歐盟《通用數據保障條例》生效一週年
談數據安全現代化

GDPR One Year On – Never Too Late To Modernize Your Data Protection

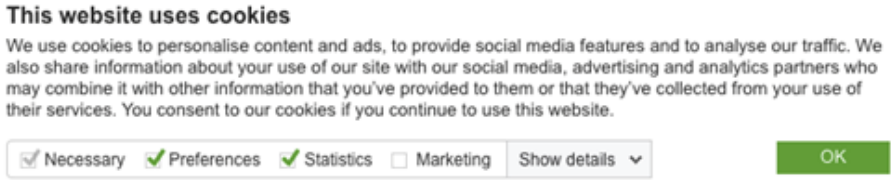
譚偉基
亞太區技術總監
wtam@forcepoint.com
linkedin.com/in/willitam/

FORCEPOINT

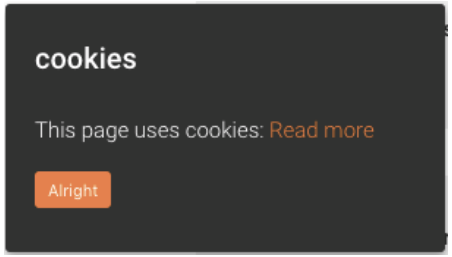
Data Protection | Web Security | CASB | NGFW | Advanced Malware Detection | Behavioral Analytics | Insider Threat | Email Security | Data Guard | Cross Domain

EU “The Cookie Law”

EU “The Cookie Law”



vs



Source : https://www.cookiebot.com/en/cookie-consent/

What is **GDPR** ?

What is GDPR ?

General Data Protection Regulation - regulation on data protection for personal data across the EU effective May 25th, 2018

What is it Important ?

The cost of compliance will be significant and cost of non-compliance even higher !

Am I affected ?

If you possess or manage data on an EU resident, then GDPR applies to your organization

Why should I care ?

Penalties of up to **4% of annual revenue** or **€20 million**, whichever is greater

Major Difference between GDPR and PDPO

	EU GDPR	Hong Kong PDPO
Application	Either in EU **or offer goods or services to; or monitor the behavior of individuals in EU**	Data users who process personal data in or from Hong Kong
Personal Data	**Any information relating** to an identifiable natural person, directly or indirectly, e.g. **location and online identifier**	Directly or indirectly to a living individual which can be ascertained
Accountability and Governance	• **Technical** and organizational measures • Data protection **by design** • Impact **assessment** on high risk processing • Designated **Data Protection Officer**	Not explicitly stated but privacy management programme and best practices are recommended

Reference : https://www.pcpd.org.hk/english/data_privacy_law/eu/files/eugdpr_e.pdf

Major Difference between GDPR and PDPO

	EU GDPR	Hong Kong PDPO
Sensitive Personal Data	**Special categories** (art9), e.g. racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, health data, sex life or sexual orientation	N/A
Consent	• **Opt-in** with unambiguous indication • Parental authorization below 16 or 13	• **Opt-out** • No parental consent required
Breach Notification	• Notify **the authority** of a data breach without undue delay • Notify **affected data subjects** if his/her rights and interests at risk	No mandatory requirement, but recommended

Reference : https://www.pcpd.org.hk/english/data_privacy_law/eu/files/eugdpr_e.pdf

Major Difference between GDPR and PDPO

	EU GDPR	Hong Kong PDPO
Data Processors	**Regulated**	Not directly regulated
New and Enhanced Rights for Data Subjects	Rights to be "**forgotten**", **notify/ restrict / object processing / profiling**,	Only rights to access, correction, longer than required retention, opt-out direct marketing activities
Cross- jurisdiction Data Transfer	**Certification and adherence** to approved codes of conduct are explicitly made one of the **legal bases for transfer**. [Art 46]	Certification and adherence to an approved code of practice are not explicitly made a legal basis. 6 conditions for exemption [s.33(2)(a-f)]
Sanctions	Administrative fines up **to €20 million or 4% of the total worldwide annual turnover**. (art83)	Penalties only after judicial process if failure to comply enforcement notices

Reference : https://www.pcpd.org.hk/english/data_privacy_law/eu/files/eugdpr_e.pdf

GDPR 1-Year Anniversary : Looking Back

- 90,000 breach notification across Europe
- 150 “headline” fines
  - Google’s **€50M** fine by France’s data protection watchdog is the highest recorded for its data consent policies
  - UK’s ICO fines British Airways a record **£183M** over GDPR breach that leaked data from 500,000 users
- Organizations spent an average of $1.3M* on their GDPR programs

*IAPP-EY Annual Privacy Governance Report 2018

How much does it cost ?

Transport

How much will Cathay Pacific be fined by UK regulator, given British Airways' record US$229 million penalty over similar data breach?

- Both airlines last year suffered major cyberattacks, with data of 9.4 million Cathay passengers affected, and half a million customers involved for British carrier
- BA was hit with a fine equivalent to 1.5 per cent of its revenue in 2017, and by same benchmark, Cathay could lose US$186.5 million

Danny Lee
Published: 10:00am, 9 Jul, 2019

Source : https://www.scmp.com/news/hong-kong/transport/article/3017763/how-much-will-hong-kongs-cathay-pacific-be-fined-regulator

How much does it **really** cost ?

Operating results analysis

	Six months ended 30th June		
	2019 HK$M	2018 HK$M	**Change HK$M**
Airlines' profit/(loss) before exceptional items	**966**	(844)	**+1,810**
Exceptional items*	**(59)**	101	**-160**
Taxation	**(292)**	(161)	**-131**
Airlines' profit/(loss) after taxation	**615**	(904)	**+1,519**
Share of profits from subsidiaries and associates	**732**	641	**+91**
Profit/(loss) attributable to the shareholders of Cathay Pacific	**1,347**	(263)	**+1,610**

* Exceptional items in 2019 include data security costs of HK$20 million and costs of HK$39 million associated with the acquisition of Hong Kong Express (2018: a HK$101 million gain on the disposal of CO_2 emissions credits).

so far.....

Source : https://www.cathaypacific.com/content/dam/cx/about-us/investor-relations/interim-annual-reports/en/2019_CX_Interim_Final_with_bookmarks_en.pdf

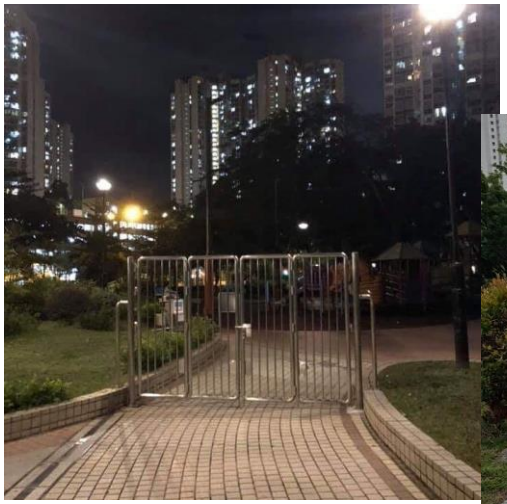
A global wave of data privacy laws

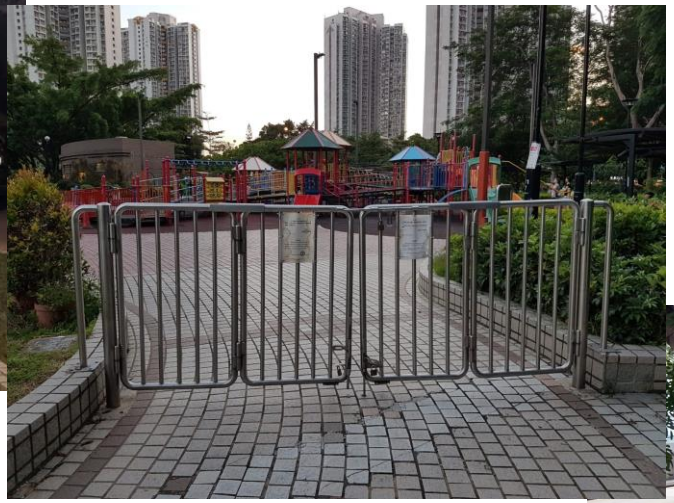
- Many non-EU countries have implemented GDPR-like laws
  - **Brazil** General Data Protection Law (LGPD) will be enforceable in Feb 2020
  - **Canadian** Personal Information Protection and Electronic Documents Act (PIPEDA)
  - **Japan's** Act on Protection of Personal Information was amended in May 2017
  - **Australia's** Privacy Amendment Act 2017
  - **China** national standard Personal Information Security Specification
  - **Facebook and Apple CEOs are lobbying for global GDPR-like laws**

Top GDPR Challenges – 1 Year Later

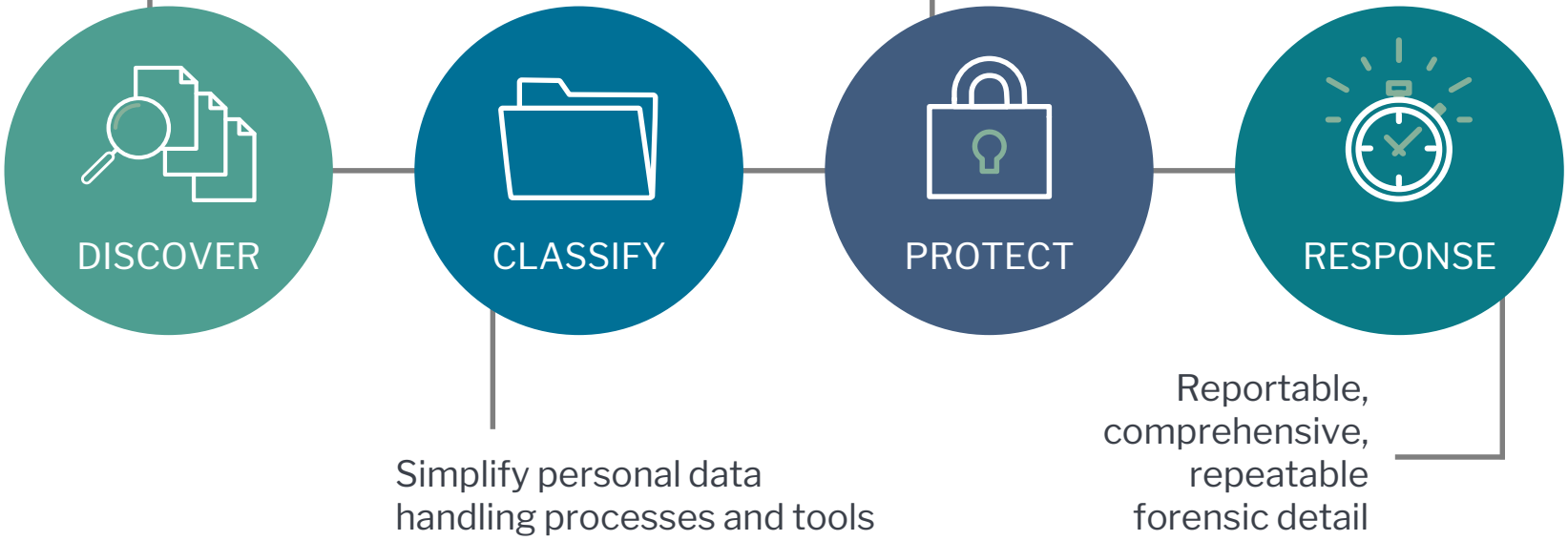
- **Data Subject Access Requests** (DSAR) are challenges for organizations and need **automation**
- **Big data**, filled with personal information, is a big challenge
  - Many organizations implemented over-compliance and **deleted too much data**
- There is an **existential threat** to organizations
  - **Lower spending** organizations treated GDPR as a **compliance exercise** while **higher spending** organizations tackled it as a **privacy exercise** and took a programmatic approach
  - Those that tackled GDPR as a compliance exercise over a privacy program are **at a higher risk**

What's wrong with a "Compliance Exercise" ?



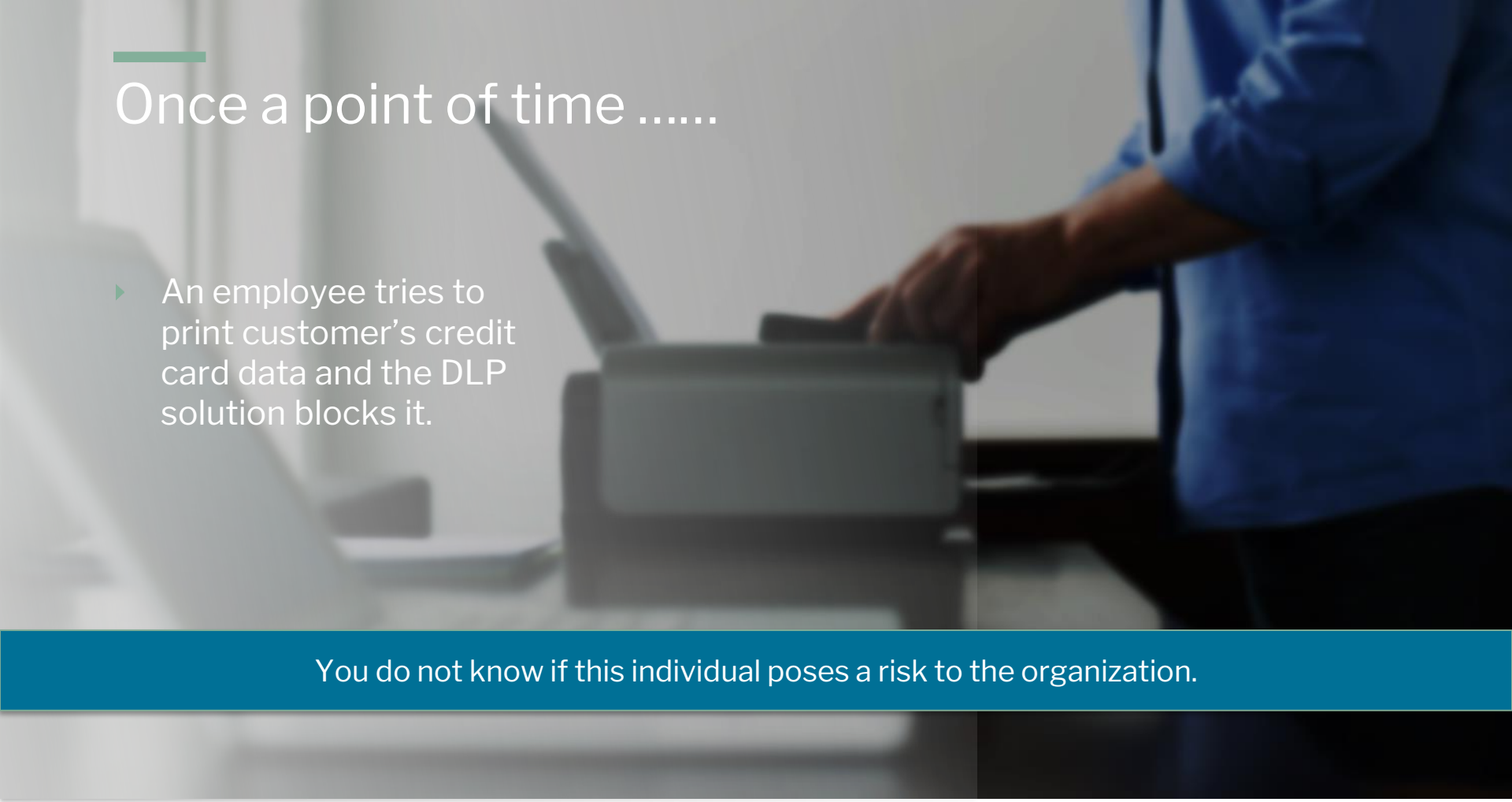


Standard Approach to GDPR or Any Data Protection



Once a point of time .....

- An employee tries to print customer's credit card data and the DLP solution blocks it.



You do not know if this individual poses a risk to the organization.

What If You Can Better Understand The Intent

What if your employee tries to print a customer's credit card data? DLP blocks it, but then he…

tries to copy the data to USB. DLP blocks it, but then he…

tries to upload it to Google Drive. CASB blocks it, but then he…

tries to upload it to Dropbox. CASB blocks it, but then he…

tries to send it to a personal email address. DLP blocks it, but then he…

tries to download to his mobile phone. DLP blocks it, but then he……

The behavior indicates this person is a risk, but your security team still does not know.

Once a point of time .....

User connect to a classified system

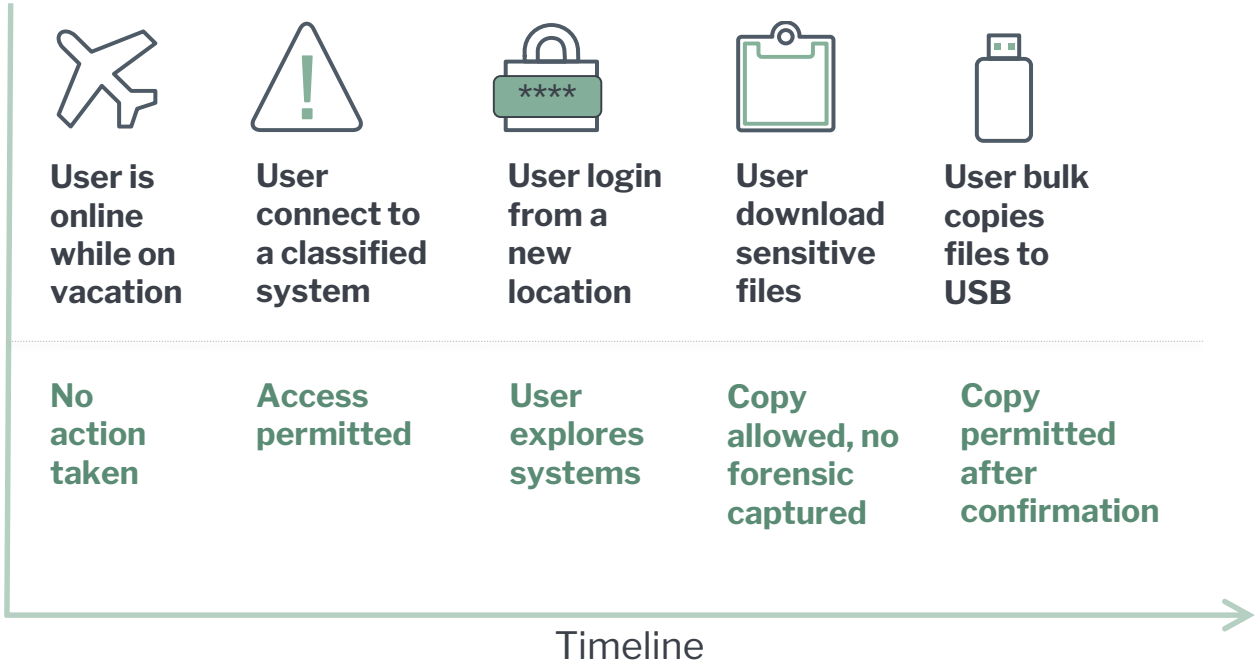
User is online while on vacation

User login from a new location

User download sensitive files

User bulk copies files to USB

What We Got Today – Just Another "Noisy" Day



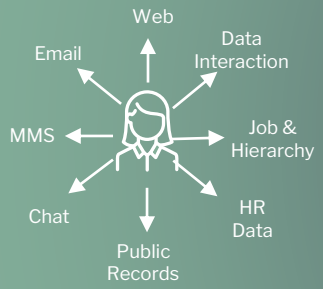
Forcepoint Critical Data and Intellectual Property Point of View

Embrace a risk-adaptive, dynamic approach to data protection

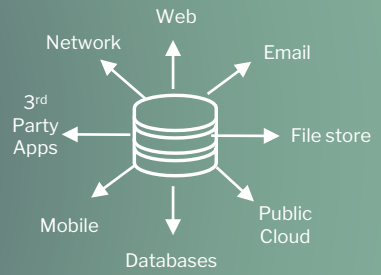
1 Analytics Driven Visibility

2 Risk-Adaptive Controls

3 Intelligent and Dynamic Automation



Delivered by Understanding Users and Data



1 Analytics driven visibility

Oversight everywhere users work and collaborate

Locate and understand the data

- Discover data at-rest, in-use, and in-motion across on-premises and cloud assets
- Data labeling and classification
- Structured and unstructured data

Identify your riskiest users

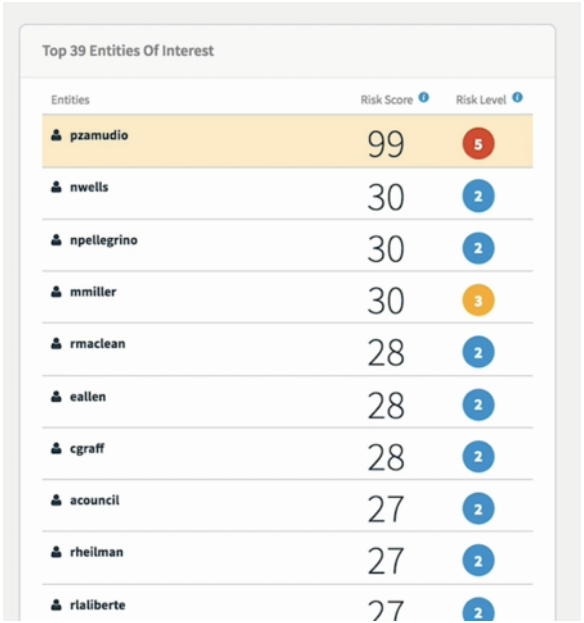
- Both security and non-security data sources
- Additional context derived through deep forensics
- Earlier identification of risky users

Gain insights by leveraging analytics

- Understanding behaviors to establish baseline
- Gaining contextual correlation
- Building an informed narrative

Analytics Sources

Prioritized list of risky users

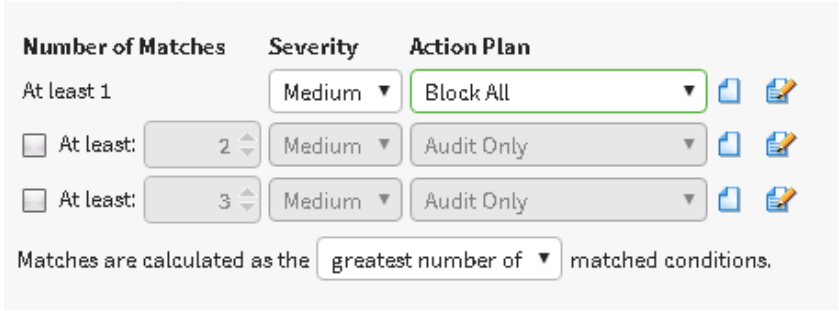


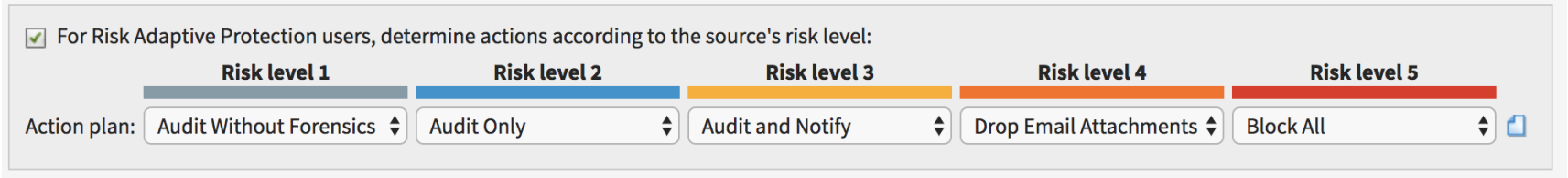
2

Risk-Adaptive Controls

Automated the response according to the risk level

- **Single, risk-adaptive policies**
  - Centralized policy management
  - Protection across multiple channels, including endpoint, network and cloud.
- **Individualized data protection**
  - User risk-aware policies
  - Allows for increased user productivity, improving security while reducing user frustration
- **Automated smart enforcement**
  - Surface anomalies, adjust individualized security controls
  - Dynamic, adaptive enforcement based on risk





3 Intelligent and Dynamic Automation

Building a better understanding of users to establish intent

Establish a repository of Adaptive Trust Profiles

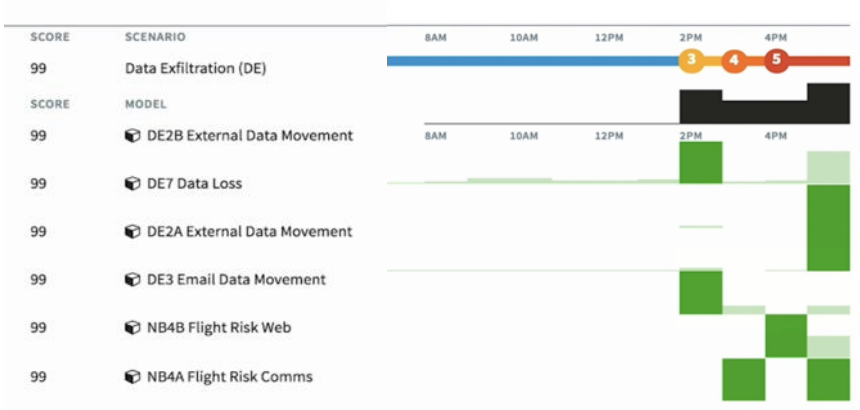
- Forcepoint has built a research division and invested in data scientists to build models to determine intent
- Understanding intent allows for graduated levels of monitoring and enforcement which can help aid investigations

Automate Intelligent Response

- The security team is alerted to the risky behavior while the policies protect the data
- The SOC moves from alert coordination to case prosecution

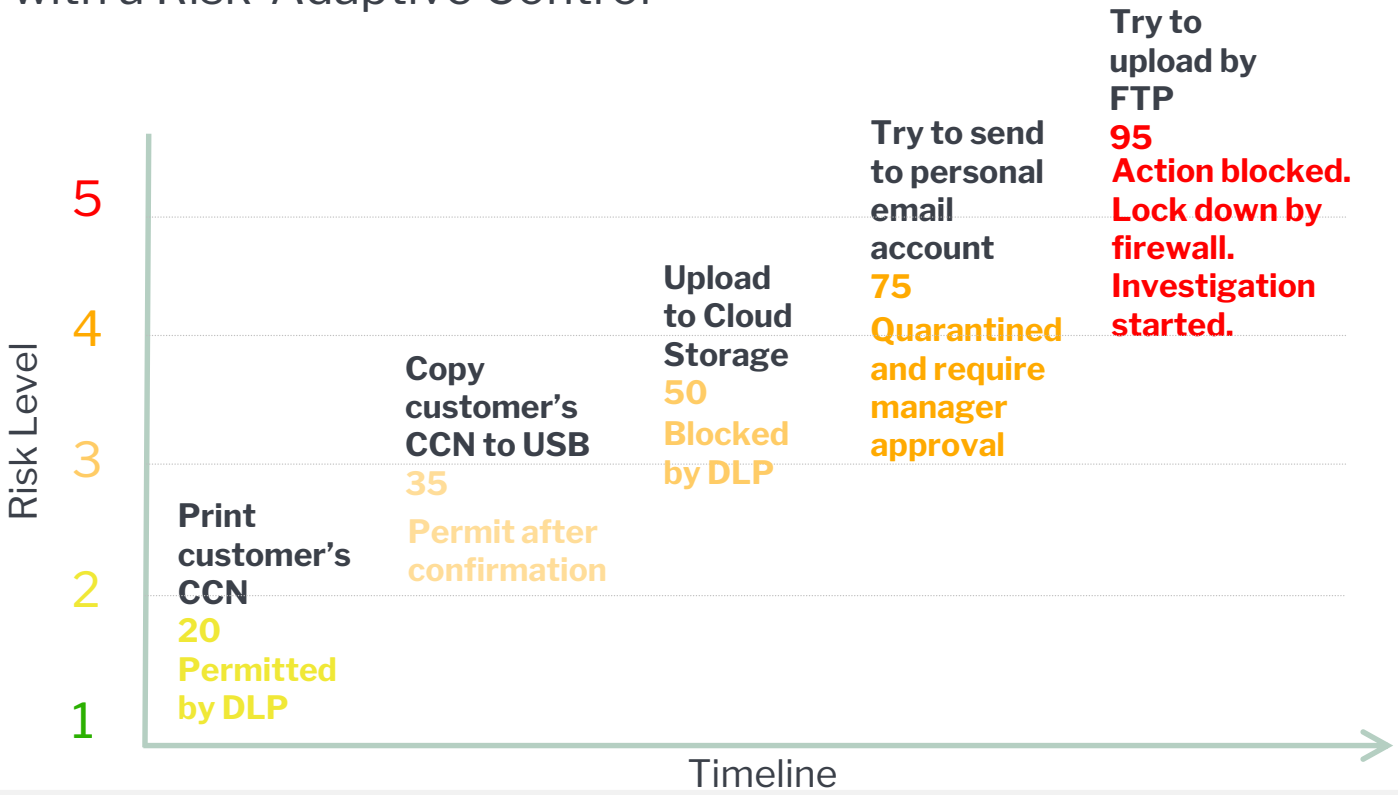
Move from "what happened?" to a more prescriptive posture

- By understanding behaviors and intent, we can graduate enforcement to accompany varying levels of risk
- Combining inferences and observables with enforcement allows for proactive identification and remediation against potential risk



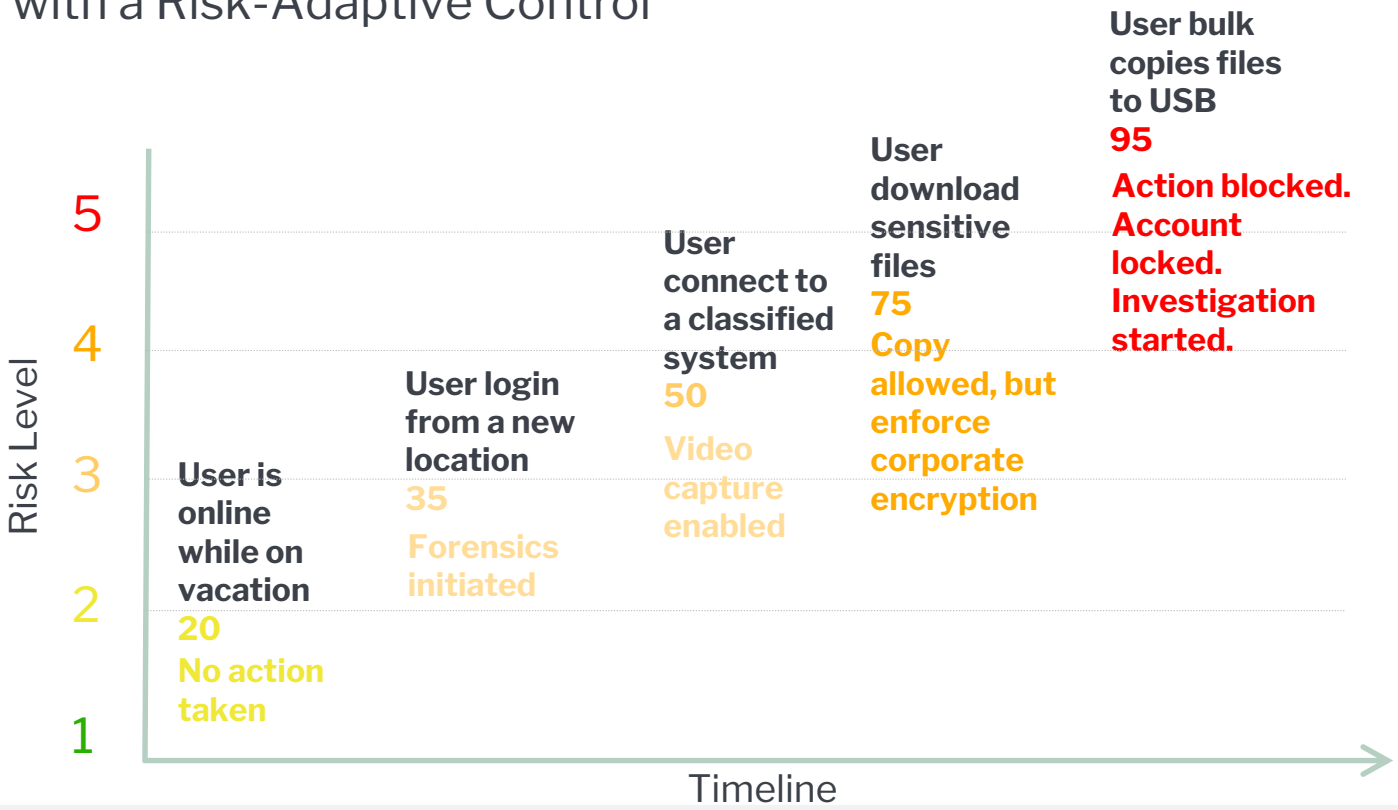
Now again, when someone trying to print .....

with a Risk-Adaptive Control



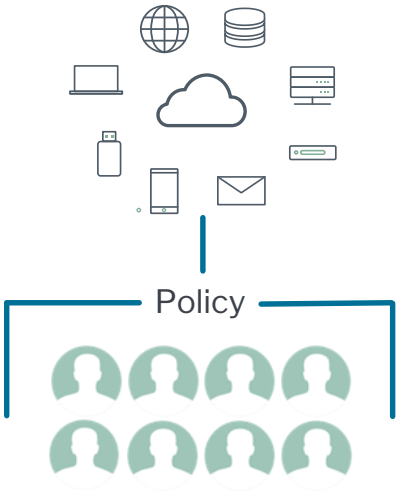
Now again, when someone on vacation .....

with a Risk-Adaptive Control



Modernization of Data Protection

From Traditional Security

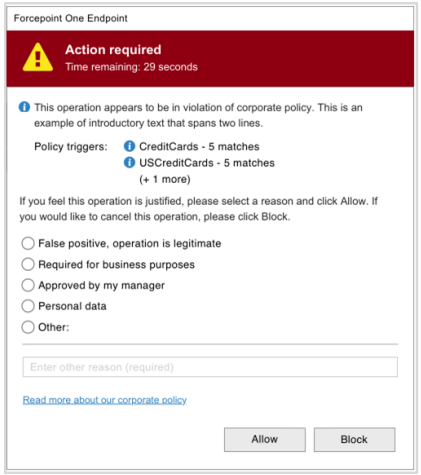


One-to-many enforcement of static, generic policies, producing high false positive rates.

To **Human-Centric Security**

One-to-one enforcement of different policies based on the risk, enabling automation.

And Capable of Handling Exceptions



Even the most individualized policies can require exemptions

Key Takeaways

- **GDPR is not over**… it's part of doing business and a continual process
- GDPR is a privacy effort – **not just compliance**
- Organizations must look for **automation** and **modernization** of their data protection strategy

THANK YOU !