demo

What’s Next?

MaaS360 Mobile Threat Management Roadmap

Q4 2022 and Beyond

★New Detections/Responses

- OS and Application Vulnerabilities
- Risk Apps
- Compromised Creds (Trusteer)
- Additional Zscaler network Threat detections
- Additional Threat Telemetry Feeds (e.g. Lookout)

★Security Dashboard/Analytics/Integration

- Consume 3rd Party Risk Score – e.g. Zscaler/Wandera
- More Widgets (Event Feed)
- Per user timeline event view

★Risk Based Conditional Access

- Automated responses based on risk score threshold
- Conditional Access based on detections as defined by policy
  - Device OOC, Azure AD CA, IBM Security Verify CA

Enabling User Risk and Threat Management Features

Turning on User Risk and Threat Management Features

User Risk Management

★ Available to ALL customers

- Go Setup/Services and enable User Risk Management
  - Leverages MDM attributes to establish User and Device risk profiles.
- View Basic Threat Incidents, User Risk and other widgets in the Security Dashboard (Security/Security Dashboard)

Threat Management

★ Available to customers that have Enterprise Suite or the Threat Management Add on Part

- If entitled, Go Setup/Services and enable Threat Management
- View Advanced Threat Incidents (Malware, Phishing, App Permission, etc..), User Risk and other widgets in the Security Dashboard (Security/Security Dashboard)
- If not entitled, upgrade the the Enterprise Suite or purchase device or user licenses for the Threat Management Add on part through your sales channel

NOTE: For customers with User Risk Management and/or Threat Management enabled, your portal will be upgraded with the new features starting in the October timeframe. You will see a notification when migrated.

Questions?

Thank you

Follow us on:

https://www.ibm.com/products/maas360

https://www.ibm.com/topics/uem

ibm.com/security

securityintelligence.com

ibm.com/security/community

@ibmsecurity

youtube.com/ibmsecurity