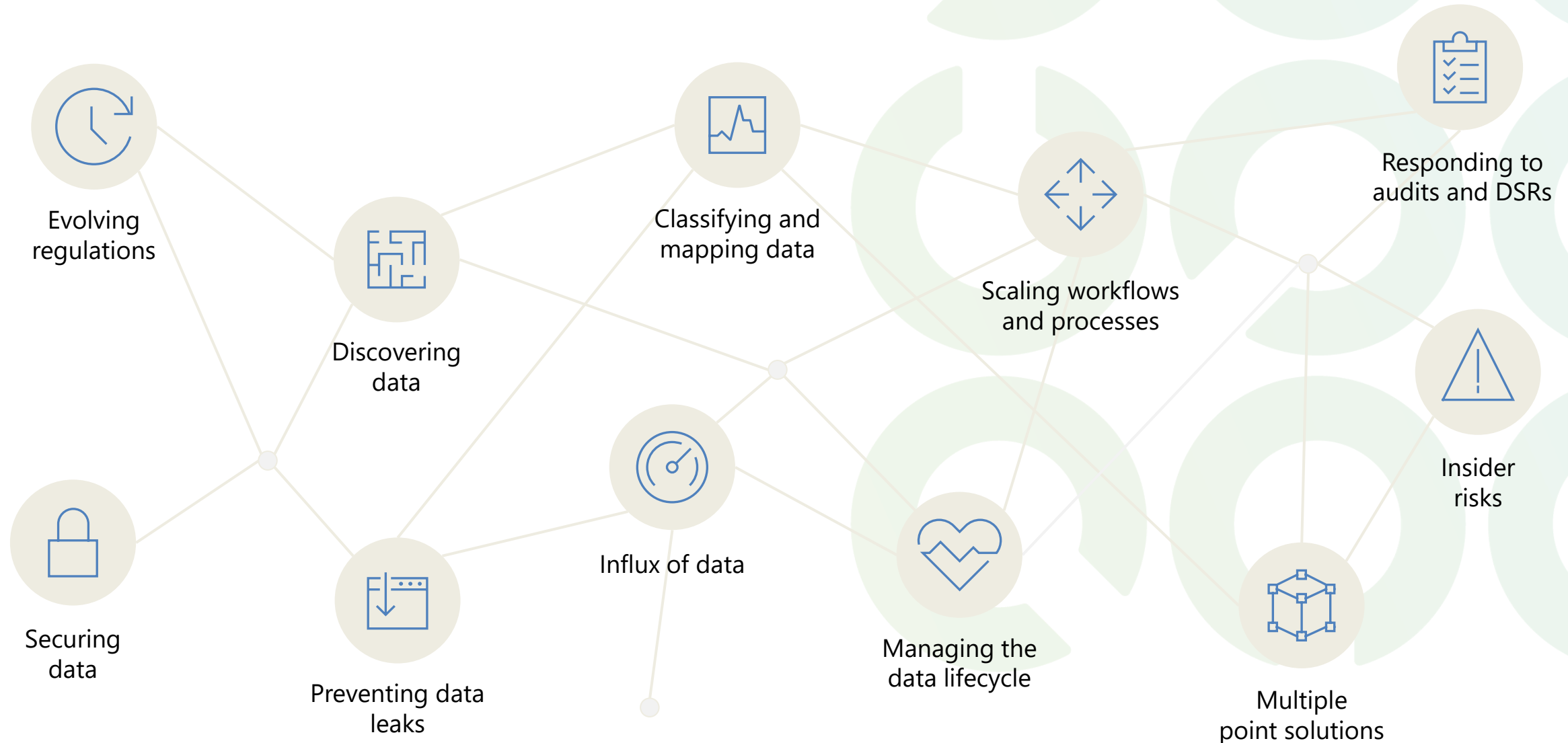


Managing Compliance Risk & Audit in a Remote Work Environment

Nelson Yuen
Compliance Global Black Belt, Microsoft

28 Aug 2020

Managing data and reducing risk is challenging



GTACS 2020
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY

ISACA
Singapore Chapter

What our customers are saying...



65%

Compliance budgets have increased in response to the pandemic.

Worldwide COVID-19 Security and Compliance flash poll 2020 report commissioned by Microsoft

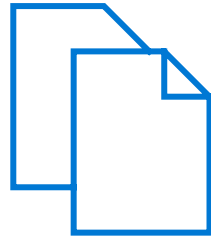


Intelligent compliance and risk management solutions



Information Protection & Governance

Protect and govern data wherever it lives



Insider Risk Management

Identify and take action on critical insider risks



Discover & Respond

Quickly investigate and respond with relevant data



Compliance Management

Simplify compliance and reduce risk

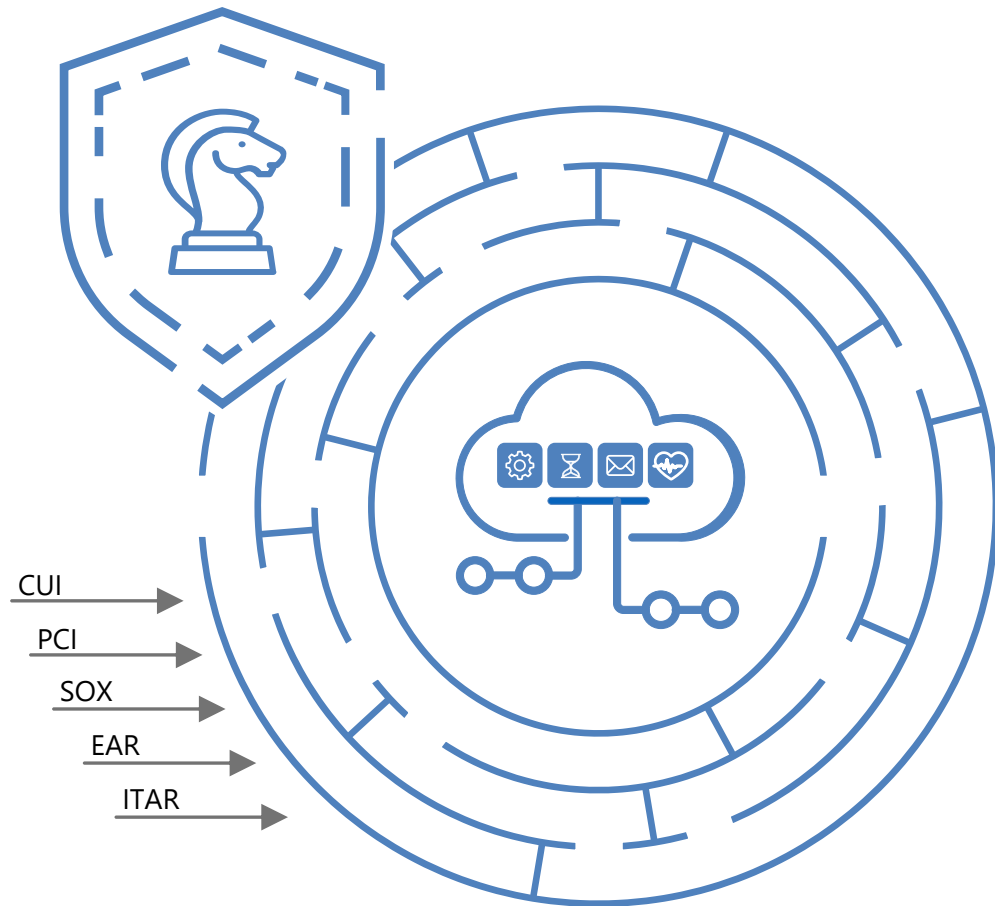


GTACS 2020
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY

ISACA
Singapore Chapter

CASE STUDY:

Security & Compliance Challenges



“



"Because Vodafone provides critical national infrastructure for millions of customers, it faces extensive security and compliance challenges. These challenges slowed the company's adoption of cloud services until it implemented Microsoft 365."

- James Elders-Rickard,
Security Architect, Global Cybersecurity Team
Vodafone

”



GTACS 2020
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY

ISACA
Singapore Chapter

What to look for in an information protection and governance solution?



Integrated
into user apps



Rich & Intelligent
classification



Extensible
to other systems



Unified
management



User-centered
balances security with
productivity

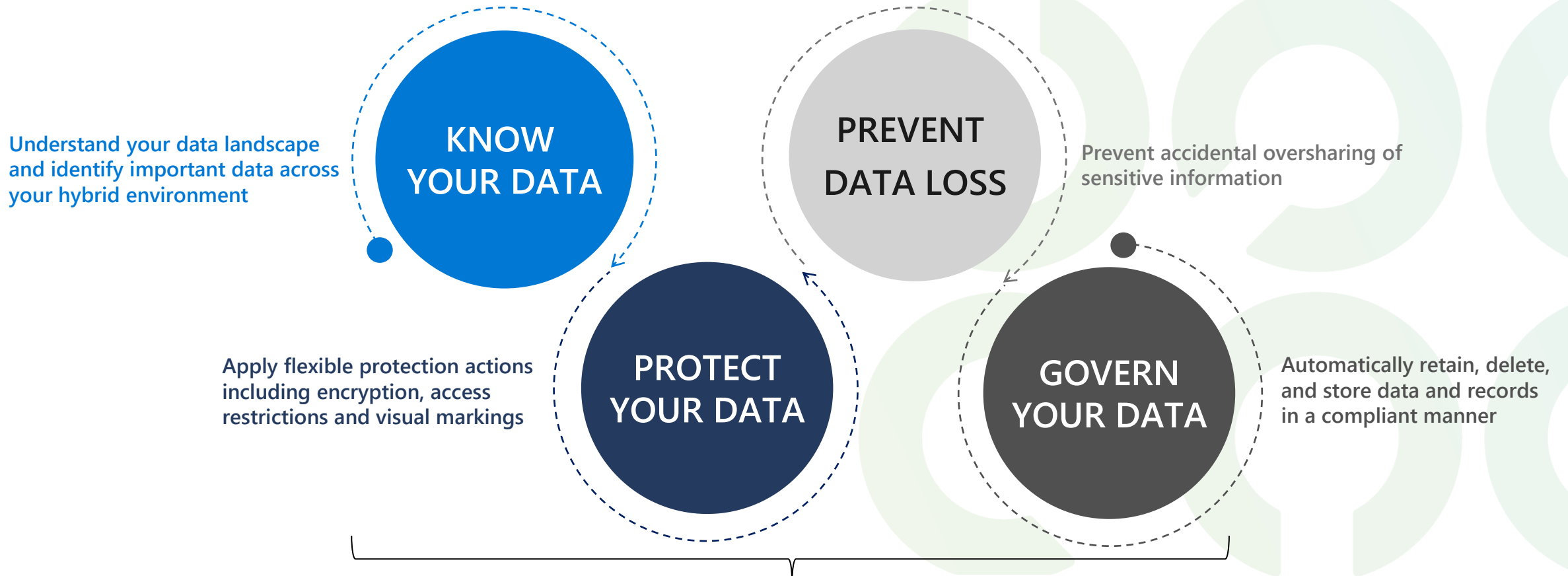


GTACS 2020
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY

ISACA
Singapore Chapter

Information protection & governance

Protect and govern data – **wherever** it lives



Powered by an intelligent platform

Unified approach to automatic data classification, policy management, analytics and APIs



GTACS 2020
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY

ISACA
Singapore Chapter

Information Protection & Governance

Comprehensive policies to protect and govern your most important data – throughout its lifecycle



Unified approach to discover, classify & label



Automatically apply policy-based actions



Proactive monitoring to identify risks



Broad coverage across locations and applications

Data growing at exponential rate



Unified approach



Discover



Classify



Label

Apply policy

Protection

- Encryption
- Restrict access
- Watermark
- Header/Footer



Governance

- Archiving
- Retention & deletion
- Records management
- Event based



Monitor

- Sensitive data discovery
- Data at risk
- Policy violations
- Label Analytics
- Proactive alerts
- Supervision



Devices



Apps



Cloud services



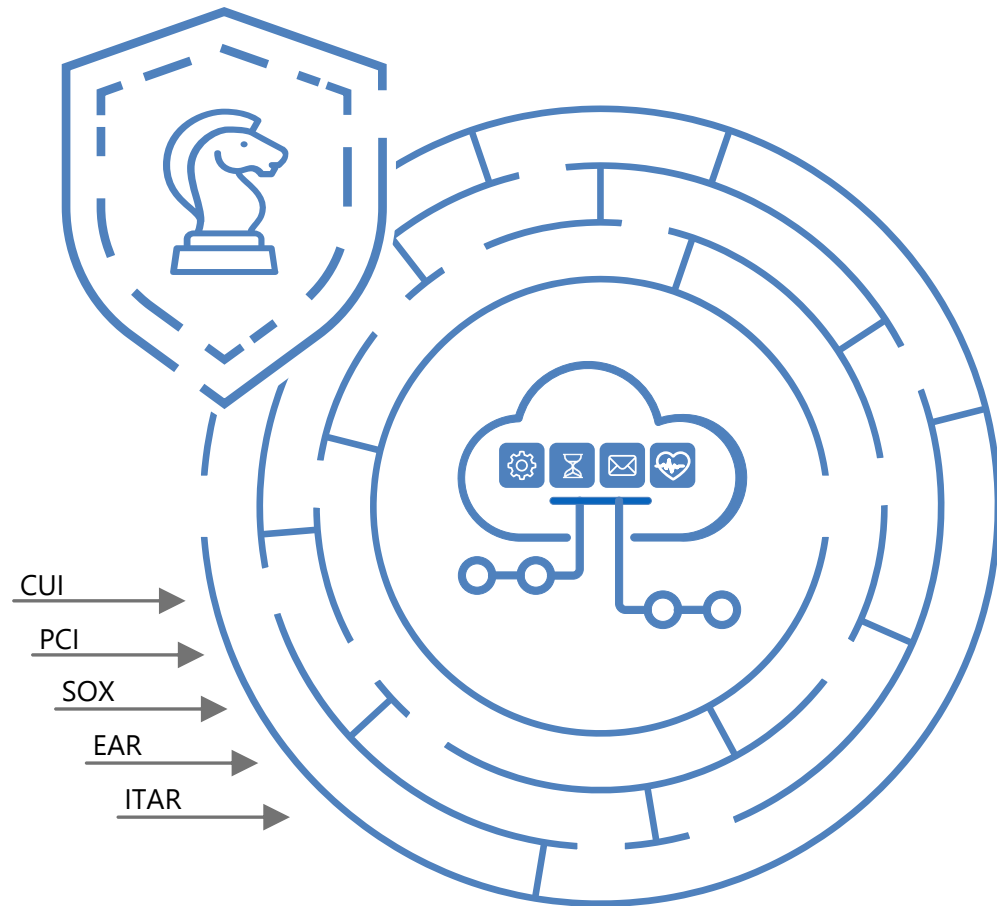
On-premises



ISVs, 3rd-party

CASE STUDY:

Risk & Privacy Management



“



"The simplest way to manage your risk is to minimize the amount of data that you store. Privacy assessments will help you know where the data is and how to protect it."

- Emma Smith, Global Security Director at Vodafone Group

Read the full blog [here](#):

”



GTACS 2020
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY

ISACA
Singapore Chapter

3 Recommendations balancing security with privacy compliance

Emma, Global Security Director at Vodafone Group



1. Develop a risk framework so you can prioritize your efforts.
2. Communicate regularly with the board and executive team to align on risk appetite.
3. Establish the right security capabilities internally and/or through a mix of partners and third parties.

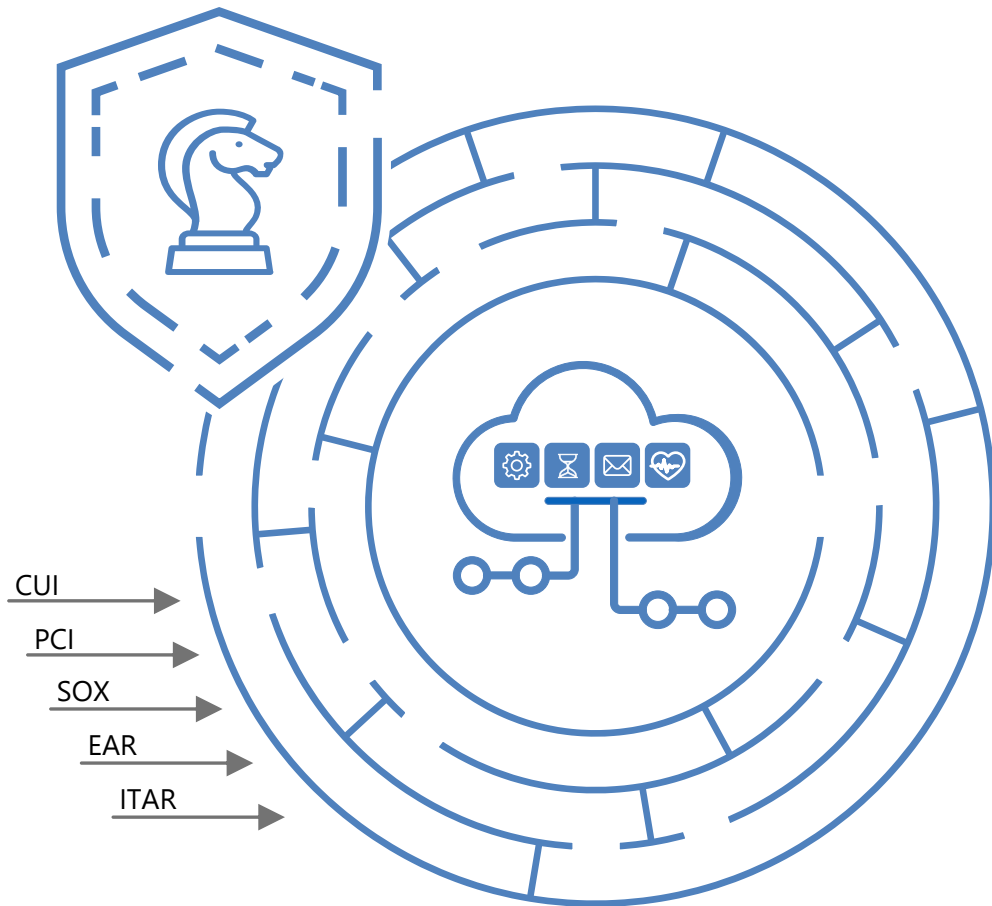


GTACS 2020
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY



CASE STUDY:

Protecting data across cloud services



“



"Microsoft Information Protection gave us the confidence we needed to put sensitive data in the cloud. The fact that the protection follows the file no matter where it resides means that we felt we'd reduced the risk to an acceptable level."

- James Elders-Rickard,
Security Architect, Global Cybersecurity Team
Vodafone

Read the full blog [here](#):

”

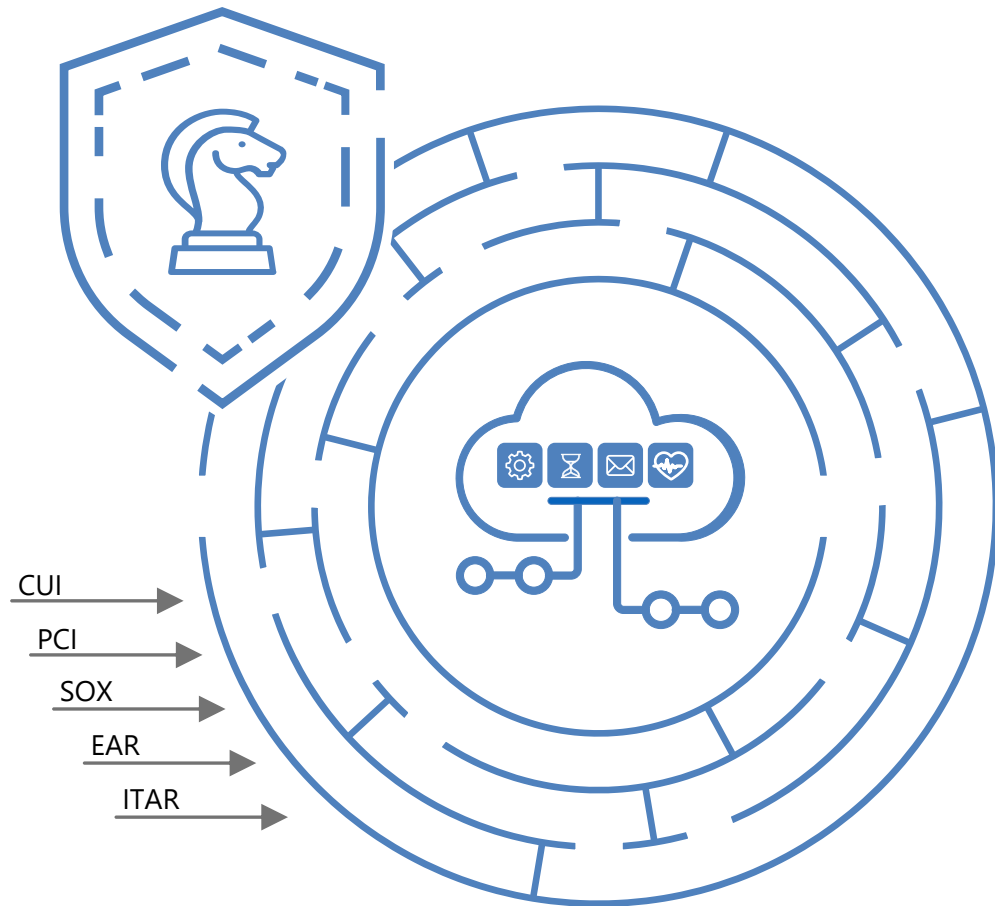


GTACS 2020
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY

ISACA
Singapore Chapter

CASE STUDY:

Stop data leaks and insider attacks



“



“With thousands of employees logging into a company’s systems every day, the threat of users — whether with inadvertent or malicious intent — may be a higher risk scenario. And that’s when we realized we needed to expand our focus.”

- Bret Arsenault,
Microsoft CVP & CISO

”



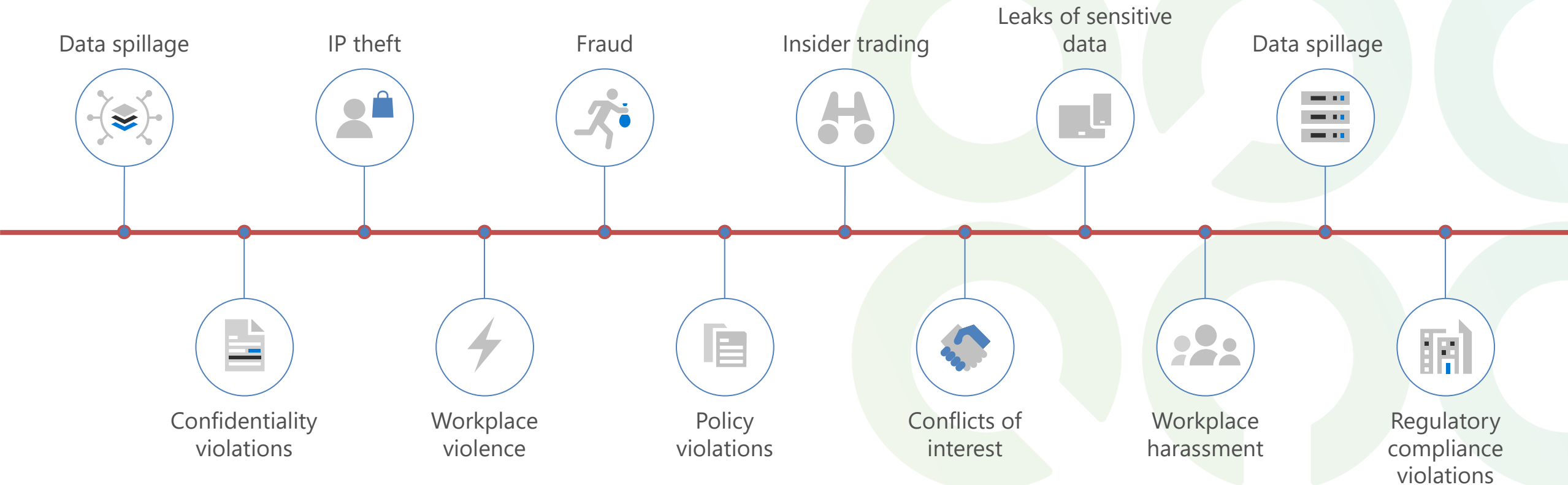
Read the full blog [here](#)

GTACS 2020
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY



ISACA
Singapore Chapter

Organizations face a broad range of risks from insiders



GTACS 2020
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY

ISACA
Singapore Chapter

Your customers have a fractured approach for insider risks



Insider risks are difficult to identify & manage

- Data growing, being accessed and shared across multiple devices and apps
- Visibility into location and movement of sensitive data is poor
- Requires analysis of millions of disparate signals and collaboration among security/HR/legal



Traditional approaches have limitations

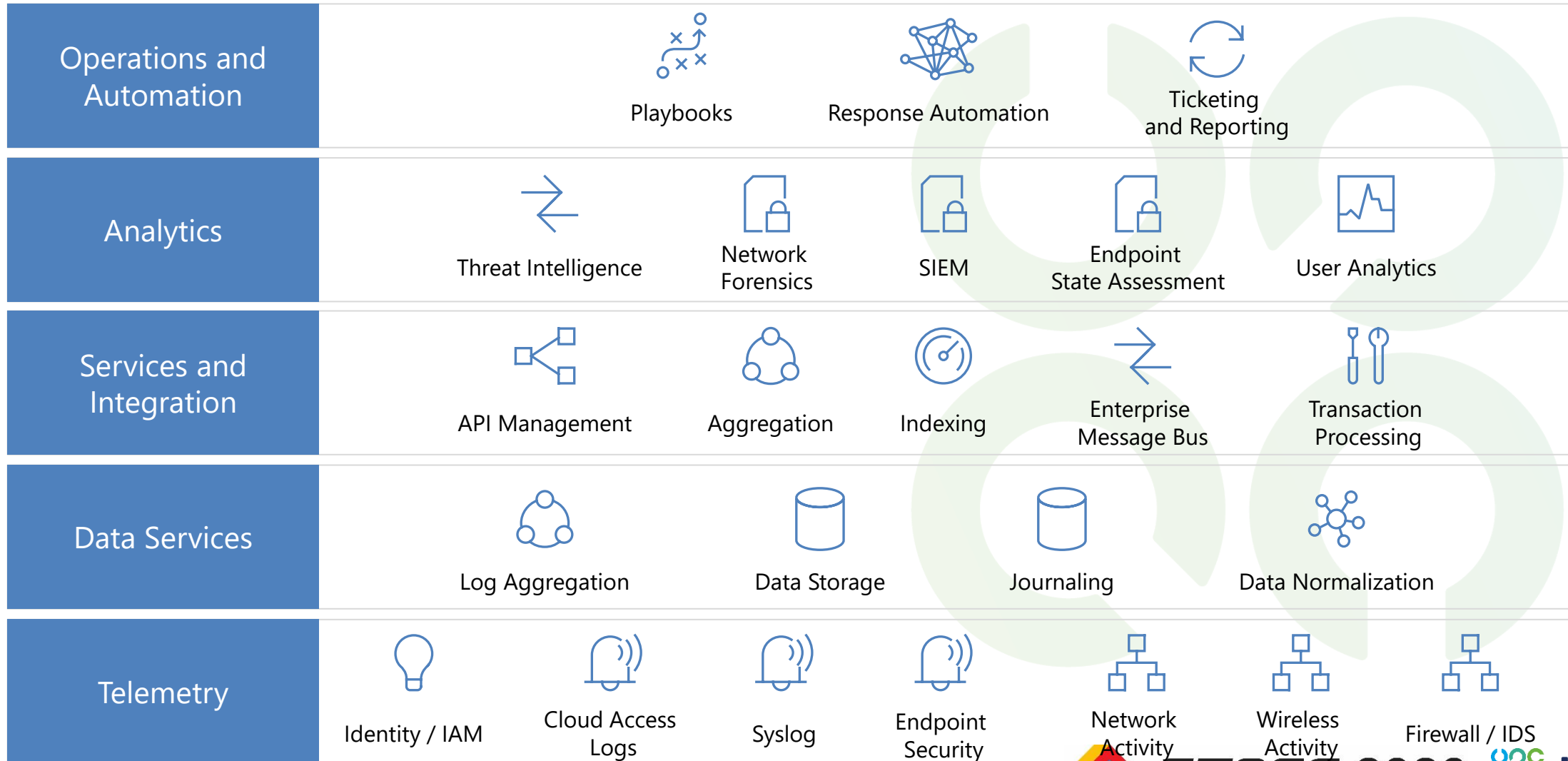
	UEBA (user behavior analytics)	UAM (user activity monitoring)	DLP (data loss prevention)
Complex setup	<ul style="list-style-type: none"> • Configuration requires scripting (engineering led or managed services) • Cost burden for storage of signals and compute for analytics • Signal curation requires additional solutions (Firewalls, UAM, DLP, EDR) • Events per second are capped • On-prem server-based model 	<ul style="list-style-type: none"> • Requires deployment of endpoint agents and on-prem servers • Management of agents is complex • Scale and performance issues with agent-based model 	<ul style="list-style-type: none"> • Requires deployment of endpoint agents and on-prem servers • Management of agents is complex • Scale and performance issues with agent-based model • Some narrowly focused on email communications
Limited enrichment	<ul style="list-style-type: none"> • Low visibility into content • Low sentiment analysis • Low understanding of content sensitivity 	<ul style="list-style-type: none"> • Low visibility into content • Low sentiment analysis • Limited signal correlation • Low understanding of content sensitivity 	<ul style="list-style-type: none"> • Low visibility into content • Low sentiment analysis • Limited signal correlation • Prone to high-false positive rate
Narrow workflows	<ul style="list-style-type: none"> • No integrated workflow beyond SOC 	<ul style="list-style-type: none"> • No integrated workflow beyond SOC 	<ul style="list-style-type: none"> • No integrated workflow beyond SOC



GTACS 2020
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY

ISACA
Singapore Chapter

Insider risk practice built on Microsoft overcomes a complicated landscape

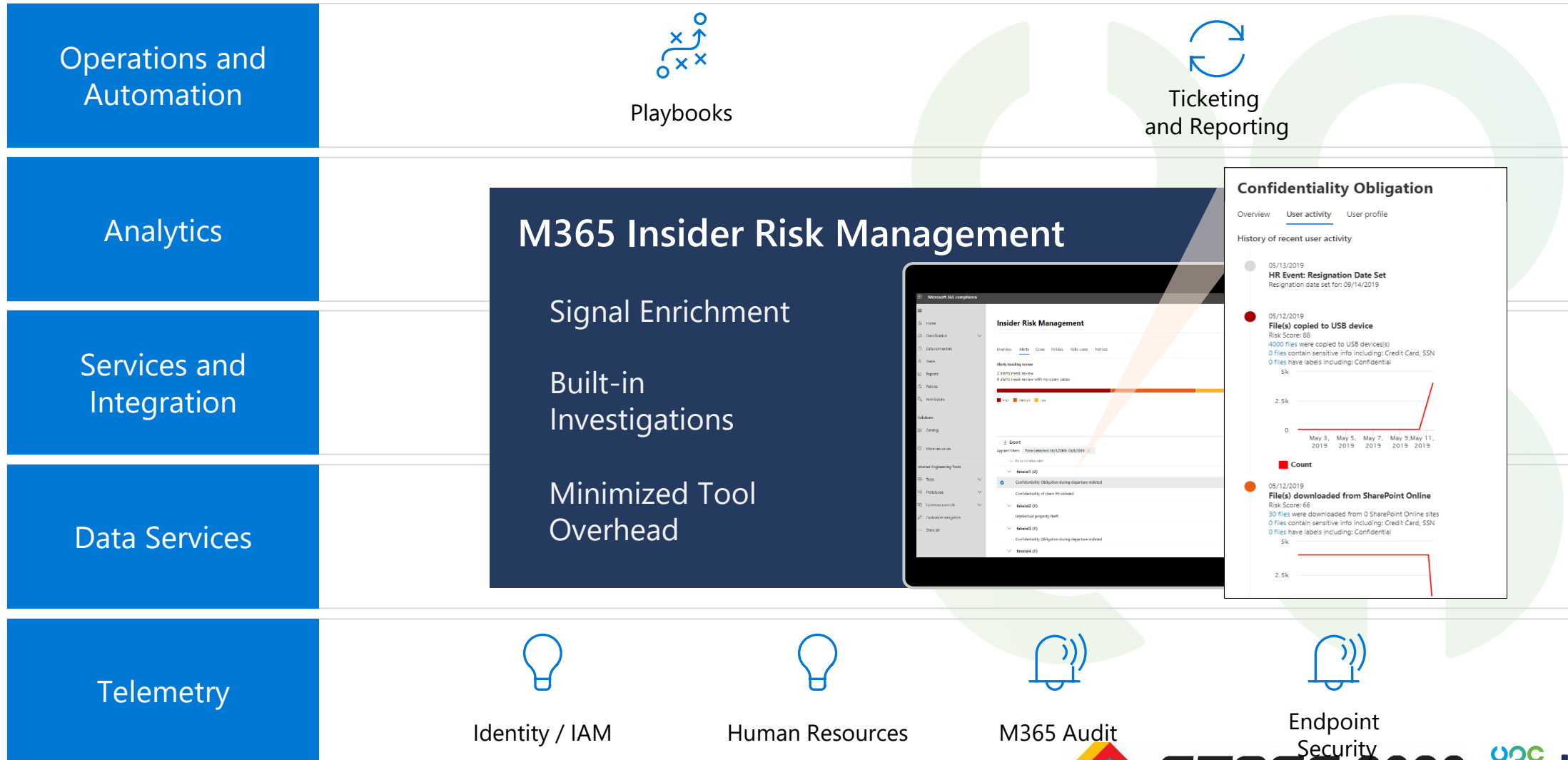


GTACS 2020
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY



ISACA
Singapore Chapter

Insider risk practice built on Microsoft overcomes a complicated landscape



GTACS 2020
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY





GTACS 2020

GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY



ISACA®

Singapore Chapter