

What's new in iOS 16 and Android 13 this Fall

Dhanasekar Varadarajan

Product Manager

IBM Security MaaS360

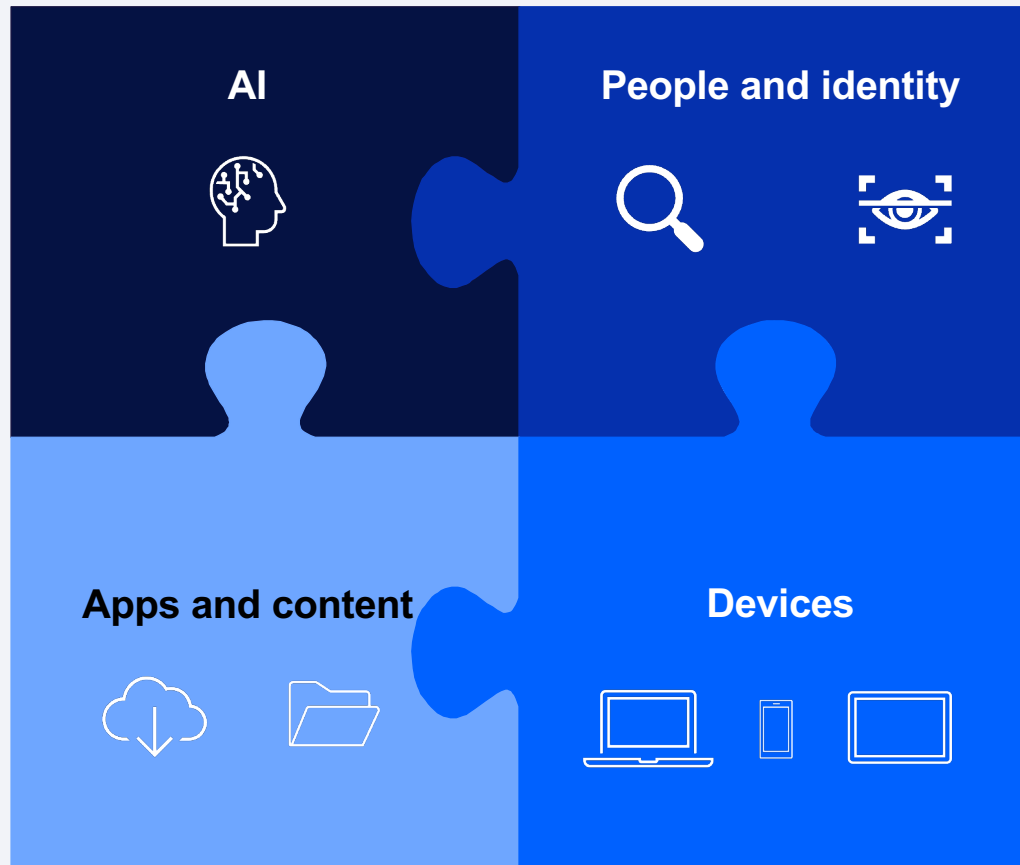
Olga Madalina Barbu

Product Marketing Manager

IBM Security MaaS360

Offering Strategy IBM Security MaaS360 with Watson

Unifies, secures, and manages devices and users



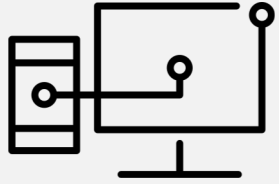
Unified Endpoint Management

- 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

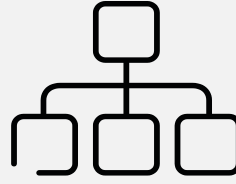
What sets IBM MaaS360 with Watson apart?



Complete UEM
of mobile devices,
laptops & things



Best-in-class cloud
on a mature, trusted
platform



Open
platform
for integration with
leading IT systems



Industry-best user
interfaces
for app catalogs & workplace
container



Dedicated to your
success
with 24x7x365 support by
chat, phone, email



**With
Watson™**

for actionable insights &
cognitive analytics



Fast deployment

Simple, self-service provisioning
process designed for maximum
configurability

Effortless scalability

Trial instantly becomes production
environment with ability turn up new
devices, users, apps

Automatic upgrades

Continuously updated daily with new
capabilities and same day OS support for
the latest platform

iOS 16

iPad OS 16

macOS 13



iOS 16 Restrictions – Zero Day (Q3 released)

- Mail Privacy Protection (iOS 15.2)
- Rapid Security Response
 - Automatic Install
 - Removal by end user

Allow Mail Privacy Protection 

If disabled, the device will not be able to use mail privacy protection

Allow Rapid Security Response Installation 

If disabled, the security patches cannot be pushed automatically.

Allow Rapid Security Response Removal 

If disabled, the end-user cannot remove the rapid security response

macOS 13 Restrictions – Zero Day (Q3 released)

- Allow Universal control
- Allow profile installation through interactive UI

Allow Universal Control



If disabled, disables Universal Control.

Allow UI Configuration Profile Installation

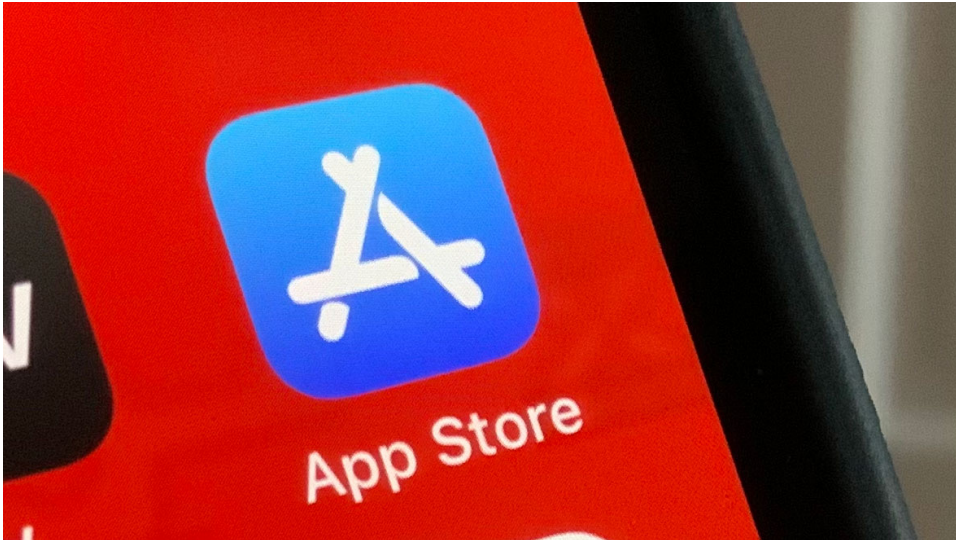


If disabled, prohibits the user from installing configuration profiles and certificates interactively.

Apple Business Manager

VPP 2.0 - Beta

- Utilizes new VPP 2.0 APIs from Apple.
- A more efficient and error free VPP license assignment and management.



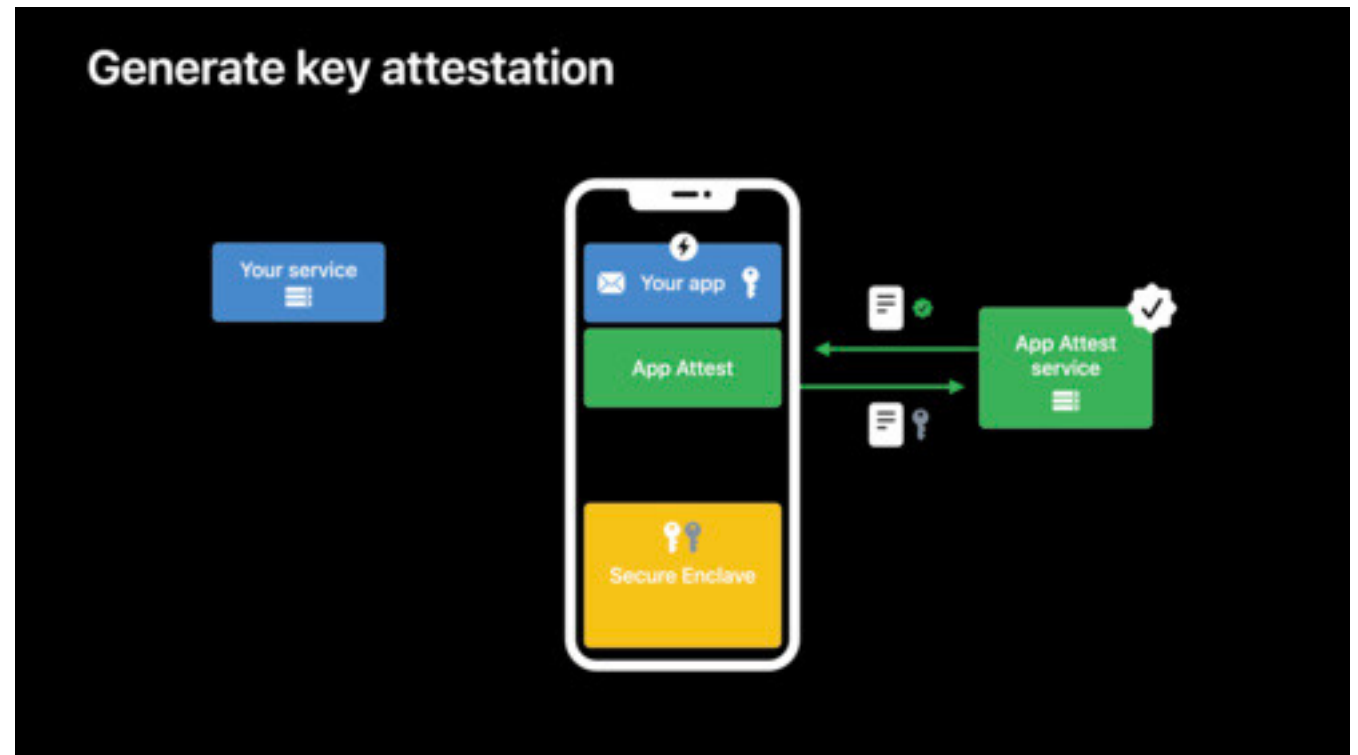
Managed Apple ID

- Apple Business Manager supports Google Workspace Directory
- Directory syncs automatically after connection and authentication is redirected.



Device Attestation - Roadmap

- Attestation helps to makes sure device is not compromised.
- Avoids attackers from stealing TLS private keys, spoofing legitimate devices or lying about device properties.
- Secure Enclave and cryptographic attestations to secure communications



User Enrollment - Roadmap



Single Sign-on

- Enroll devices through SSO.
- Needs support from Idp for SSO Extension app
- Oauth 2.0 support is added

Per-app networking

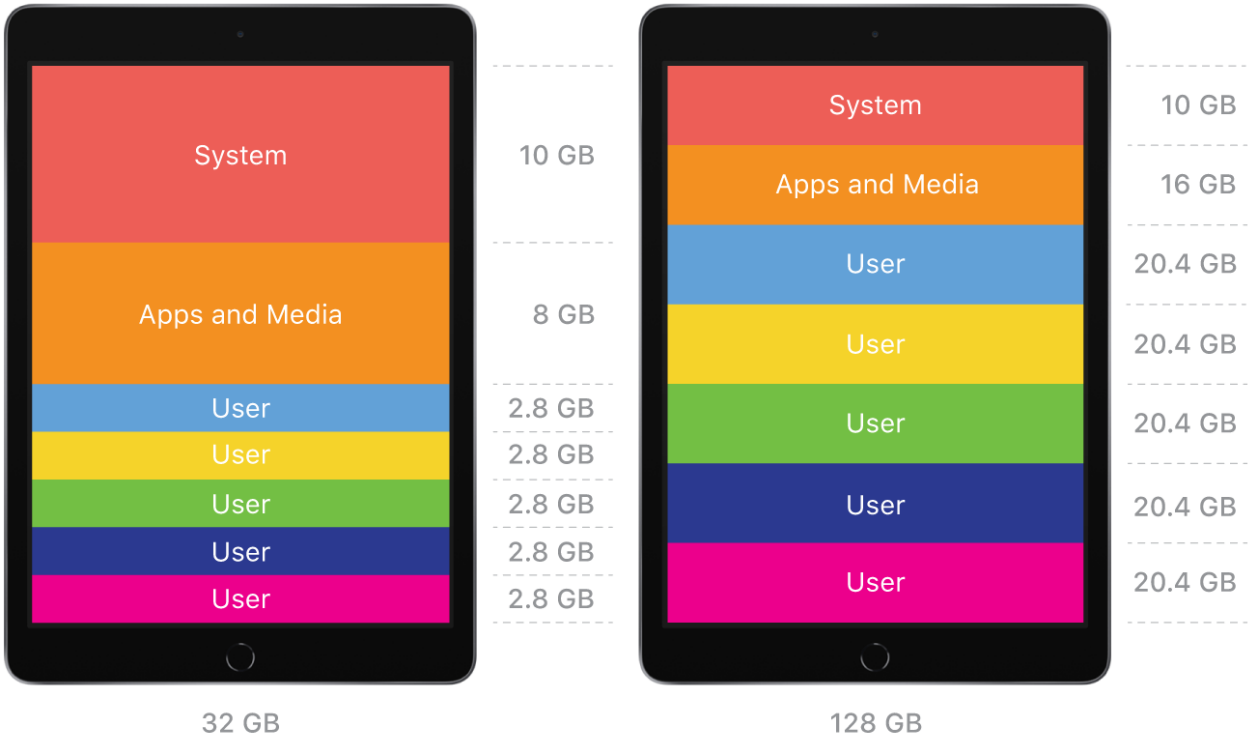
- DNS proxies and web content filters can be routed through this tunnel
- Personal apps traffic does not go through this tunnel

More apps..

- Full data separation for Calendar and Reminder apps for Managed Apple ID.

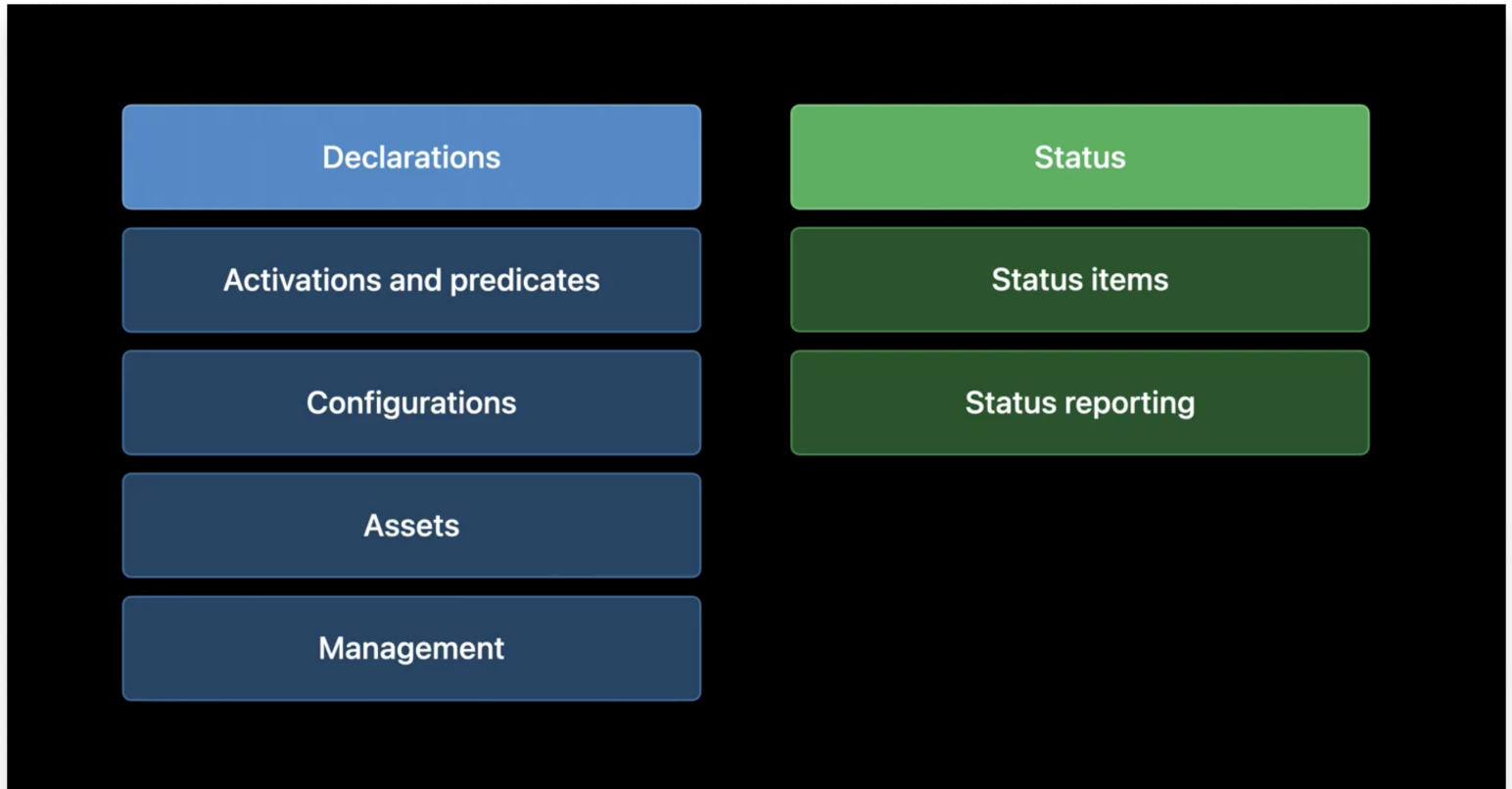
Shared iPads - Roadmap

- Default domain can be configured by administrator
- Offline authentication with grace period.



Declarative Management - Roadmap

- More efficient way to manage Apple devices.
- Better control over payloads processing.
- Now available from Apple for all enrollment types
- Status reporting is being targeted first.

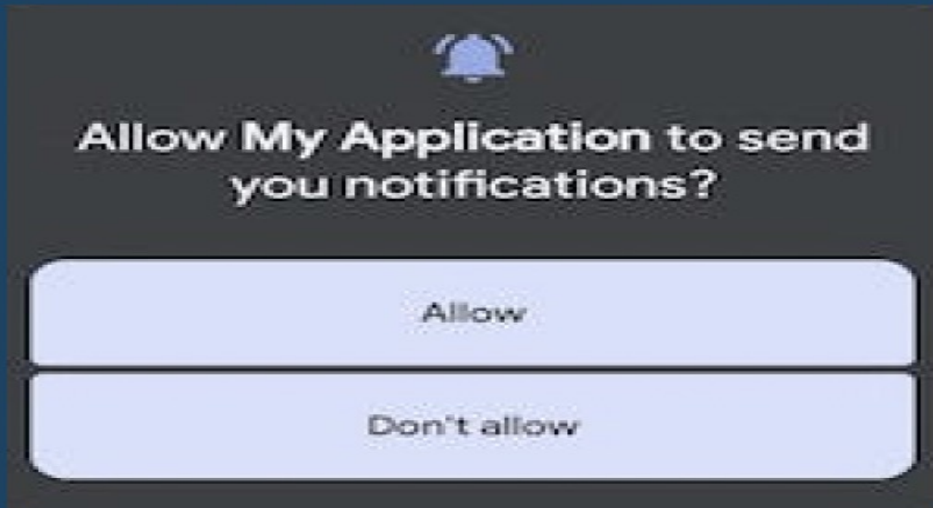


Android 13



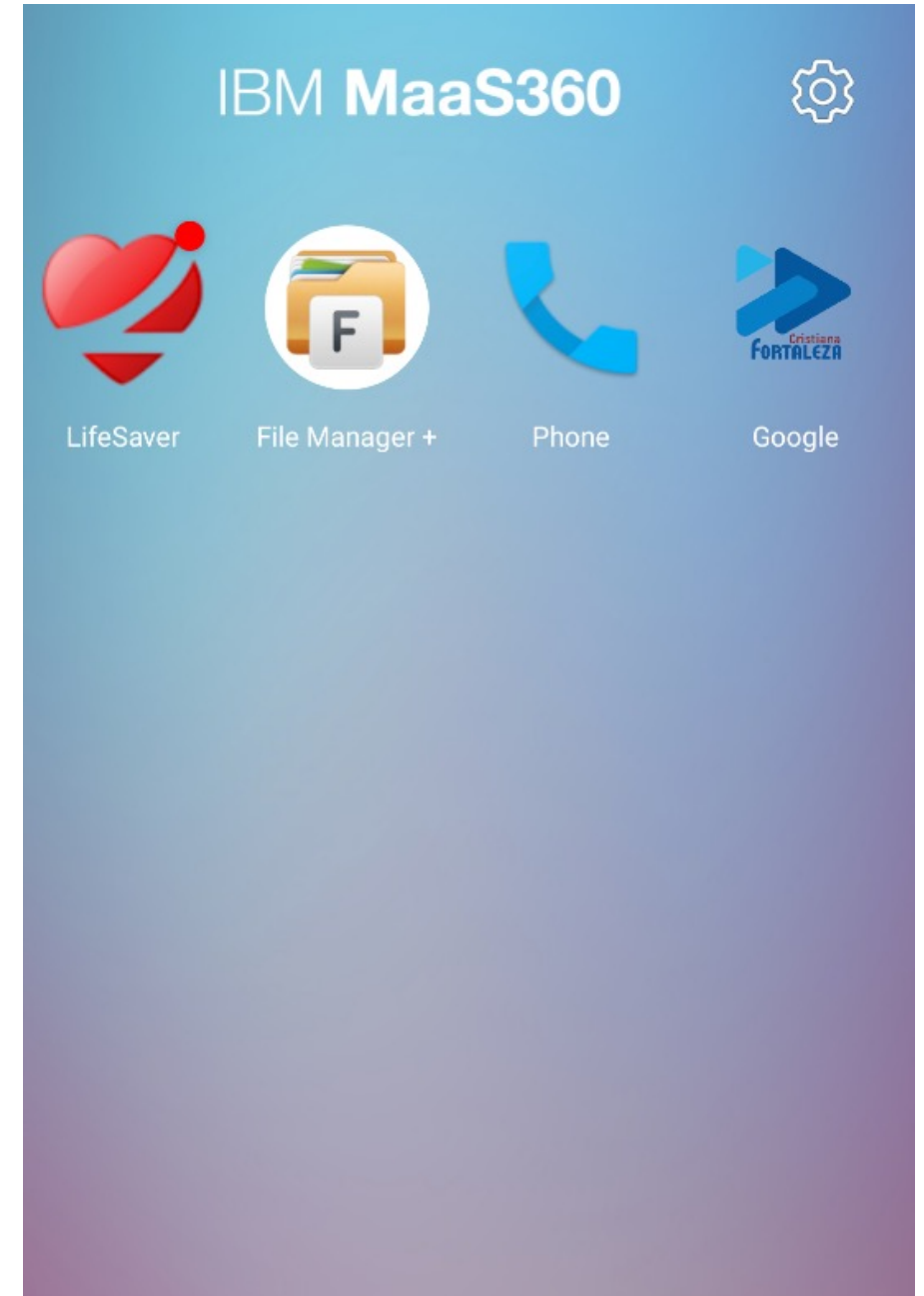
Notifications Permission – Zero Day

- Android 13 does not allow notifications for apps by default.
- End user will be prompted for permission.
- Instead, through MaaS360, runtime permission for notification can be set for apps.
- MaaS360 family of apps has default runtime permission granted in MDM enrolled devices.



Deprecation – Kiosk APIs

- Google deprecated Kiosk APIs for Non-OEM devices for Device Admin mode.
- Google encourages customers to move to Android Enterprise mode with more deprecations.
- No impact on Android Enterprise devices.



More Configurations - Roadmap

Network Configuration

- Preferred network configuration to be used for Android devices.

Wi-fi Connection Modification

- Let administrator to control an end user to add/share/enable wifi

Device Provisioning

- Offline option for device provisioning
- Keep screen on throughout provisioning.



Q & A

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](https://twitter.com/ibmsecurity)

youtube.com/ibmsecurity

© Copyright IBM Corporation 2020. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.