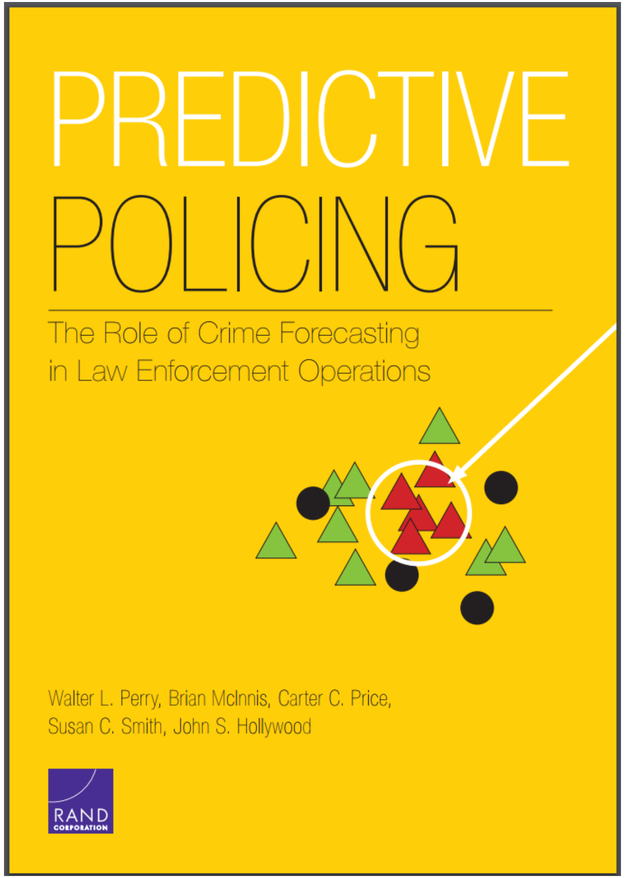
Introducing Risk-Adaptive Protection

Carl Leonard
Principal Security Analyst

Copyright © 2018 Forcepoint.

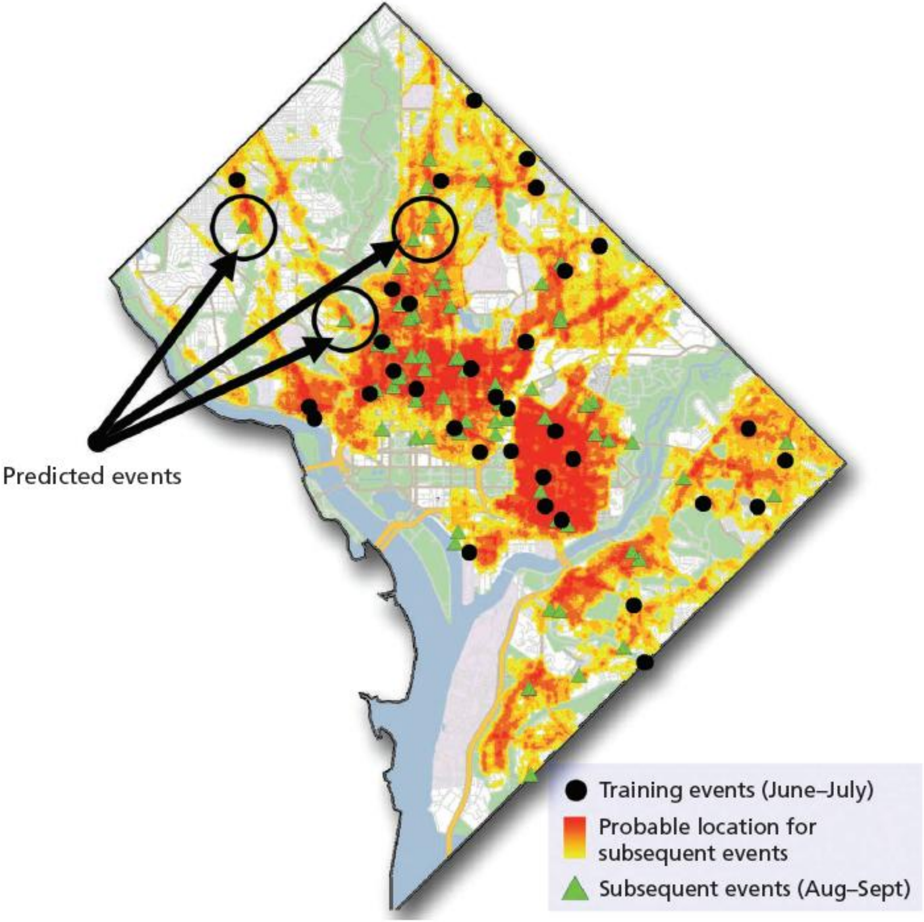


PREDICTIVE POLICING

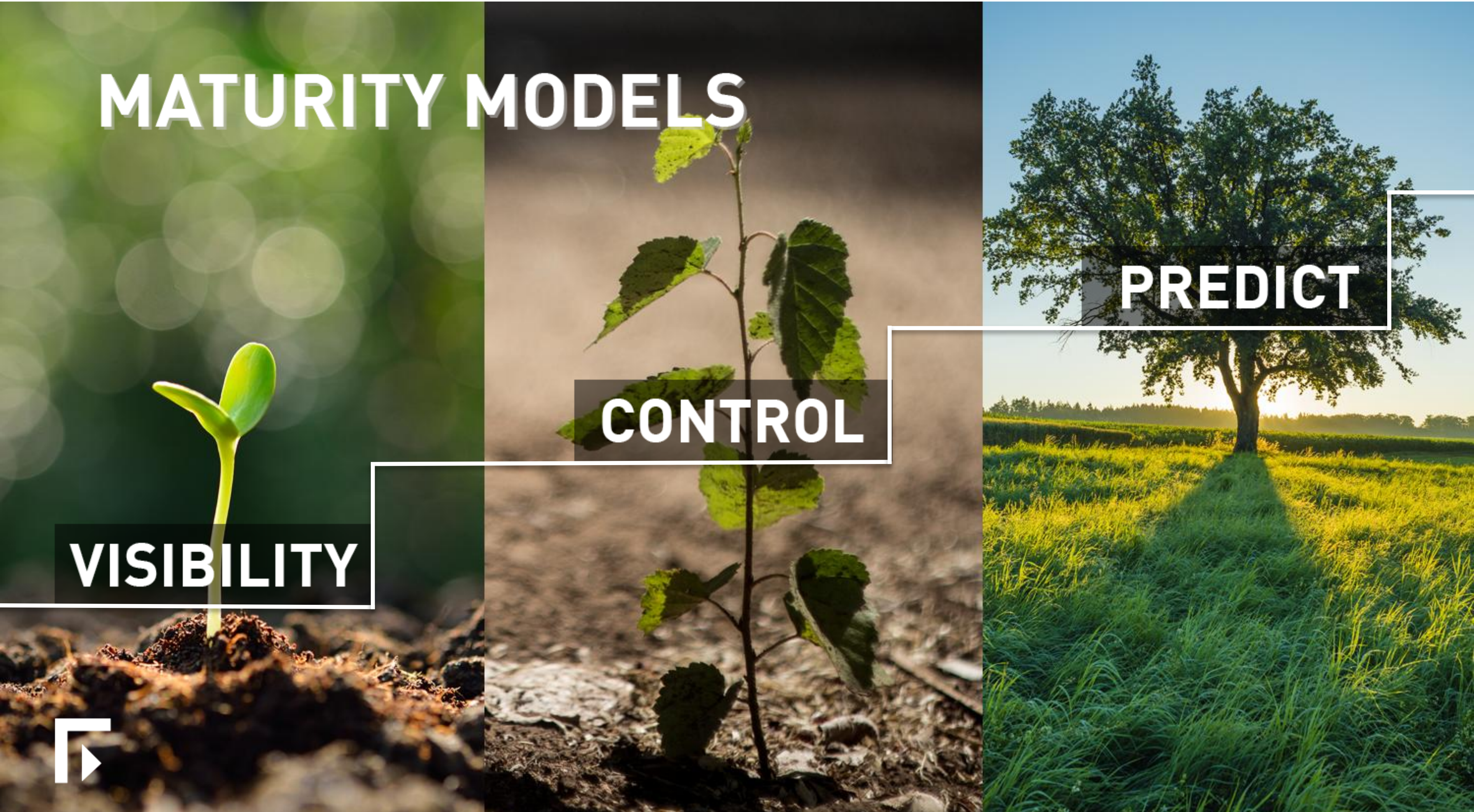
The Role of Crime Forecasting in Law Enforcement Operations

Walter L. Perry, Brian McInnis, Carter C. Price,
Susan C. Smith, John S. Hollywood

RAND
CORPORATION


Predicted events
● Training events (June–July)
🟥 Probable location for subsequent events
▲ Subsequent events (Aug–Sept)

MATURITY MODELS

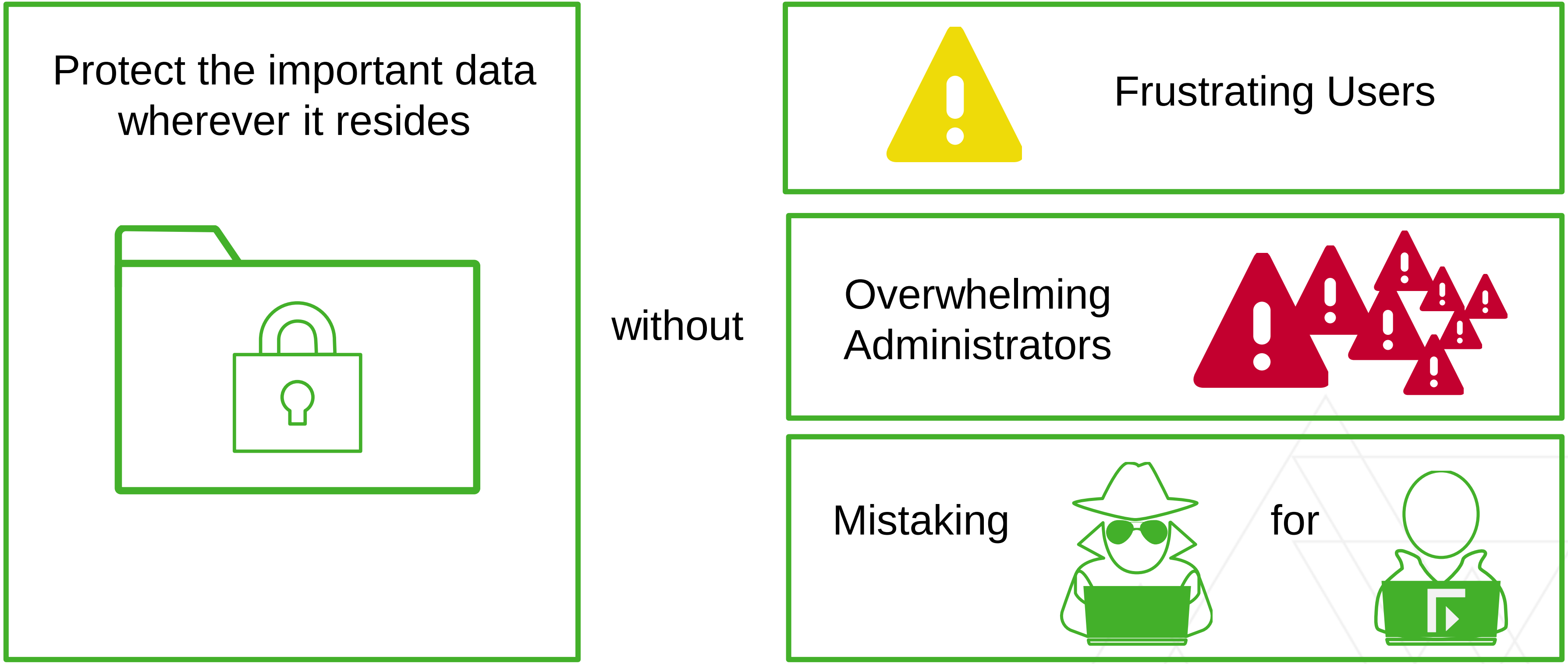


VISIBILITY

CONTROL

PREDICT

CURRENT MISSION FOR MODERN SECURITY ORGANISATIONS



Protect the important data wherever it resides

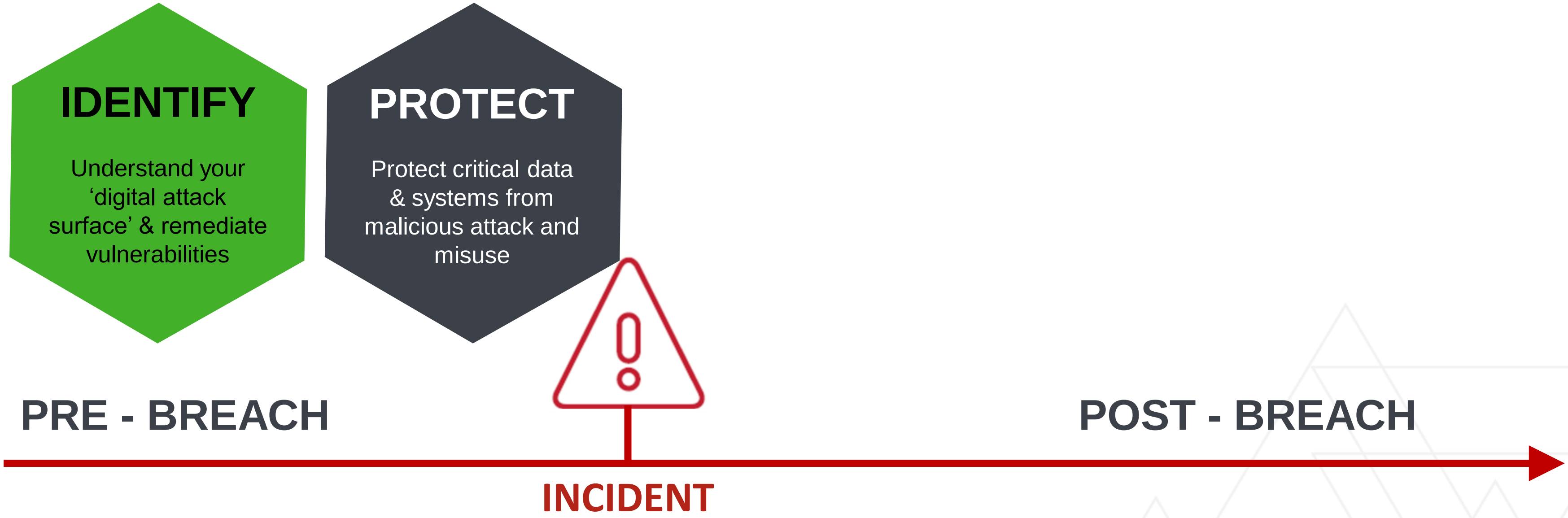
without

Frustrating Users

Overwhelming Administrators

Mistaking for

TODAY’S SECURITY APPROACH – DEFEND AS MUCH AS POSSIBLE!



IDENTIFY

Understand your ‘digital attack surface’ & remediate vulnerabilities

PROTECT

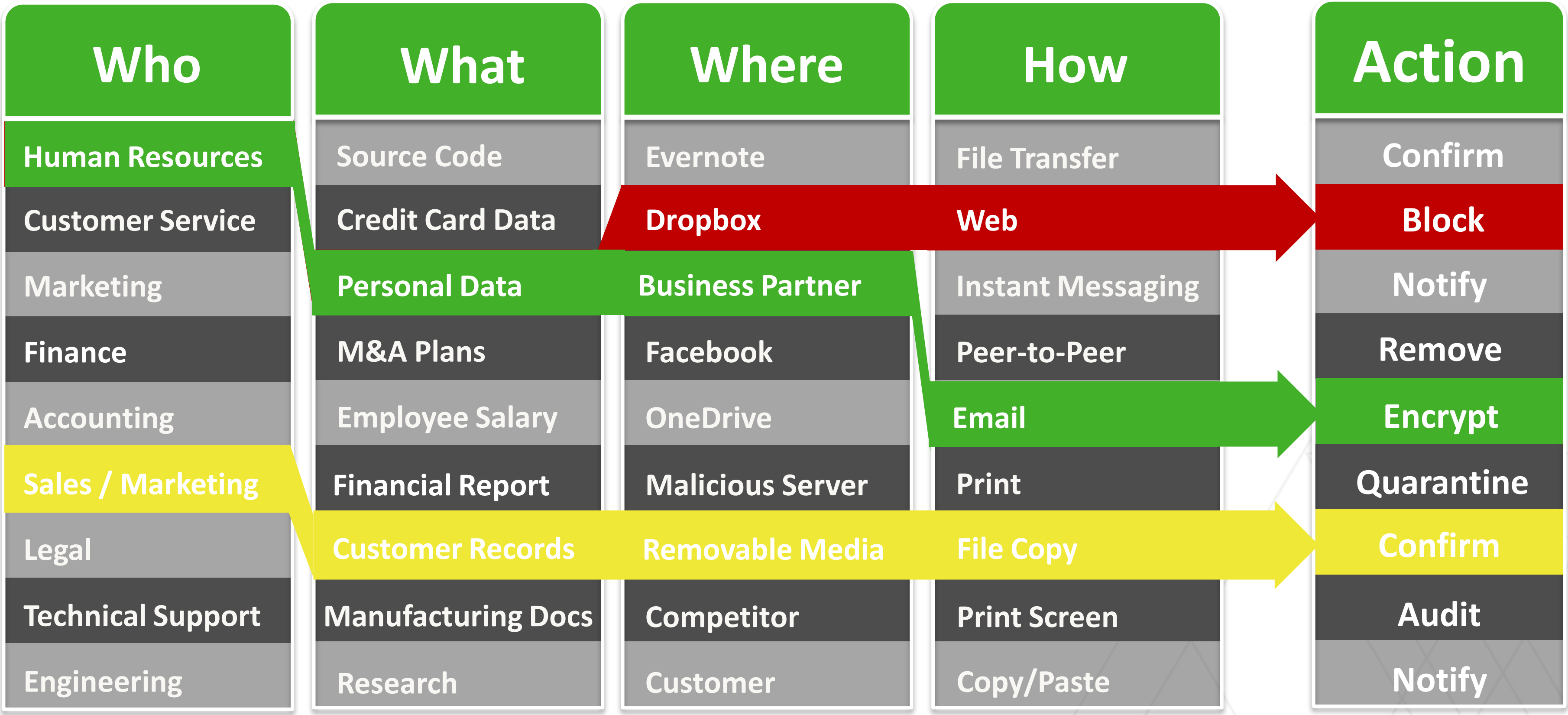
Protect critical data & systems from malicious attack and misuse

PRE - BREACH

INCIDENT

POST - BREACH

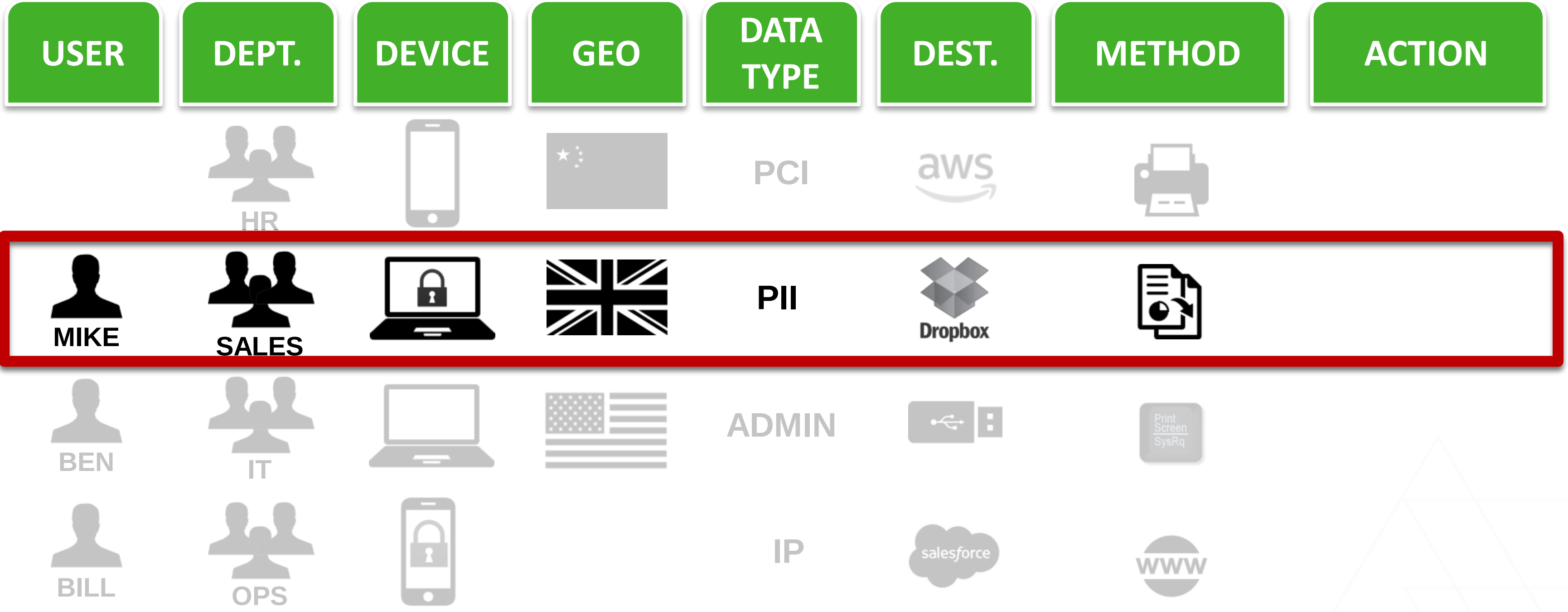
HOW DO YOU MANAGE AND CONTROL DATA WHEN IT’S IN USE & IN MOTION?



Who	What	Where	How	Action
Human Resources	Source Code	Evernote	File Transfer	Confirm
Customer Service	Credit Card Data	Dropbox	Web	Block
Marketing	Personal Data	Business Partner	Instant Messaging	Notify
Finance	M&A Plans	Facebook	Peer-to-Peer	Remove
Accounting	Employee Salary	OneDrive	Email	Encrypt
Sales / Marketing	Financial Report	Malicious Server	Print	Quarantine
Legal	Customer Records	Removable Media	File Copy	Confirm
Technical Support	Manufacturing Docs	Competitor	Print Screen	Audit
Engineering	Research	Customer	Copy/Paste	Notify

Copyright © 2018 Forcepoint. |

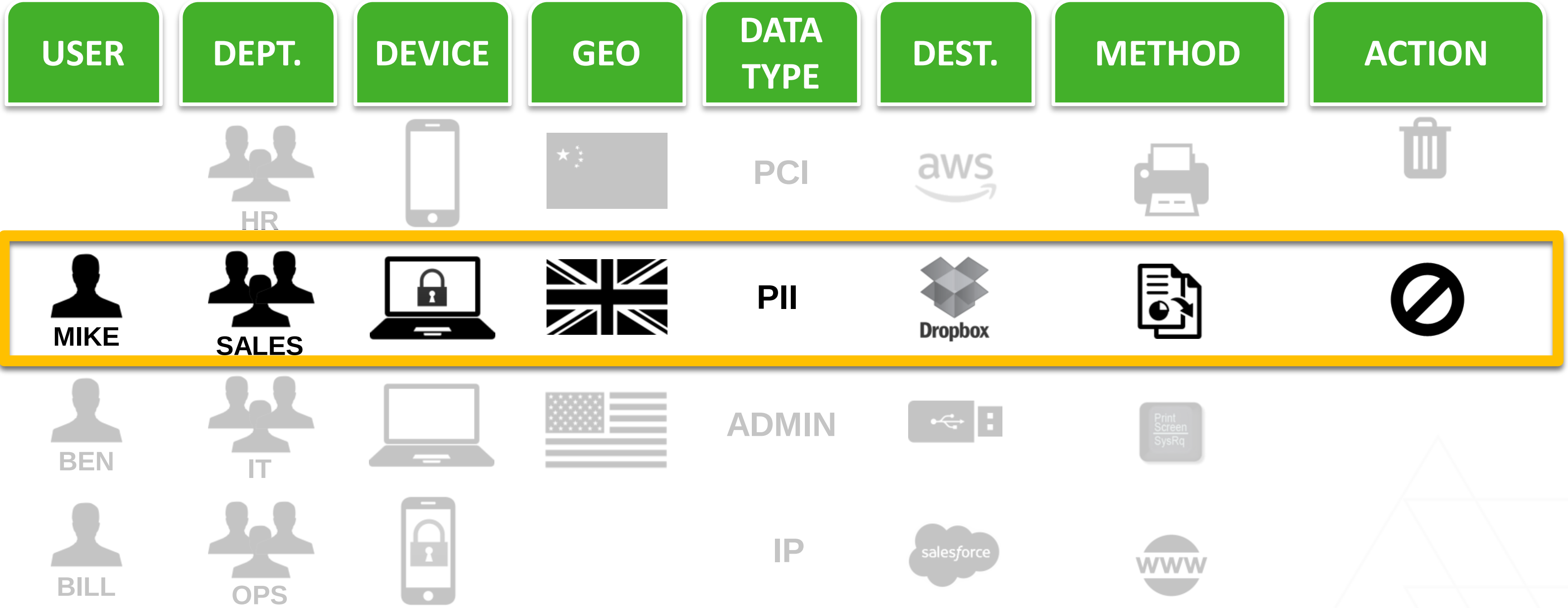
TODAY'S SECURITY APPROACH



USER	DEPT.	DEVICE	GEO	DATA TYPE	DEST.	METHOD	ACTION
	HR			PCI	aws		
MIKE	SALES			PII	Dropbox		
BEN	IT			ADMIN		Print Screen SysRq	
BILL	OPS			IP	salesforce	www	

Copyright © 2018 Forcepoint

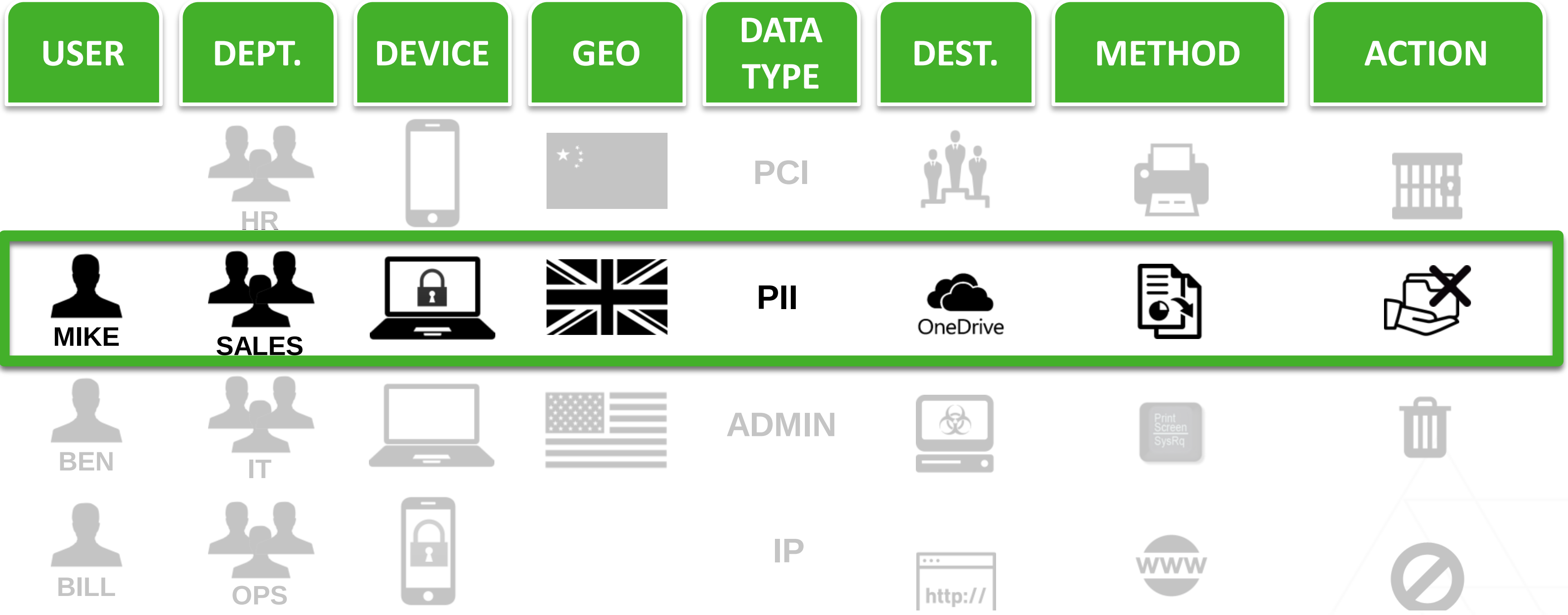
TODAY'S SECURITY APPROACH



USER	DEPT.	DEVICE	GEO	DATA TYPE	DEST.	METHOD	ACTION
	HR			PCI	aws		
MIKE	SALES			PII	Dropbox		
BEN	IT			ADMIN		Print Screen SysRq	
BILL	OPS			IP	salesforce	www	

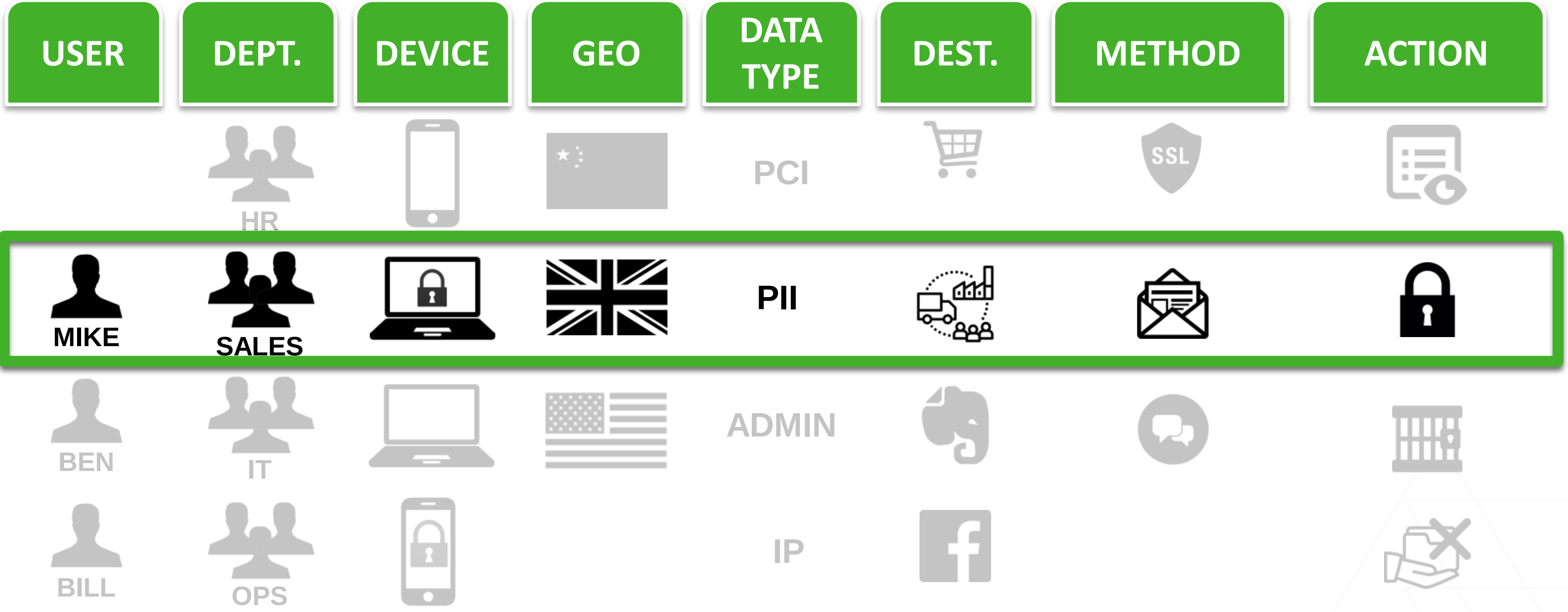
Copyright © 2018 Forcepoint

TODAY'S SECURITY APPROACH



USER	DEPT.	DEVICE	GEO	DATA TYPE	DEST.	METHOD	ACTION
	HR			PCI			
MIKE	SALES			PII	OneDrive		
BEN	IT			ADMIN		Print Screen SysRq	
BILL	OPS			IP	http://	WWW	

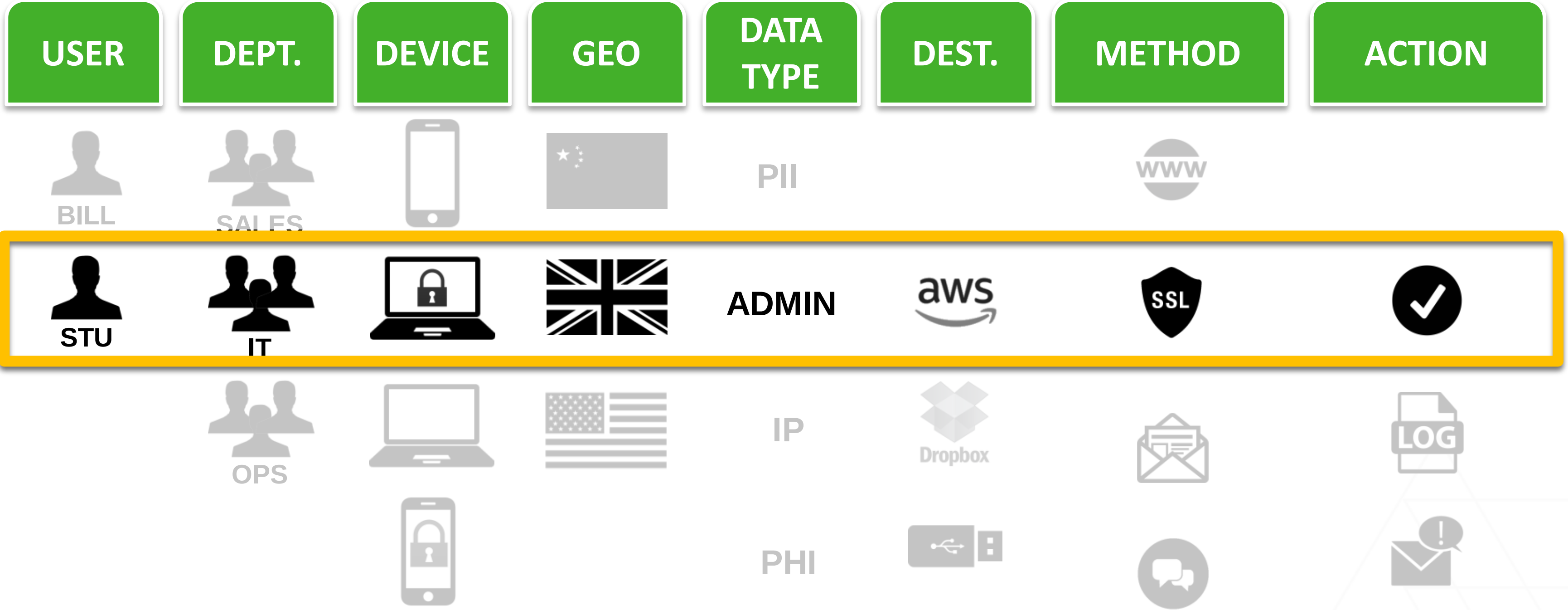
TODAY'S SECURITY APPROACH



USER	DEPT.	DEVICE	GEO	DATA TYPE	DEST.	METHOD	ACTION
	HR			PCI			
MIKE	SALES			PII			
BEN	IT			ADMIN			
BILL	OPS			IP			

Copyright © 2018 Forcepoint

TODAY’S SECURITY APPROACH



USER

DEPT.

DEVICE

GEO

DATA TYPE

DEST.

METHOD

ACTION

BILL

SALES

PII

STU

IT

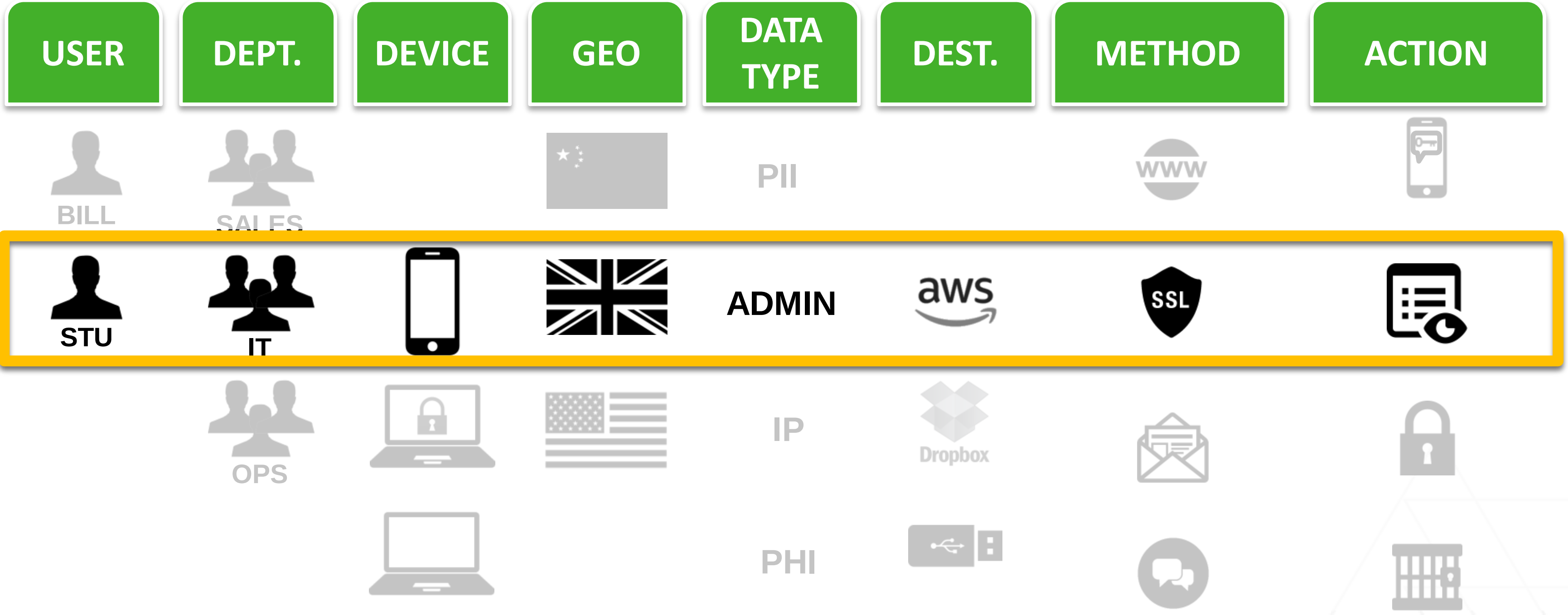
ADMIN

OPS

IP

PHI

TODAY’S SECURITY APPROACH



USER

DEPT.

DEVICE

GEO

DATA TYPE

DEST.

METHOD

ACTION

BILL

SALES

PII

STU

IT

ADMIN

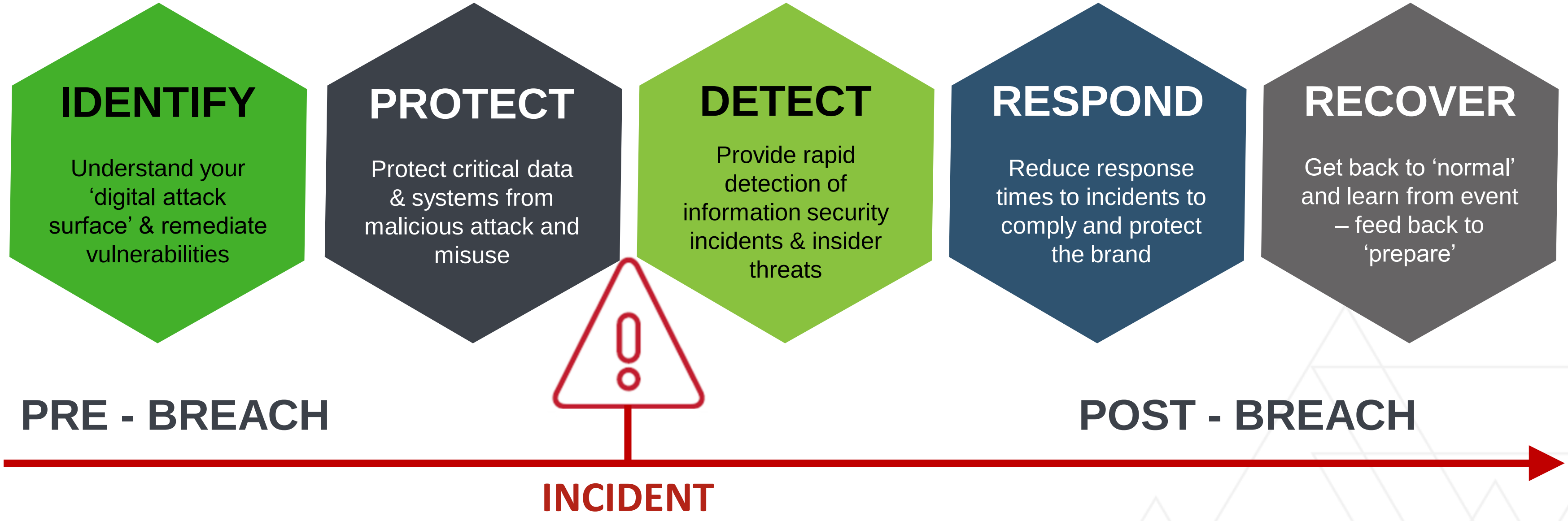
OPS

IP

PHI

Copyright © 2018 Forcepoint

POST-EVENT DETECTION WITH BEHAVIOURAL ANALYTICS



IDENTIFY

Understand your 'digital attack surface' & remediate vulnerabilities

PROTECT

Protect critical data & systems from malicious attack and misuse

DETECT

Provide rapid detection of information security incidents & insider threats

RESPOND

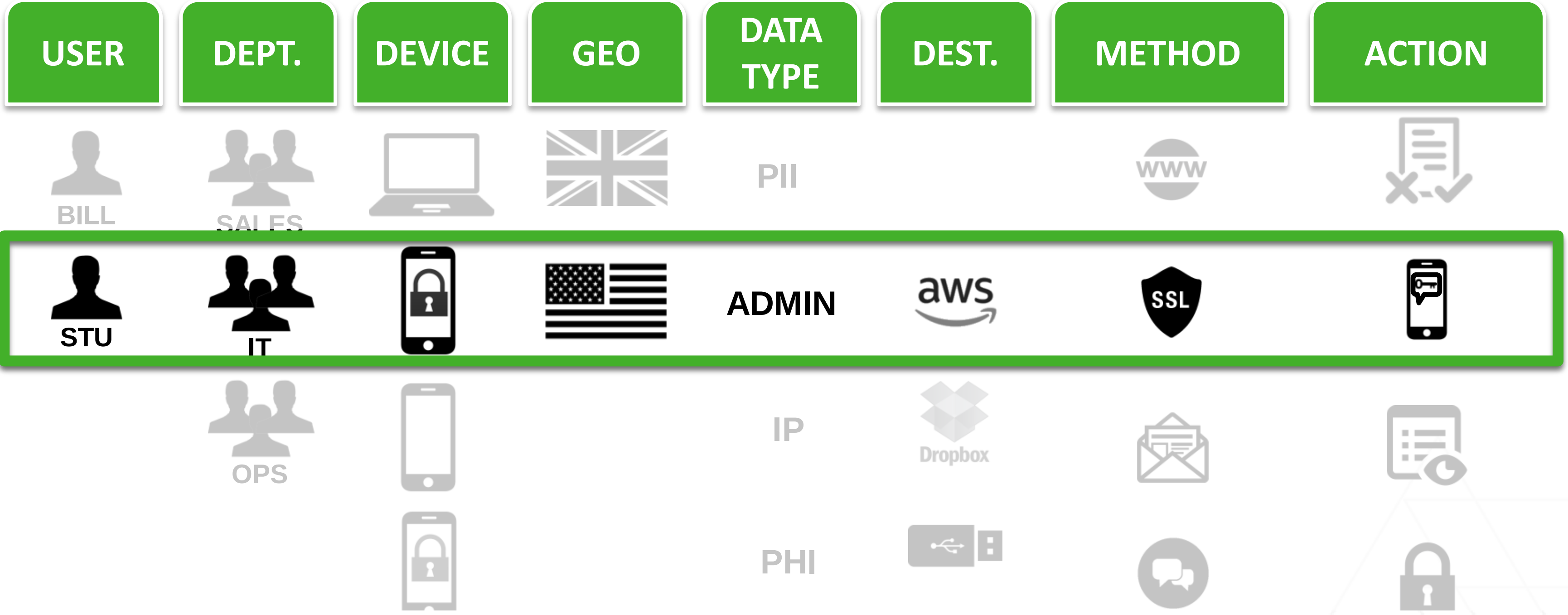
Reduce response times to incidents to comply and protect the brand

RECOVER

Get back to 'normal' and learn from event – feed back to 'prepare'

Copyright © 2018 Forcepoint.

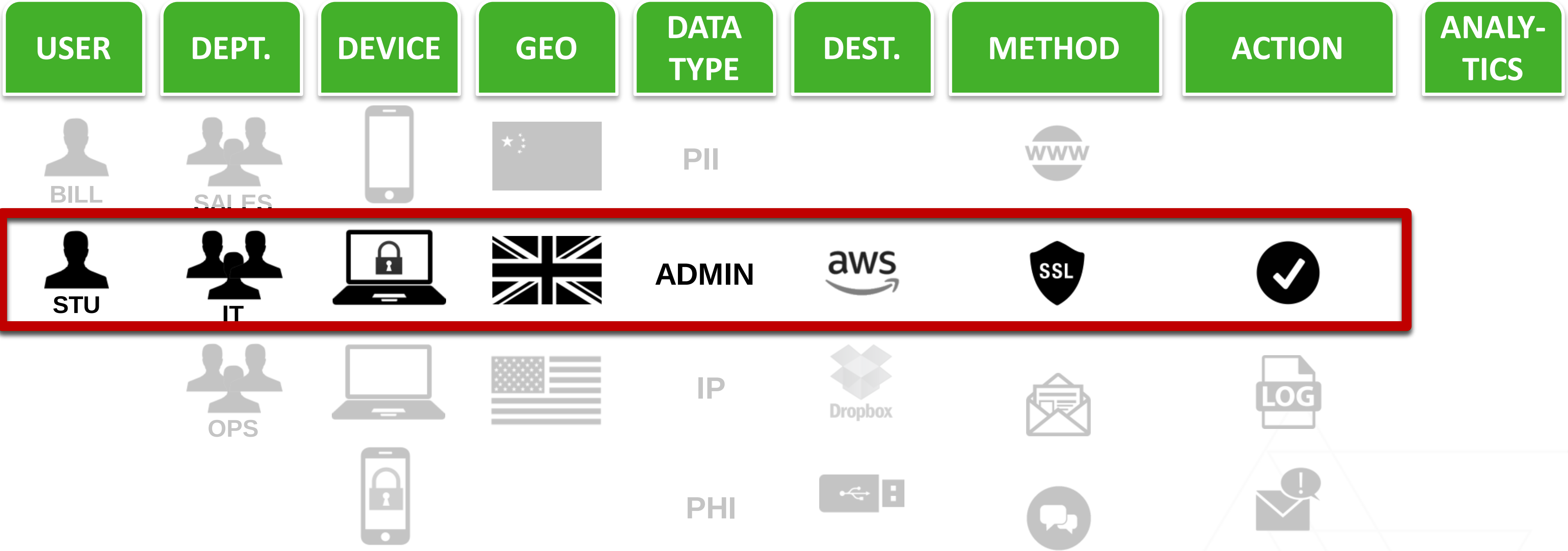
POST-EVENT DETECTION WITH BEHAVIOURAL ANALYTICS



USER	DEPT.	DEVICE	GEO	DATA TYPE	DEST.	METHOD	ACTION
BILL	SALES			PII		WWW	
STU	IT			ADMIN	aws	SSL	
	OPS			IP	Dropbox		
				PHI			

Copyright © 2018 Forcepoint

POST-EVENT DETECTION WITH BEHAVIOURAL ANALYTICS



USER | DEPT. | DEVICE | GEO | DATA TYPE | DEST. | METHOD | ACTION | ANALY-TICS

BILL | SALES | PII

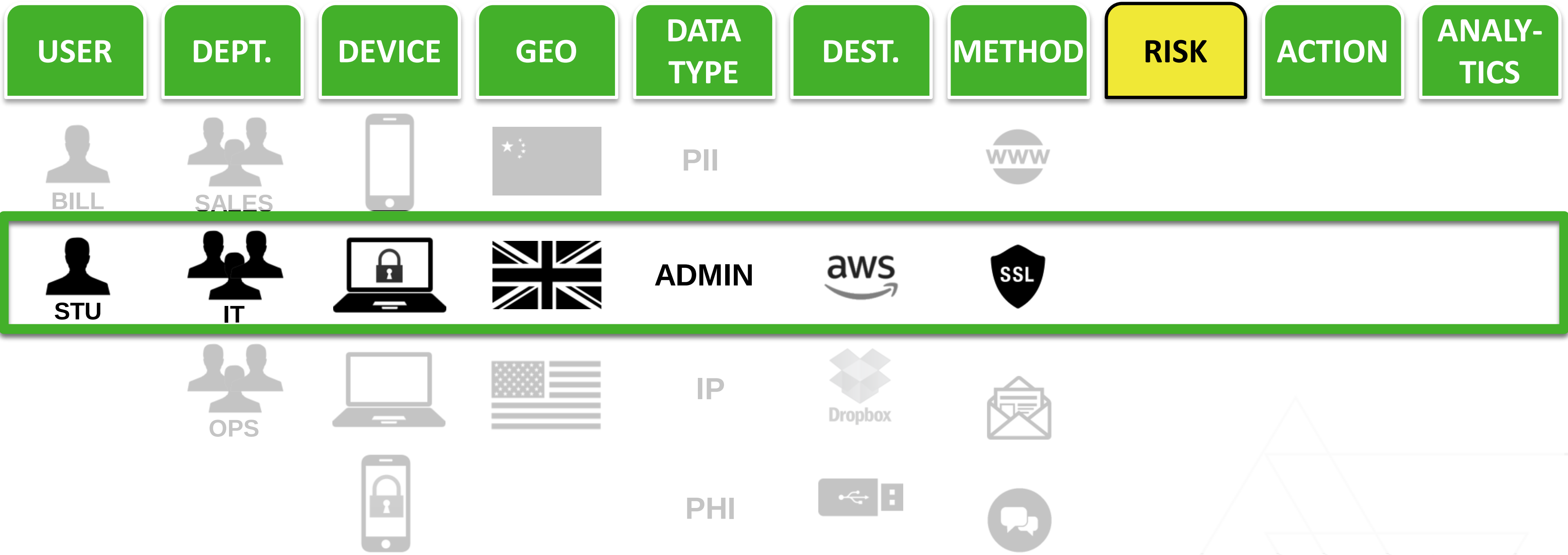
STU | IT | ADMIN

OPS | IP

PHI

Copyright © 2018 Forcepoint

RISK-ADAPTIVE PROVIDES ***PRE-EVENT*** DETECTION



USER

DEPT.

DEVICE

GEO

DATA TYPE

DEST.

METHOD

RISK

ACTION

ANALY-TICS

BILL

SALES

PII

STU

IT

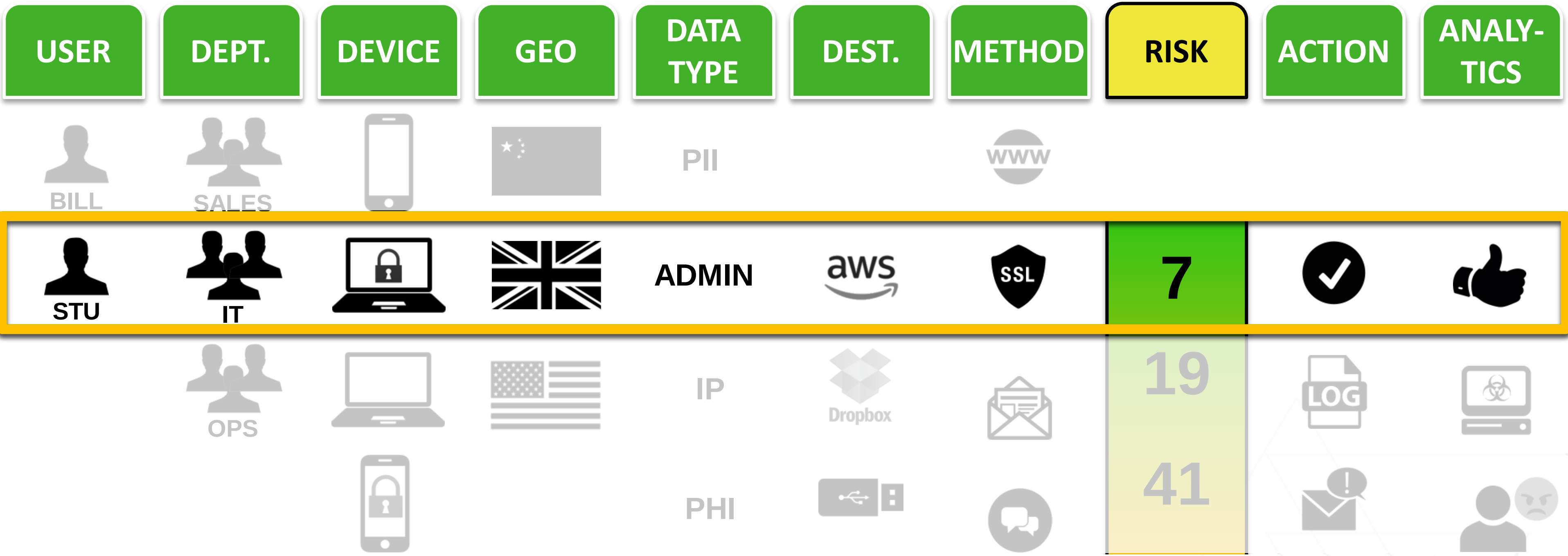
ADMIN

OPS

IP

PHI

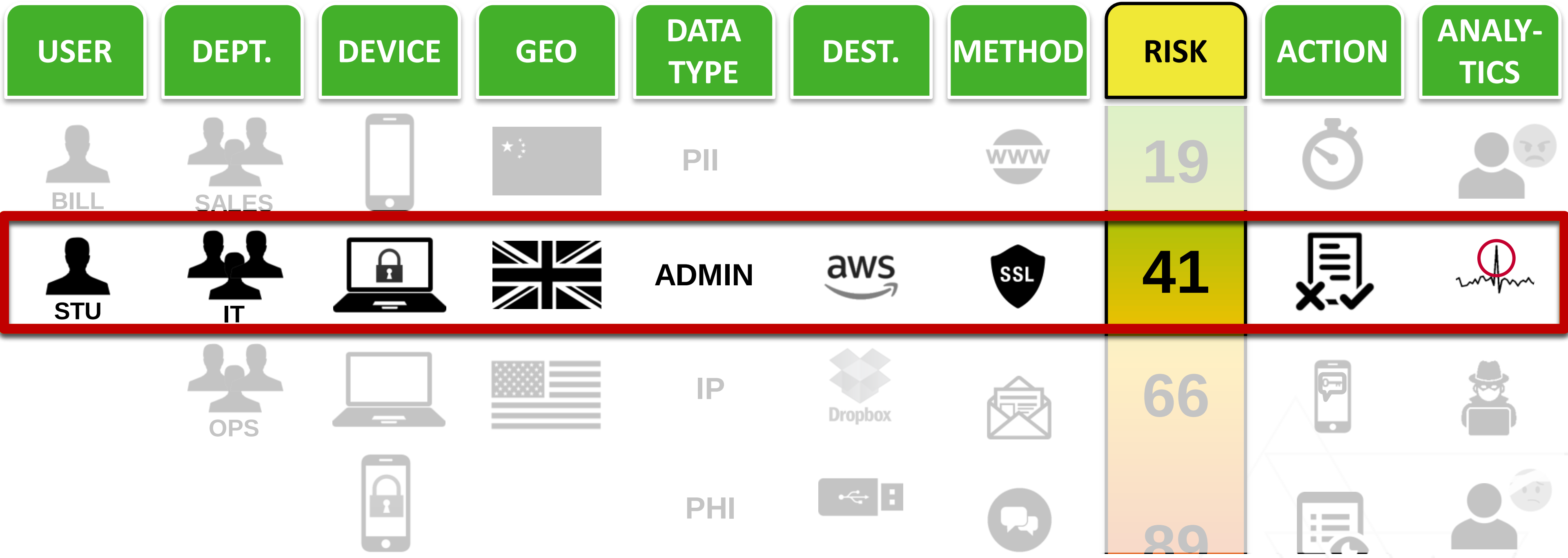
PROVIDES ***PRE-EVENT*** DETECTION



USER | DEPT. | DEVICE | GEO | DATA TYPE | DEST. | METHOD | RISK | ACTION | ANALY-TICS

Copyright © 2018 Forcepoint | 2

PROVIDES *PRE-EVENT* DETECTION



USER	DEPT.	DEVICE	GEO	DATA TYPE	DEST.	METHOD	RISK	ACTION	ANALYTICS
BILL	SALES			PII		WWW	19		
STU	IT			ADMIN	aws	SSL	41		
	OPS			IP	Dropbox		66		
				PHI			89		

Copyright © 2018 Forcepoint

YOU NEED RISK-ADAPTIVE PROTECTION

Risk-adaptive protection dynamically applies monitoring and enforcement controls to protect data based on calculated behavioural **risk level of users** and the **value of data** accessed.

This allows security organisations to better understand risky behaviour and automate policies, dramatically reducing the quantity of alerts requiring investigation.

HOW RISK-ADAPTIVE PROTECTION WORKS:

1) Risk levels are driven up and down by human behaviour

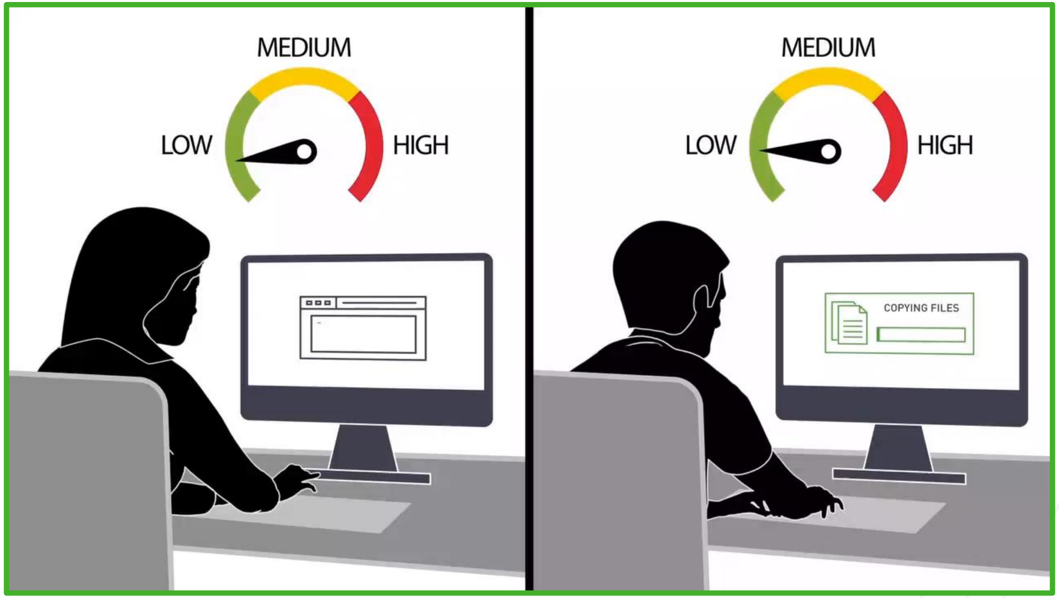
2) Each user has a unique and dynamic Risk Level which changes based upon behaviour

3) Risk Levels drive different outcomes

4) The security adapts to the risk levels as behaviours change

Copyright © 2017 Forcepoint.

RISK-ADAPTIVE IN ACTION



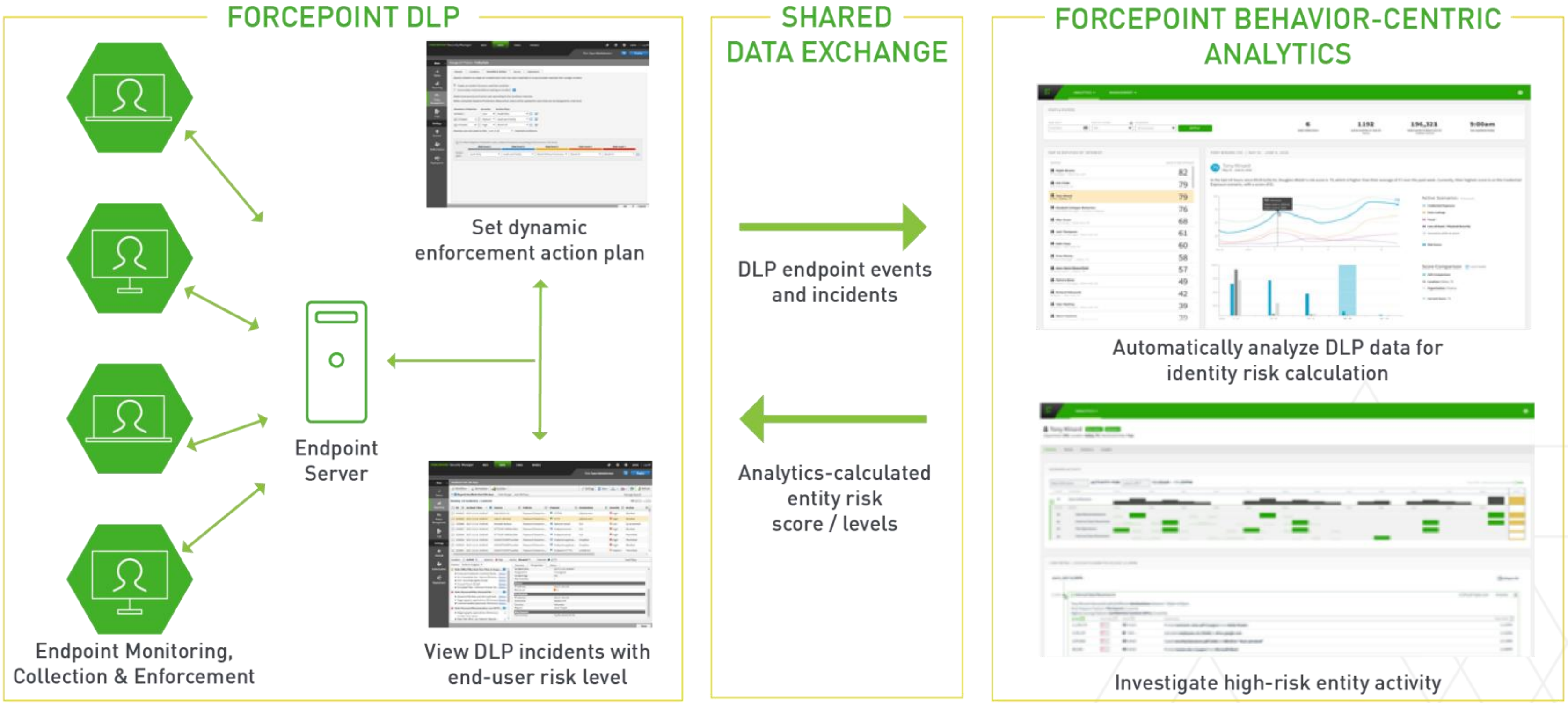
E[illegible] RISK

LEVEL [illegible] AVIOUR

Copyright © 2018 Forcepoint.

INTRODUCING DYNAMIC DATA PROTECTION

DELIVERING RISK-ADAPTIVE PROTECTION



FORCEPOINT DLP

Set dynamic enforcement action plan

Endpoint Server

Endpoint Monitoring, Collection & Enforcement

View DLP incidents with end-user risk level

SHARED DATA EXCHANGE

DLP endpoint events and incidents

Analytics-calculated entity risk score / levels

FORCEPOINT BEHAVIOR-CENTRIC ANALYTICS

Automatically analyze DLP data for identity risk calculation

Investigate high-risk entity activity

Copyright © 2017 Forcepoint.

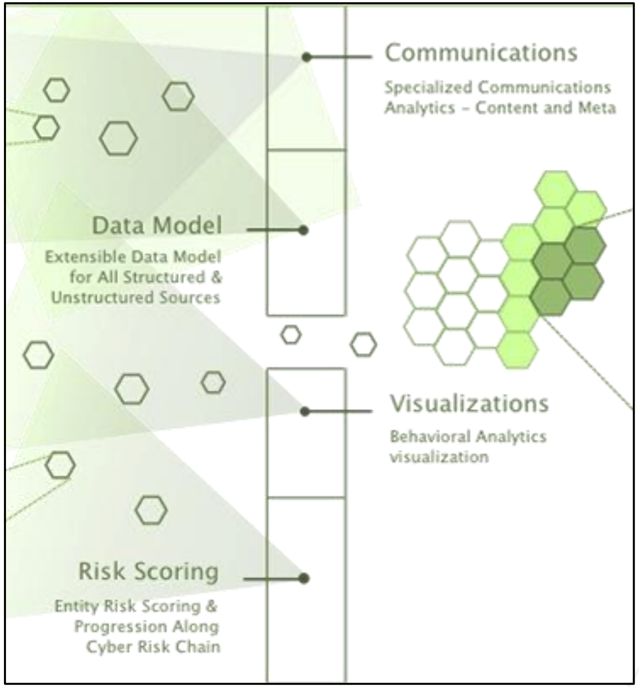
DYNAMIC DATA PROTECTION PROVIDES AUTOMATED ENFORCEMENT

DATA SOURCES 〉 ANALYTIC ENGINE AND INSIGHTS 〉 POLICY ENFORCEMENT

Forcepoint DLP

OR

Any Data Source

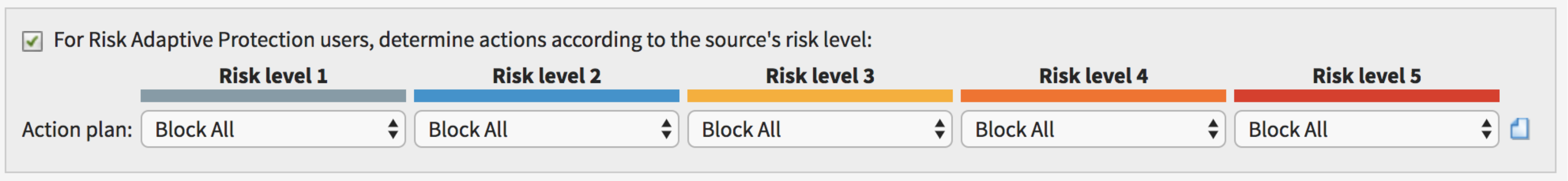

Communications
Specialized Communications Analytics – Content and Meta
Data Model
Extensible Data Model for All Structured & Unstructured Sources
Visualizations
Behavioral Analytics visualization
Risk Scoring
Entity Risk Scoring & Progression Along Cyber Risk Chain

Forcepoint Endpoint

Copyright © 2017 Forcepoint. |

GRADUATED ENFORCEMENT BASED ON RISK

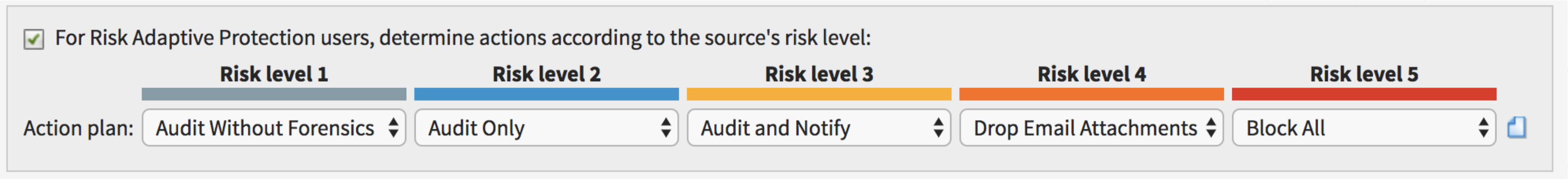
For policies governing compliance use-cases or highly sensitive information, “Block All” can be the action plan for all risk levels.



☑ For Risk Adaptive Protection users, determine actions according to the source's risk level:

	Risk level 1	Risk level 2	Risk level 3	Risk level 4	Risk level 5
Action plan:	Block All	Block All	Block All	Block All	Block All

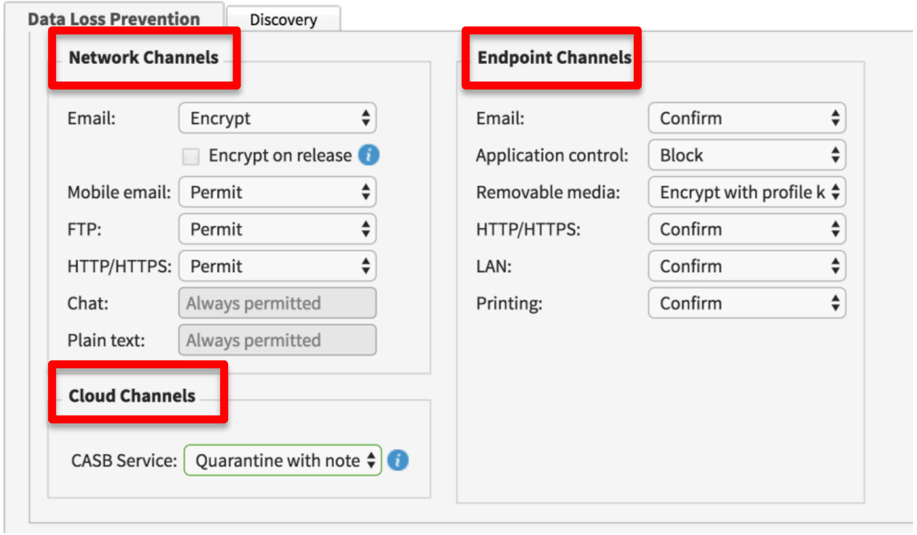
For policies where additional context can help inform decisions, additional granularity is now available.



☑ For Risk Adaptive Protection users, determine actions according to the source's risk level:

	Risk level 1	Risk level 2	Risk level 3	Risk level 4	Risk level 5
Action plan:	Audit Without Forensics	Audit Only	Audit and Notify	Drop Email Attachments	Block All

COMMON POLICY ENFORCEMENT ACROSS MULTIPLE CHANNELS



Network Channels

Email:	Encrypt
	□ Encrypt on release
Mobile email:	Permit
FTP:	Permit
HTTP/HTTPS:	Permit
Chat:	Always permitted
Plain text:	Always permitted

Cloud Channels

CASB Service:	Quarantine with note

Endpoint Channels

Email:	Confirm
Application control:	Block
Removable media:	Encrypt with profile k
HTTP/HTTPS:	Confirm
LAN:	Confirm
Printing:	Confirm

With the DLP for IP Protection Suite, customers implement multiple action plans that provide the ability to protect data in motion, data in use and data at rest, even when the data gets stored in SaaS applications

Copyright © 2017 Forcepoint.

BENEFITS OF DYNAMIC DATA PROTECTION

Intelligent DLP

Reduce the amount of DLP alerts that need to be triaged, transition DLP from broad to individual policies.

Increased Productivity

Provide greater flexibility in policies, and adapt enforcement based on calculated risk.

Proactive Security Management

Detect and respond to high-impact events in a shorter amount of time.

Copyright © 2017 Forcepoint.

KEY TAKEAWAYS

- Leveraging analytics to inform enforcement leads to a proactive security posture
- A system in which control of both the analytics and enforcement mechanism allows for uniform policy enforcement and flexibility
- Learn more about Dynamic Data Protection at: **https://www.forcepoint.com/solutions/need/dynamic-data-protection**

Copyright © 2017 Forcepoint.