NTT DATA Services

CASB to Enable Secure Remote Work
NTT DATA Services for Microsoft Cloud App Security

April 2021

© 2021 NTT DATA, Inc. All rights reserved.

Enterprise-class technology to work securely in office or while remote

The Way We Work Has Evolved – Security Needs To Evolve As Well

CASBs Help Protect and Govern Your Cloud Apps

Cloud Access Security Broker (CASB):

Gartner defines a CASB as a security policy enforcement points, placed between cloud service consumers and cloud providers to combine and interject enterprise security polices as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement.

- CASB is a top ranked security priority for most companies
- Microsoft has the largest CASB market share with >30%**
- Microsoft Cloud App Security is a leader in the Gartner CASB Magic Quadrant

By the end of 2020

85%

of large enterprises will use CASBs*

>1,000
cloud apps used by the average enterprise, 80% of employees use unsanctioned apps

28%
increase in cloud and SaaS threats over the last year alone*

73
Data records are stolen every second

12%
of IT teams understand how GDPR will affect their cloud services**

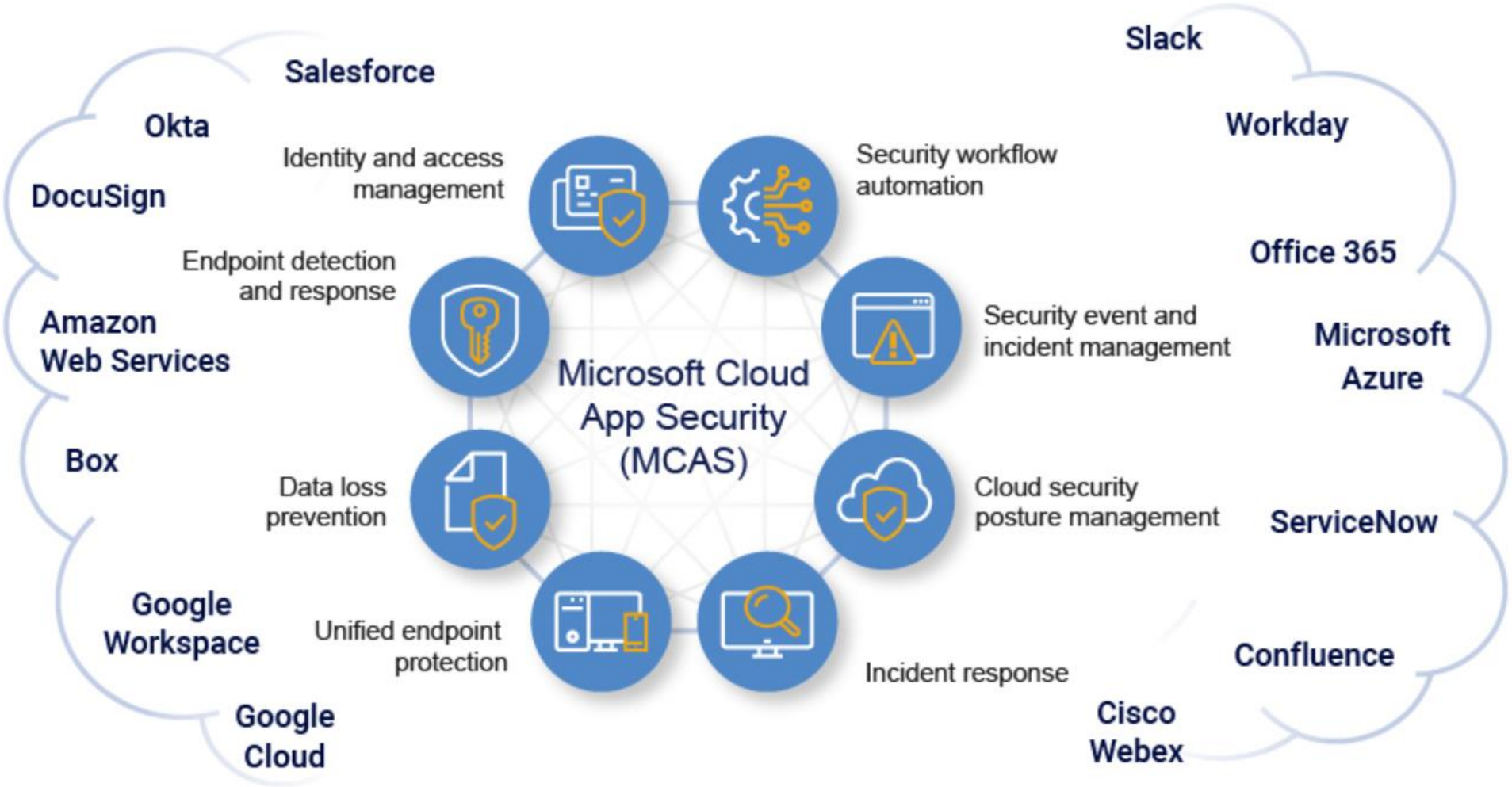
© 2021 NTT DATA, Inc. All rights reserved.

Microsoft

CASBs Help Protect and Govern Your Cloud Apps

Serving As An Integral Element of Your Holistic Security Program

- Connects to your existing security solutions
- Natively integrated across the broader Microsoft product stack to deliver unique capabilities
- Enables policy enforcement across your SaaS apps
- Helps drive zero trust objectives



Maximize your security posture by integrating your existing solutions and investments with MCAS

Defense in Depth – Securing your Data, Apps & Users

The challenge

- Bad actors are using increasingly creative and sophisticated attacks
- The digital estate offers a very broad surface area that is difficult to secure
- Data & users no longer reside behind your firewalls
- Intelligent correlation of signals is difficult, time-consuming, and expensive

The solution

Better together – Microsoft 365 Security products to protect your organization from threats

Microsoft Cloud App Security + Microsoft Defender for Endpoint + Microsoft (Azure) Information Protection + Azure Active Directory

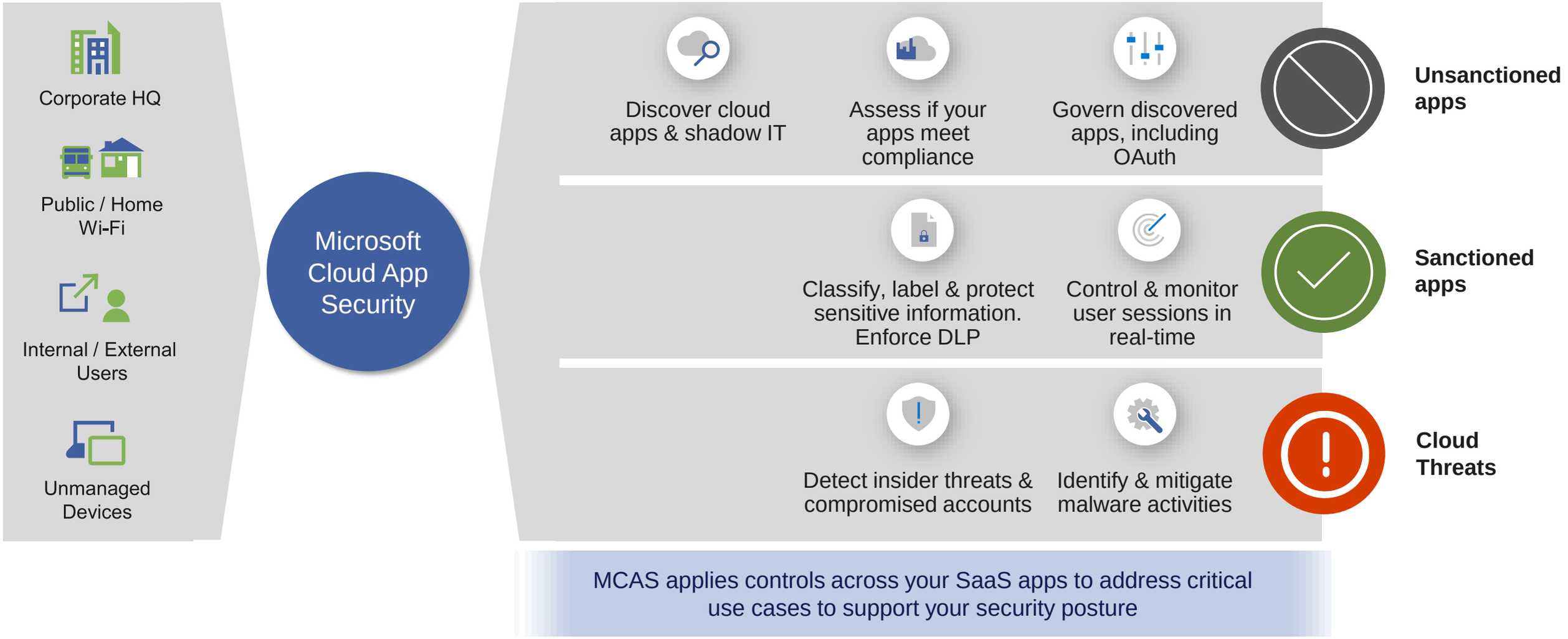
Focusing on MCAS, NTT DATA recommends a strategic approach targeted at specific use cases to optimize your cloud security posture

Identify & Discover Shadow IT → Protect Your Information → Detect & Prevent Threats → Monitor & Control in Real Time

A pragmatic and phased deployment will allow for the refinement of controls and best practices in a mindful manner

© 2021 NTT DATA, Inc. All rights reserved.

Microsoft Cloud App Security Helps Protect Your Organization From the Inside Out



MCAS applies controls across your SaaS apps to address critical use cases to support your security posture

© 2021 NTT DATA, Inc. All rights reserved.

Identify and Prevent Shadow IT: Detect and control apps in your environment

Leverage MCAS's shadow IT capabilities to increase governance and control, reduce vulnerabilities and ensure your security and compliance requirements are met

Continuous monitoring

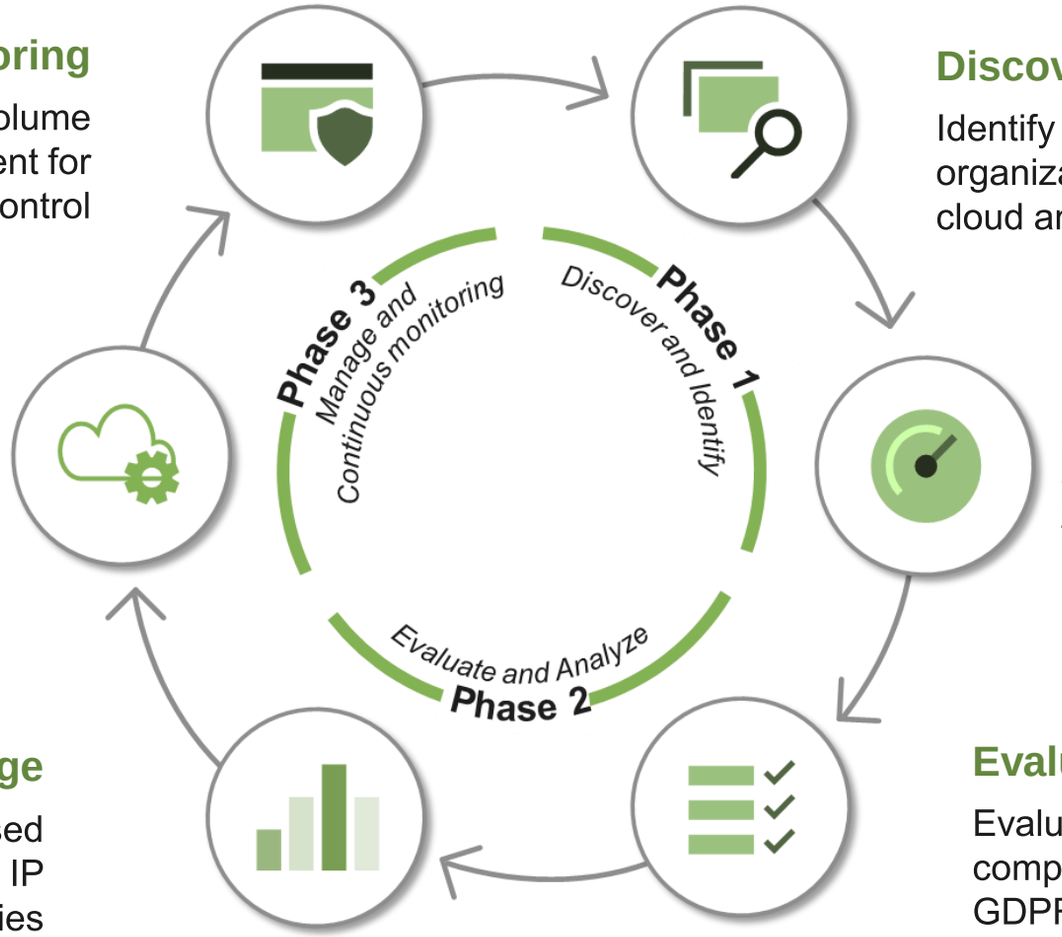
Be alerted when new, risky or high-volume apps are found in your environment for continuous monitoring and ongoing control

Govern your cloud apps

Managing cloud apps with governance capabilities such as sanction, unsanction, or blocking them from your network

Analyze usage

Understand usage patterns based on traffic data, top users, IP addresses and app categories



Discover Shadow IT

Identify which apps are being used in your organization from a catalog of 16,000 cloud and custom apps

Identify app risk levels

Understand the risk associated with your apps, based on more than 70 risk factors (e.g. security, industry and legal regulations)

Evaluate compliance

Evaluate whether the discovered apps meet compliance standards against factors like GDPR or HIPAA readiness

© 2021 NTT DATA, Inc. All rights reserved.

Protect Your Information: Safeguarding Files and Data in the Cloud

Data is ubiquitous and you need to make it accessible and collaborative, while safeguarding it

Understand your data and exposure in the cloud

- Connect your apps via API-based App Connectors
- Visibility into sharing level, collaborators and classification labels
- Quantify over-sharing exposure, external- and compliance risks

Classify and protect your data no matter where it's stored

- Govern data in the cloud with granular DLP policies
- Leverage Microsoft's IP capabilities for classification
- Extend on-prem DLP solutions
- Automatically protect and encrypt your data using Microsoft (Azure) Information Protection

Monitor, investigate and remediate violations

- Create policies to generate alerts and trigger automatic governance actions
- Identify policy violations
- Investigate incidents and related activities
- Quarantine files, remove permissions and notify users

We leverage your Microsoft (Azure) Information Protection & DLP solutions to extend the ability to classify and protect sensitive information exposure with embedded policies and automated controls. We do this while blocking specific users from taking malicious or dangerous actions within your applications.

© 2021 NTT DATA, Inc. All rights reserved.

Detect and Prevent Threats: Protection Against Cloud Risks

MCAS allows for the monitoring of unusual behavior and anomalies across SaaS apps to mark malware and ransomware attempts, compromised identities, or rogue applications. MCAS can be leveraged to analyze high-risk usage and automatically remediate issues to limit negative impacts.

Malicious insider

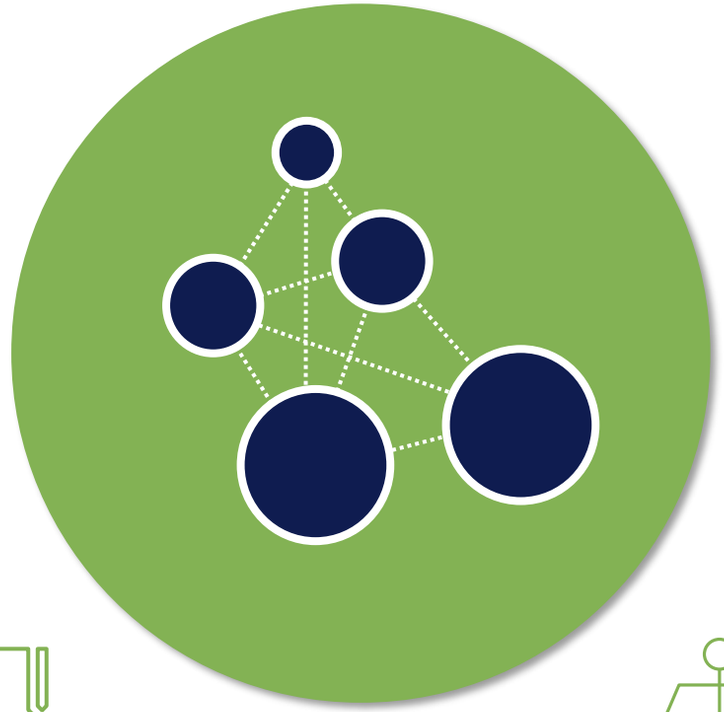
Protect against disgruntled employees before they cause damage

Malware

Detect and detonate malware in cloud apps as soon as it's uploaded

Ransomware

Identify ransomware using sophisticated behavioral analytics technology



Rogue application

Identify rogue applications that access your data

Data exfiltration

Detect unusual flow of data outside of your organization

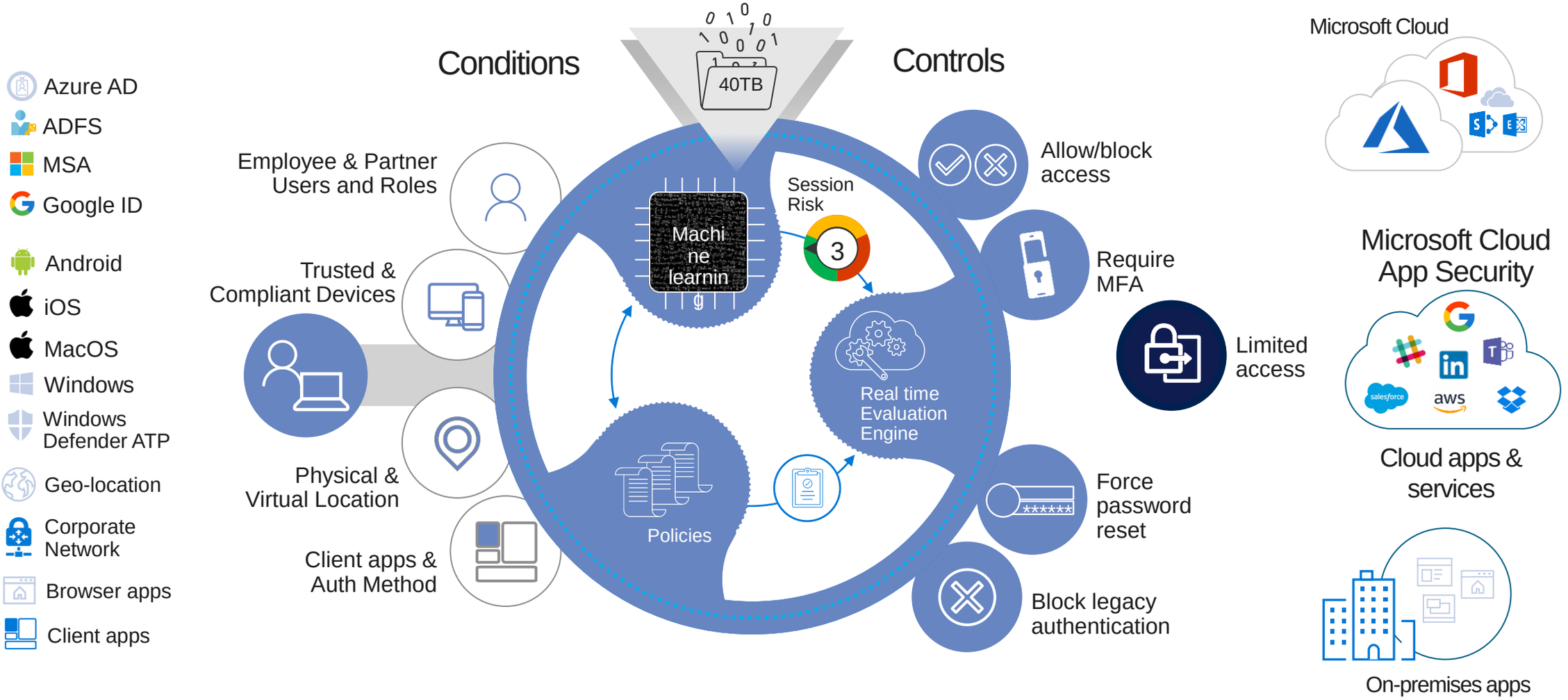
Compromised accounts

Combat advanced attackers that leverage compromised user credentials

© 2021 NTT DATA, Inc. All rights reserved.

Monitor & Control in Real-time with Conditional Access App Control

Enable access and session controls on SaaS applications, to help stop breaches or leaks in real-time as well as limit access to regulated or sensitive data



© 2021 NTT DATA, Inc. All rights reserved.

NTT DATA's Approach To Maximize Your MCAS Controlled Landscape

Advisory

A workshop series to educate your team and develop a strategic approach for deploying MCAS tailored to your organization's requirements

- Consultative 8-part workshop series to educate your teams on MCAS functionality and best practices
- Develop a CASB strategy that aligns with your security framework, compliance requirements and in-scope applications
- Perform SaaS app discovery to assess risk levels of in-scope applications
- Validate risk-tolerance levels for low-trust apps and determine specific policies to safeguard against threats
- Develop a comprehensive design guide and implementation plan

Implementation

A phased approach to ensure MCAS is configured and deployed to best practice standards to enable robust functionality that safeguards against malicious activity

- Identify & Discover Shadow IT – Identify and prevent unauthorized access to apps in use
- Protect your Information – Data classification and integration with Azure Information Protection to shield sensitive data
- Detect & Prevent Threats – Anomaly and malware detection to identify and mitigate vulnerabilities
- Monitor & Control in Real Time - Enable Conditional Access App Control to prevent and restrict risky activities
- Enabling Controls – Fine tune policies and configurations set in earlier phases, enable automated policies

Managed Services

Comprehensive operational support and security posture optimization to help future-proof your organization from ever-maturing and complex threat actors

- Monitor for threats, risky behavior and abnormal patterns, investigate alerts.
- Tune anomaly detection to reduce false positives
- Investigate questionable apps or usage, analyze data exposure & review activity logs
- Incident and remediation support to mitigate threats, such as quarantining infected files
- Continual optimization to improve your security posture, including automation to reduce manual intervention
- Support audit preparations

© 2021 NTT DATA, Inc. All rights reserved.

Why Partner With NTT DATA

Microsoft Partner

Microsoft

- Gold Security
- Gold Cloud Platform
- Gold Cloud Productivity
- Gold DevOps
- Gold Application Integration

A **Leader** in cyber resiliency (security consulting, strategy, incident response and business continuity)

NelsonHall, "NEAT report for Cyber Resiliency," June 6, 2019

Regulatory & Industry Compliance & Certifications

HIPAA

Gartner peerinsights customers' choice 2019

SAS 70 Type II

INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2019

ITIL®

A **Leader** Worldwide Managed Security Services

IDC MarketScape for Worldwide Managed Security Services 2020

- Microsoft Azure Expert Managed Service Provider
- Microsoft Azure Advanced Specializations: SAP on Azure & Windows Server & SQL Server Migration
- 15 Gold Competencies, 2 Silver
- NTT & Microsoft Strategic Alliance
- CSA Corporate & CNCF Silver Member

- **3500** cloud architects & engineers
- **500+** cloud clients
- **5000+** cloud migrations
- **430+** Azure certifications
- **4300** experts on Microsoft technologies

- **3000+** security experts
- **6.1+ trillion** logs analyzed annually
- **9** SOCs and **7** R&D centers
- **6.2 billion** attacks defended annually
- **150+ million** identities managed

A **Leader** in the Gartner Magic Quadrant for Application Security Testing

Gartner, Inc. Magic Quadrant for Application Security Testing, April 29, 2020

Application Modernization:

- **9500** app clients, globally
- **1000+** DevOps build & release (CI/CD) engineers
- **200+** Agile certified resources

© 2021 NTT DATA, Inc. All rights reserved.

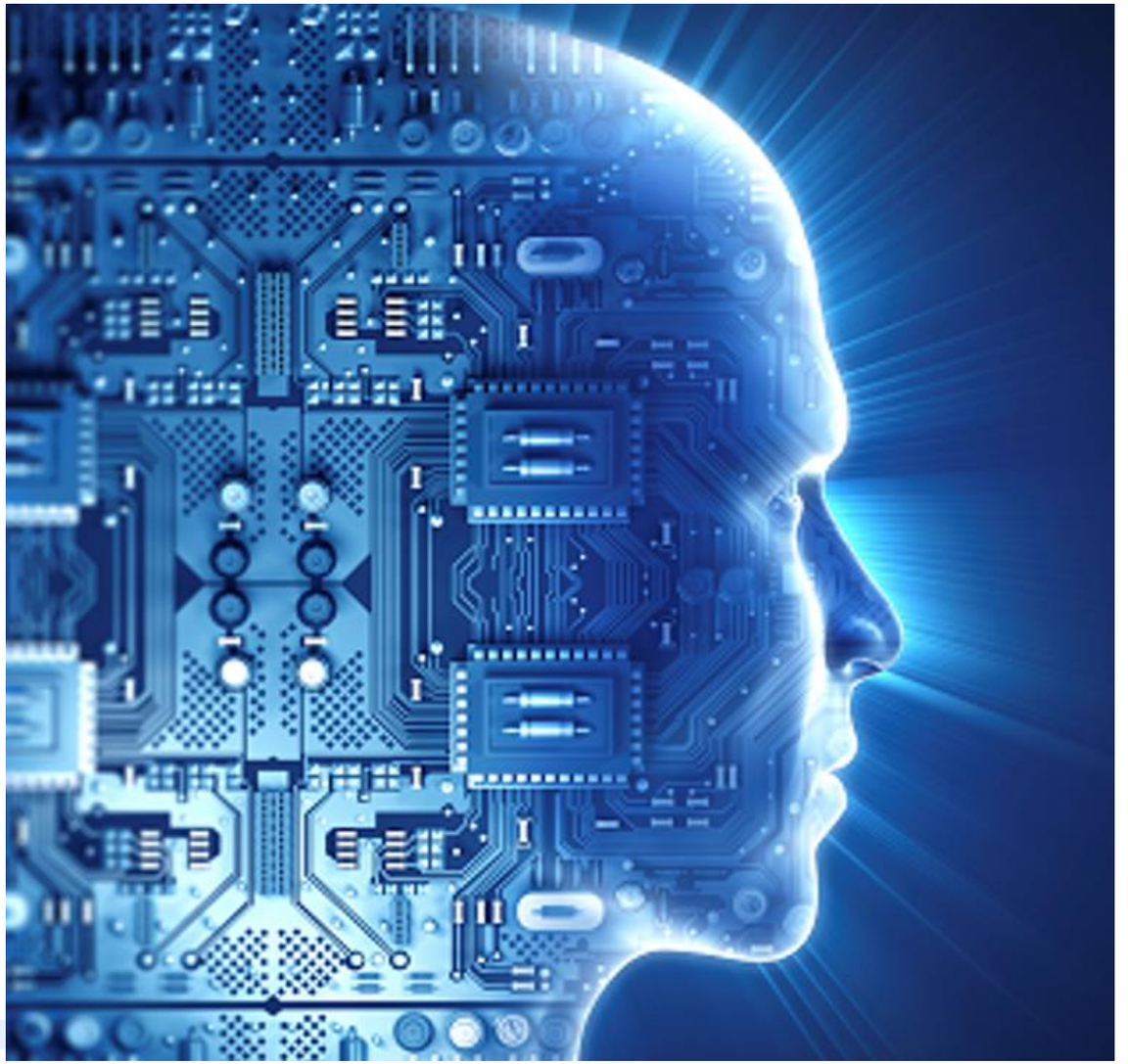
NTT DATA

Trusted Global Innovator

© 2021 NTT DATA, Inc. All rights reserved.

Extend Real-Time Monitoring Capabilities with SIEM

NTT DATA Cyber Security Defense and Response Center



NTT DATA's next gen SIEM uses machine learning to detect advanced threats and provides AI-based security incident response capabilities for fast remediation.

Capabilities include:

- Incident and event management
- Security Operations
- Log management
- Threat-detection & mitigation
- User and entity behavior analytics
- Service Orchestration & Automation Remediation (SOAR)

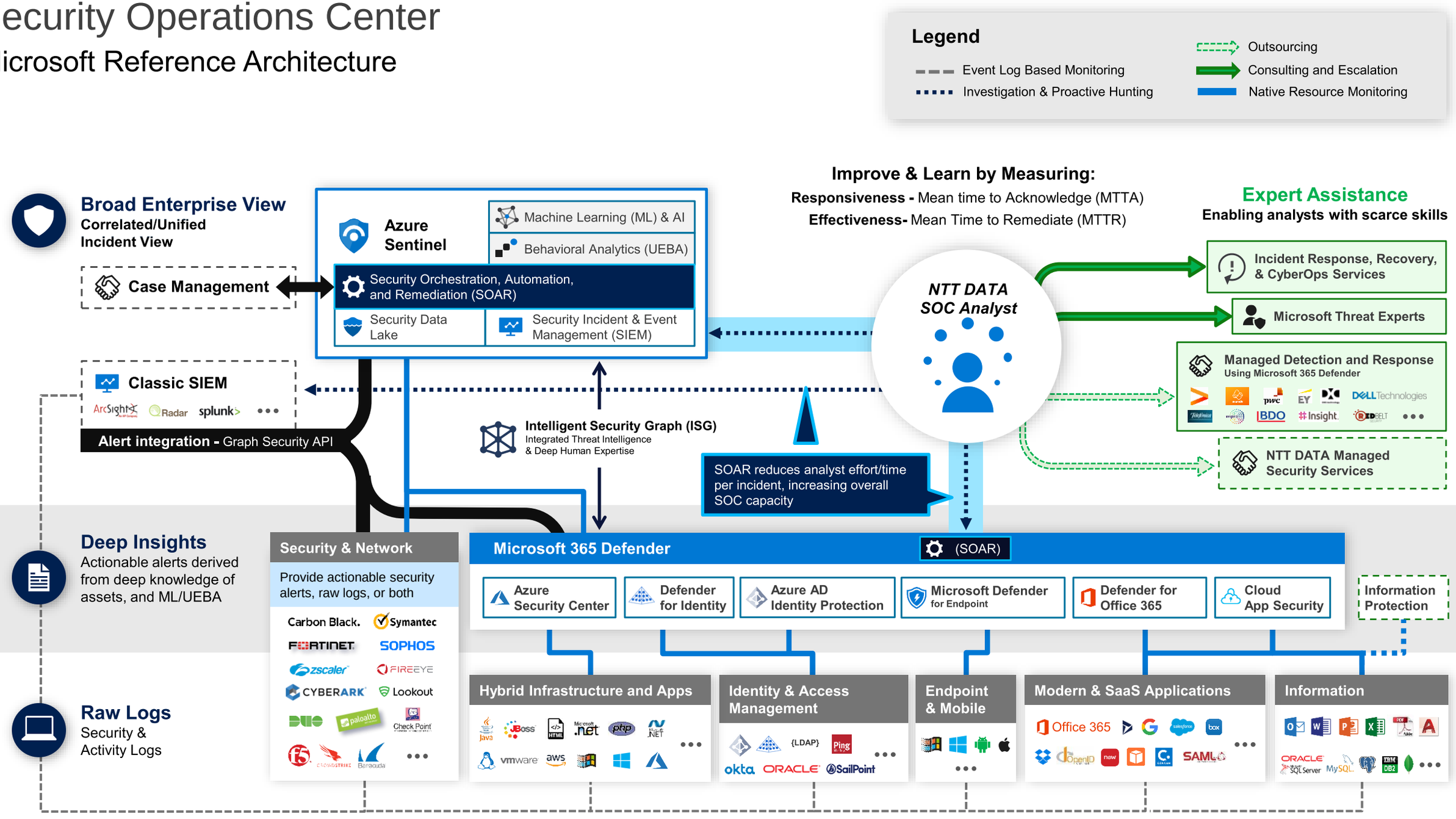
NTT DATA's Next-Gen SIEM, powered by Securonix

NTT DATA's SIEM Gathers Alert Data Across the Microsoft Ecosystem

- Azure Security Center
- Azure Active Directory Identity Protection
- Microsoft Cloud App Security
- Microsoft Defender Advanced Threat Protection
- Azure Advanced Threat Protection
- Azure Sentinel
- Office 365 ATP
- Azure Monitor
- Azure Log Analytics
- Event Hub
- (Plus parallel AWS capabilities)

Security Operations Center

Microsoft Reference Architecture



Licensing

Microsoft Cloud App Security

CASB for any cloud app

- Standalone
- Microsoft Cloud App Security + Enterprise Mobility & Security E3
- Enterprise Mobility & Security E5
- Microsoft 365 E5 Security (Includes: O365 ATP Plan 2, MCAS, Azure ATP, Azure AD P2, Microsoft Defender ATP)
- Microsoft 365 E5 (Highest tiers across Enterprise Mobility + Security, Office 365 & Windows)

Azure Active Directory

Identity & Access Management - AAD Premium 1 or Premium 2 provides CAS Discovery of Shadow IT

Premium Plan 1

- Standalone
- Enterprise Mobility + Security E3
- Microsoft 365 Enterprise E3

Premium Plan 2

- Standalone
- Enterprise Mobility + Security E5
- Microsoft 365 Enterprise E5
- Microsoft 365 E5 Security

Microsoft Defender for Endpoint

Protection and optics into endpoint activities

- Standalone
- Windows 10 Enterprise E5
- Microsoft 365 E5
- Microsoft 365 E5 Security
- Windows VDA E5

Microsoft Azure Information Protection

AIP Premium 2 - Data Protection & unified labeling

- Standalone
- Enterprise Mobility + Security E5
- Microsoft 365 E5
- Microsoft 365 E5 Compliance

NTT DATA MCAS Advisory Engagement Overview

Zero Trust Assessment

- Conduct a zero trust assessment. Review high-level environment architecture and security solutions currently in place
- Discuss business concerns and requirements
- Output - a Zero Trust evaluation report and top line objectives, concerns and requirements

Introduction to MCAS

- Review MCAS features and functionality and how these can be used to protect your SaaS apps
- Discuss how MCAS capabilities can address your concerns and specific goals to accomplish
- Output - prioritized list of objectives

Discover Shadow IT

- Perform a SaaS Discovery to assess risk levels of your current apps
- Validate risk-tolerance levels and determine specific policies to safeguard against threats
- Output - defined policies and controls that meet your Shadow IT reduction requirements

Protect Your Information

- Identify parameters, policies and to meet your data protection objectives
- Discuss your data classification strategy and labeling taxonomy
- Output - defined policies that meet your data protection requirements and what actions will be taken should a policy be violated.

Detect & Prevent Threats

- Define parameters and controls conducive to your business, technical and compliance requirements
- Discuss OAuth usage, history of threats, as well as known issues or concerns
- Output - defined policies and controls that meet your threat prevention requirements and what actions will be taken to mitigate risks

Monitor & Control in Real-time

- Determine what actions should be taken to enable real-time controls (i.e. preventing data exfiltration, low trust session handling, etc.)
- Outline session and access policies for non-standard apps
- Output - defined policies that meet your goals, as well as what actions will be taken for remediation

Enabling Controls

- Discuss the test plan process for enabling controls across the environment and determine the preferred approach so that productivity is not disrupted
- Output - agreed upon test plan approach and procedures

Design Guide

- Summarize all gathered intel & established parameters, configuration details and data.
- Output - a design guide, architectural diagram and an implementation plan combining your requirements and NTT best-practices

Overview of the NTTD MCAS Implementation Phases

Discover & Prevent Shadow IT *Apps are assessed to identify shadow IT & what risk levels they carry*	Protect Your Information *Data protection is enables to safeguard sensitive information*	Detect & Prevent Threats Prohibit malicious behavior stemming from malware, ransomware & compromised identities	Monitor & Control in Real-time *Enable controls to restrict breach attempts and leaks in real-time*
• Configure MCAS, admins, network settings, connect relevant domains, create IP tags/ranges, and operational settings • Integrate data via MDATP, network and proxy traffic, firewall and/or SWG logs, as well as SIEM agent • Work with the IAM team to enable Azure AD integration to unlock the ability to assess specific user behavior. • Evaluate the app landscape for risk, un/sanction or restrict • Develop policies to automatically identify at-risk or non-compliant app usage, set to alert.	• Integrate mail server and MIP/DLP • Develop file policies to validate protected data is not shared, accessed or handled inappropriately, set policies as an alert • Anonymize data • Help develop automated remediation actions • Determine automated governance actions to reduce manual intervention • Develop File & Session policies to address and alert on scenarios	• Enable threat and identity-related anomaly detection, create policies to identify events (ransomware activity, mass download, impossible travel) • Configure Session Controls to prevent the infiltration of malware • Develop policies to suspend user sessions if abnormal behavior is detected, set alerts for the activities to assess patterns • Enable policies to support advanced threat detection via UEBA & ML to include IP ranges and sensitivity settings	• Configure Conditional Access App Control to enable access and session controls to prevent threats (i.e. data exfiltration, low trust session handling, etc.) • Work with the IAM team to configure Azure AD Conditional Access policy to route relevant apps to MCAS • Configure the apps being deployed to route requests and cookies through MCAS to enable session policies • Configure applicable policies

Enabling Controls

Assess usage and performance patterns from the captured alerts established during the preceding phases to validate the controls meet the objectives. Configure governance controls based on required modifications as indicated during the testing process.

NTT DATA MCAS Managed Services

Operational Support

Operational support to ensure MCAS is operating efficiently. We monitor for threats and provides remediation to help mitigate exposure to risk.

- Monitor for policy violations (e.g. compromised identities, infected files, sensitive data exposure, internal threats, and session/access policy violations
- Investigate policy violation alerts, analyze exposure. Investigation includes:
  - Tune anomaly detection to reduce false positives
  - Review audit trails of high severity incidents to determine cause and help prevent recurrence
  - Assess infected files and determine path to mitigate, as well as impacts of breaches
  - Analyze suspicious user activity (e.g. suspicious behavior, lateral movements, etc.)
- Remediate detected violations per preapproved responses (automated when possible to reduce potential human error). Examples include:
  - Quarantine an app with a known security breach. Suspend a comprised user's credentials. Block an unmanaged device from accessing sensitive data. Place an admin quarantine on files that contain a threat.

Optimization Support

Continual improvement efforts to consistently improve the client's security posture

On a monthly basis:

- Assess usage patterns and risk levels, determine points of concern
- Capture newly added apps that may pose a Shadow IT risk; for consideration of un/sanctioning, or blocking
  - Capture data being shared externally for visibility and client required action to mitigate risk
  - Note unusual behavior, present recommendations
  - Identify users that pose an internal risk, to include an analysis of the top 10 users identified for investigation. With approval, suspend user for further investigation.

On a quarterly basis:

- Identify automation opportunities, to reduce manual intervention based on identified patterns
- Provide recommendations of additional policies if identified patterns appear to be risky

Audit Support

Support client-let audit preparations for compliance or security program-related efforts

Audit assistance on up to a biannual basis. Such entitlements include:

- If data anonymization is in place, upon request we can resolve usernames and PII should it be required for an audit
- Export MCAS data upon request
- Detailed data usage reports
- Off-band reporting per client-directed requirements