

New threats from a changing security landscape.

Symantec insights from ISTR

Ramsés Gallego

**CISM, CGEIT, CISSP, SCPM, CCSK, ITIL, COBIT, Six Sigma Black Belt
Strategist & Evangelist, Symantec - Office of the CTO**



Past International Vice President, ISACA, Board of Directors

Immediate Past President, ISACA Barcelona Chapter

Executive Vice President, Quantum World Association

Privacy by Design Ambassador, Government of Ontario, Canada

ramses_gallego@symantec.com

 **@ramsesgallego**





ISTR

Internet Security
Threat Report

Volume

23





CYBER ATTACKS
JUST AHEAD

A word cloud of cybersecurity terms. The word 'Attacks' is the largest and most prominent, located in the lower-left quadrant. Other large words include 'Malware', 'Spionage', 'Botnets', 'Trojans', 'Phishing', 'Vulnerabilities', 'Spoofting', and 'Hacktivism'. Smaller words include 'Worms', 'Hackers', 'Spam', 'DDos', 'Intrusions', 'SQL Injection', 'Session hijacking', 'Remotes scans', 'Internal Threat', 'Virus', 'Scams', 'Spyware', 'Control', 'Zombie', 'Scripting', 'Malicious code', and 'Disgruntled employees'. The words are arranged in a roughly circular pattern around the center, with varying colors and orientations.

Brute force attacks

Trojans Phishing

Worms Malware

Hackers Spam

DDos Intrusions SQL Injection

Session hijacking Vulnerabilities

Remotes scans Botnets

Internal Threat Virus Spoofting

Spyware Scams

Control Spionage

Attacks Zombie Scripting

Malicious code Hacktivism

Disgruntled employees

A word cloud featuring various business and technology-related terms. The words are arranged in a roughly triangular shape, with 'Information' at the top and 'Risk' at the bottom. The words are in different colors and sizes, with 'Strategy' and 'Indicators' being the largest. The colors include purple, brown, green, blue, orange, red, and grey.

Information
Tactics Auditing
Trust Strategy
Business
Technology KPIs Real-time
Dashboards Efficiency
Partners Metrics Availability
Responsibility Value Resiliency
KGIs Access
Governance Indicators
Architectures Effectiveness
Compliance Integration
Identity Management
Risk





Art of WAR!

“ Every battle is won
BEFORE
it is fought. ”

Sun Tzu



An aerial, black-and-white photograph of a military airfield. Several aircraft are visible on the tarmac, including a large bomber in the foreground with a star insignia on its fuselage. The background shows a grid-like pattern of fields and roads.

Know thy self know thy

ENEMY

a thousand

BATTLES

a thousand

VICTORIES




Internet of Things

Internet of Everything

Internet of Threats

Internet of Trouble

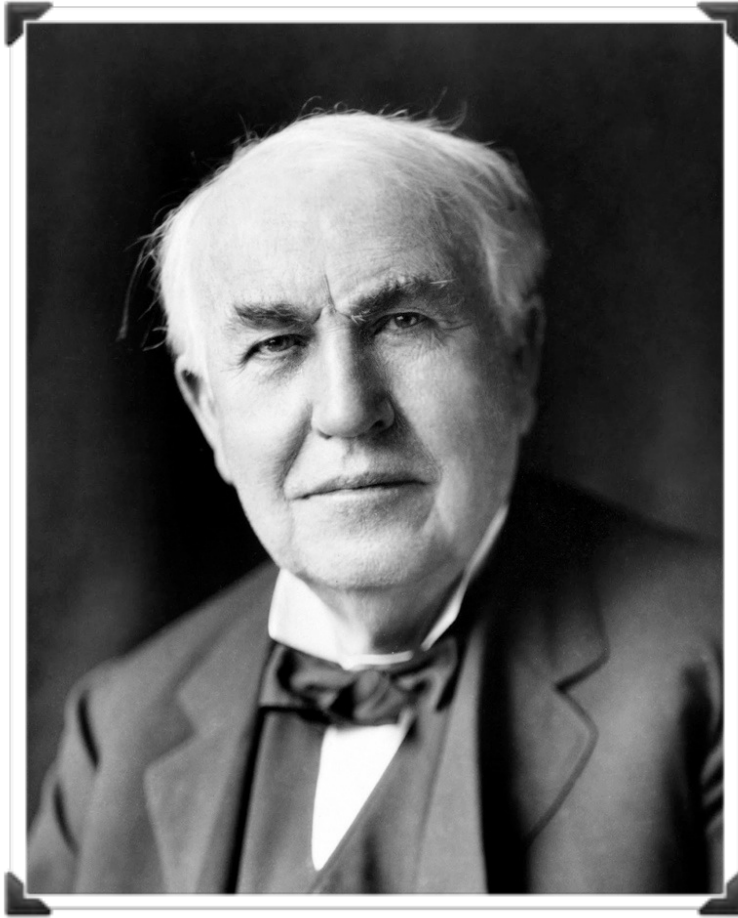




Who?
What?
How?
When?
Where?
What for?

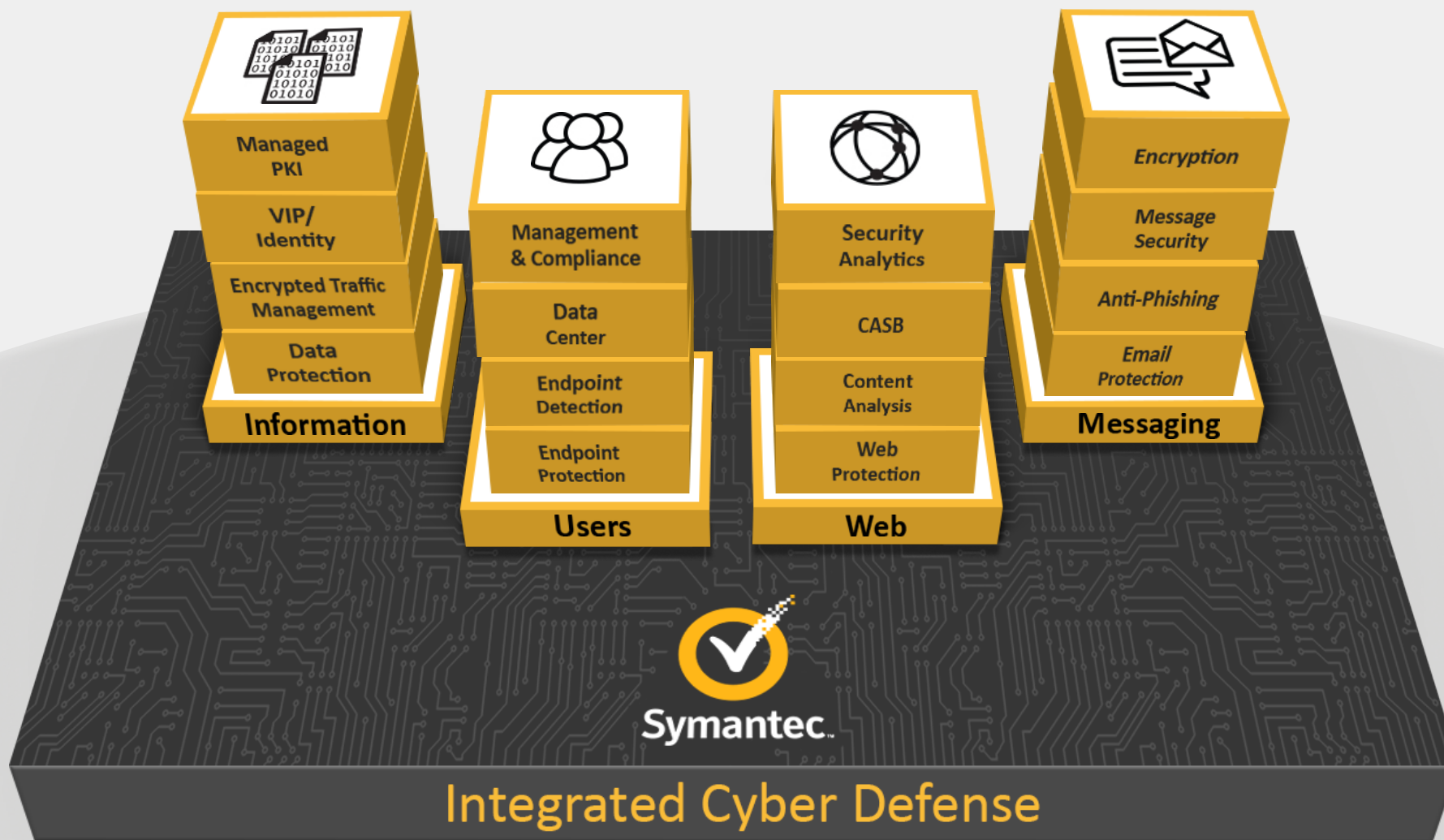


A holistic vision

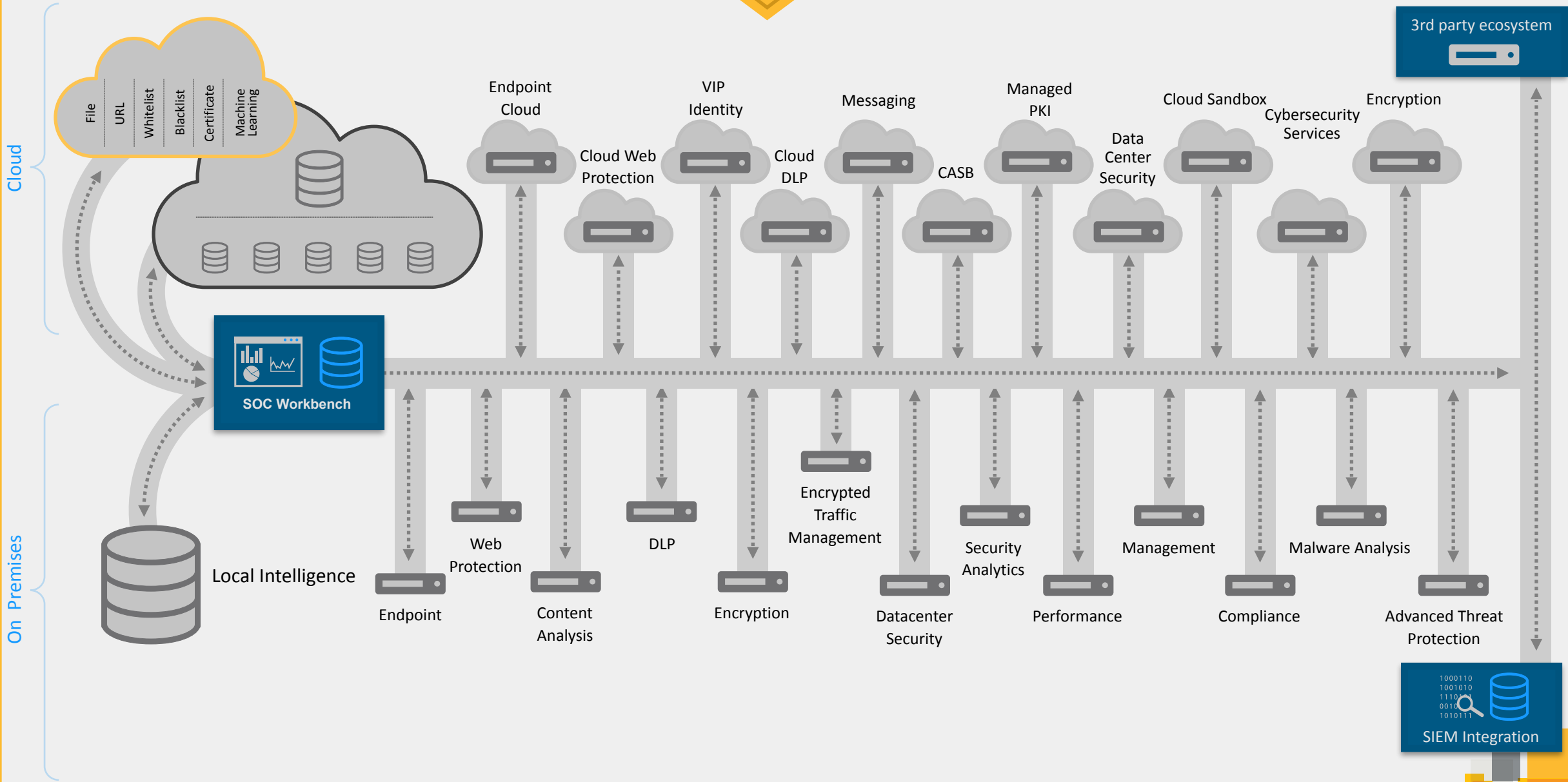


Thomas Edison, 1847-1931

‘A vision without execution is a hallucination’

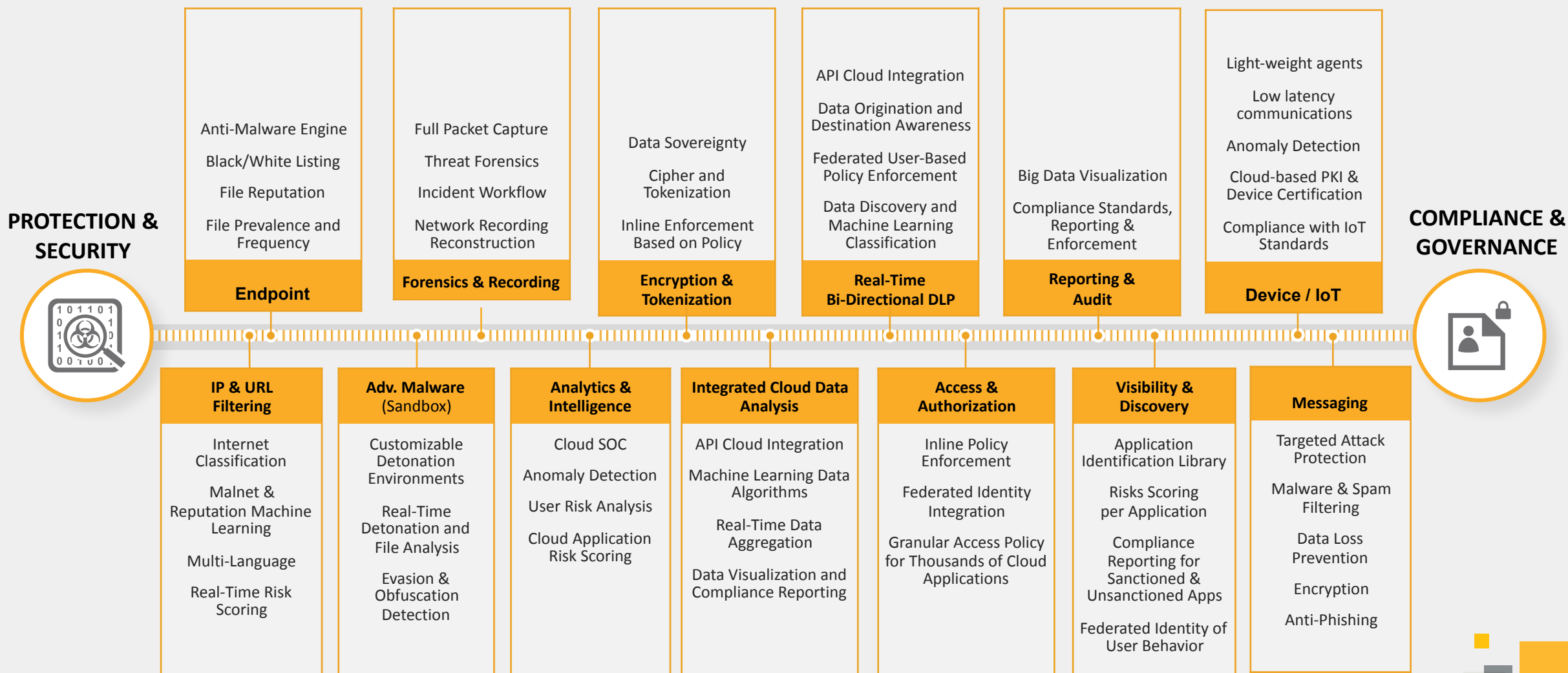


Cyber Defense Integrated Platform



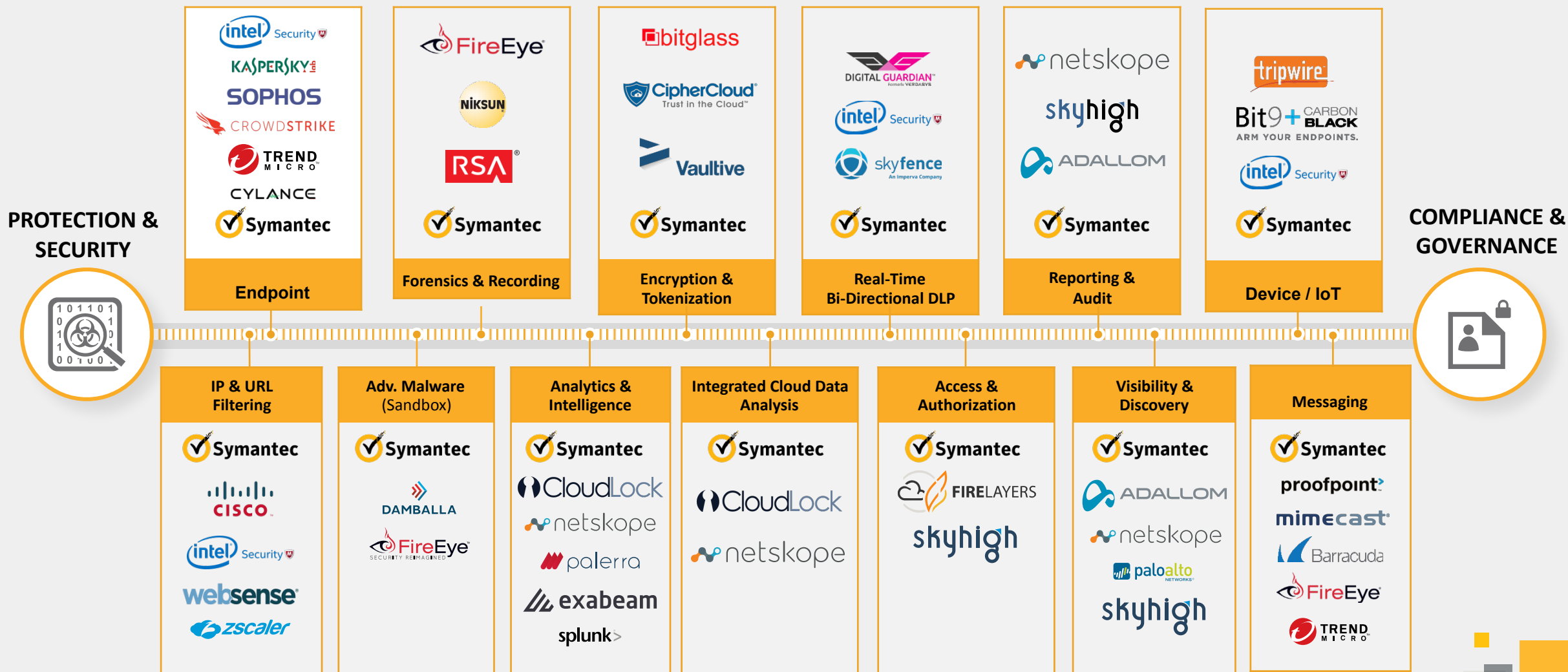
Security Vendors Arising Across Cloud Continuum

Needs Exist in Several Distinct Areas



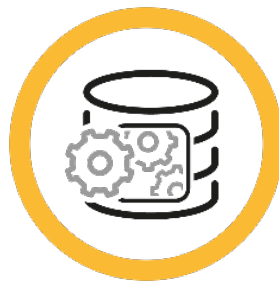
Security Vendors Arising Across Cloud Continuum

Needs Exist in Several Distinct Areas





Collect



Process



Retain and secure



Govern

Define and locate
personal data

Secure technology
that collects
personal data

Record consent from
data subjects

Pseudoanonymize
and obfuscate
personal data

Detect and block
threats to data in
use

Validate data
processors

Evaluate the impact
on privacy (PIA)

Secure transfer and
storage of collected
data

Restrict processing of
data that organization
has to retain

Prevent data loss

Control access to
data

Protect data 'at rest'
in the datacenter

Risk Management of
Info Lifecycle

Validate data
subjects invoking
rights

Educate DPOs on
Cyber Risk

Minimize,
Anonymize, Delete
data



Collect

DLP Classification
Policies



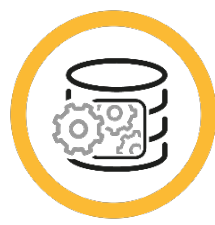
MPKI
Website Security
DCS:SA



Control Compliance
Suite



Encryption
MPKI



Process

Deepsight / CSS
SEP / ATP / DCS
.Cloud / DLP



Control Compliance
Suite Vendor
Manager



Evaluate the impact
on privacy (PIA)

Encryption
MPKI



Retain and secure

Access Control
Encryption



Encryption
DLP



Access Control
SAM / VIP / MPKI



Encryption / DLP
SEP / ATP / DCS



Govern

Risk Management
on Info Lifecycle

Validate Data
Subjects invoking
rights

Blackfin/ Security
Simulation



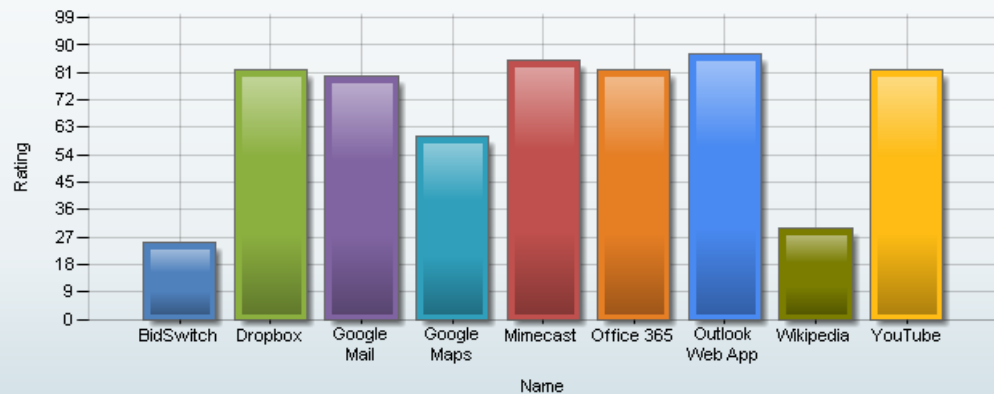
Q#	Art.	Process question	Level 0	Level 1	Level 2	Level 3	Level 4
4.1P	4(5), 11, 32(1)(a), Rec 26	Do you apply pseudonymization and anonymization to personal data you hold, so as to minimize exposure to privacy risk?	I don't know how to do that	I know about those concepts but I don't think they are relevant to us	We only implement pseudonymization and anonymization when specifically asked to do so	We integrate pseudonymization and anonymization in most of our processes when convenient	We apply them wherever possible, including technical controls to prevent the reversal of pseudonymization or anonymization
4.2P	28	Do you follow a clear selection process to choose the suppliers who process personal data for you?	I don't think we use any suppliers to process data on our behalf	We try to aim for cost efficiency and ease of use	We try to use only large reputable vendors	We select specialized vendors with references and certifications specific to our needs	We thoroughly vet eligible candidates and select those which offer all of the guarantees required by the GDPR
4.3P	46, 47, 48, 49	Do you implement mechanisms to ensure that any export of personal data outside of the European Economic Area is compliant with EU privacy law?	I am not aware that we export any personal data out of Europe	If we do any export at all, we trust our contractors to do what's required	We only export data to countries we have reasons to believe are safe	We make specific approved arrangements for every particular case	We have a structured streamlined and documented process to legally transfer data outside of the EEA
4.4P	15	Do you enable individuals to get access to personal data you hold about them?	No, the data is ours, I don't see why we should	Maybe we can do that if we get asked to	In general, if it's not unreasonable, we try to be helpful when people ask	Yes, to the extent that we are able to figure out which data belongs to the person who's asking	Yes, we have a contact point and a process to respond swiftly, giving all relevant information as required
4.9P	21	If an individual withdraws consent or raises an objection to what you are doing with his/her data, are you able to immediately stop processing that data?	No, individuals don't have a means to object in that way	If the individual can justify the request, we could probably try to accommodate	To the extent that the objection looks reasonable to us, we will consider it	Unless it is excessively cumbersome to do, we will normally respect such objections	Yes, we inform people of their right to object, we provide them means to do it, and we are able to stop processing unless we can demonstrate a compelling need for us to carry on

Q#	Article	Process question	Level 0	Level 1	Level 2	Level 3	Level 4
Binary answer for general readiness evaluation:			NO (not ready for GDPR)			YES (on track for GDPR)	
Binary answer for strict GDPR compliance:			NO (not compliant)				YES (compliant)
1.1 K	3	Have you integrated privacy law into your legal compliance framework?	<u>No</u>	<u>Unsure</u>	<u>To some extent</u>	<u>To a large extent</u>	<u>Absolutely</u>
1.2 K	4(1)	Can you separate personal data from your overall data assets?	<u>No</u>	<u>Unsure</u>	<u>To some extent</u>	<u>To a large extent</u>	<u>Absolutely</u>
1.3 K	4(1)	Can you recognize “indirectly identifiable personal data” within your data assets?	<u>No</u>	<u>Unsure</u>	<u>To some extent</u>	<u>To a large extent</u>	<u>Absolutely</u>
1.4 K	4(13), 4(14), 4(15), 9(1), 10	Can you specifically tell what constitutes “sensitive” personal data within your data assets?	<u>No</u>	<u>Unsure</u>	<u>To some extent</u>	<u>To a large extent</u>	<u>Absolutely</u>
1.5 P	5(1)(b), 6(4)	Do you ensure that personal data is only used for the purpose for which it was originally collected? (Purpose Limitation Principle)	<u>No</u>	<u>Unsure</u>	<u>To some extent</u>	<u>To a large extent</u>	<u>Absolutely</u>
1.6 P	5(1)(c)	Do you ensure that you only ever collect so much personal data as you really need for what you are trying to achieve? (Data Minimization Principle)	<u>No</u>	<u>Unsure</u>	<u>To some extent</u>	<u>To a large extent</u>	<u>Absolutely</u>
1.7 P	5(1)(a), 14, 15	Do you tell individuals that you are processing their personal data?	<u>No</u>	<u>Unsure</u>	<u>To some extent</u>	<u>To a large extent</u>	<u>Absolutely</u>
1.8 P	6(1)(a), 7, 8, 9	When collecting information from individuals, do you get their consent to process their personal data?	<u>No</u>	<u>Unsure</u>	<u>To some extent</u>	<u>To a large extent</u>	<u>Absolutely</u>
1.9 P	6(1)(c)	Have you mapped all the flows of personal data in your organization, including those outsourced to external suppliers?	<u>No</u>	<u>Unsure</u>	<u>To some extent</u>	<u>To a large extent</u>	<u>Absolutely</u>
1.10 P	6(1)(b) to 6(1)(f)	If not relying on individual consent, do you rely on any of the other five legal bases for data processing (contract execution, legal obligation, vital interest, public interest, legitimate interest)?	<u>No</u>	<u>Unsure</u>	<u>To some extent</u>	<u>To a large extent</u>	<u>Absolutely</u>

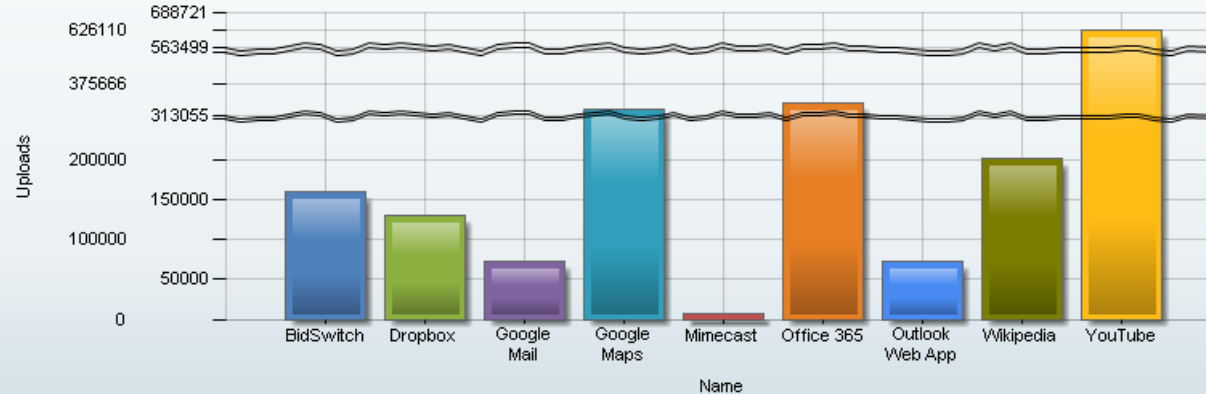
Q#	Article	Process question	Level 0	Level 1	Level 2	Level 3	Level 4
Binary answer for general readiness:			NO (not ready for GDPR)			YES (on track for GDPR)	
Binary answer for GDPR compliance:			NO (not compliant)				YES (compliant)
2.1 K	4(7), 25, 26	Are you aware of the circumstances where you are considered as a “data controller” under the GDPR?	<u>No</u>	<u>Unsure</u>	<u>To some extent</u>	<u>To a large extent</u>	<u>Absolutely</u>
2.2 P	4(8), 28	As a “data processor” under privacy law, do you embed privacy compliance in the services you provide?	<u>No</u>	<u>Unsure</u>	<u>To some extent</u>	<u>To a large extent</u>	<u>Absolutely</u>
2.3 P	37, 38, 39	Do you currently have a dedicated resource looking after your privacy compliance (e.g. a DPO)?	<u>No</u>	<u>Unsure</u>	<u>To some extent</u>	<u>To a large extent</u>	<u>Absolutely</u>
2.4 K	5(2), 24(2)	Do you have a demonstrable privacy compliance program in place? (Accountability Principle)	<u>No</u>	<u>Unsure</u>	<u>To some extent</u>	<u>To a large extent</u>	<u>Absolutely</u>
2.5 P	25(1)	Do you systematically embed privacy compliance into the creation of your internal business processes, products and services? (Privacy by Design Principle)	<u>No</u>	<u>Unsure</u>	<u>To some extent</u>	<u>To a large extent</u>	<u>Absolutely</u>
2.6 P	22	Do you know what precautions to take before profiling individuals, for example when tailoring your online advertising to the preferences of each individual, or when assessing credit-worthiness or insurability?	<u>No</u>	<u>Unsure</u>	<u>To some extent</u>	<u>To a large extent</u>	<u>Absolutely</u>
2.7 P	25(2)	Are the default settings in all your processes, products and services defined to ensure maximum privacy? (Privacy by Default Principle)	<u>No</u>	<u>Unsure</u>	<u>To some extent</u>	<u>To a large extent</u>	<u>Absolutely</u>
2.8 P	35, 36	Do you implement a policy to identify which of your activities create a high privacy risk to individuals?	<u>No</u>	<u>Unsure</u>	<u>To some extent</u>	<u>To a large extent</u>	<u>Absolutely</u>
2.9 P	35	Do you have a specific process in place to carry out Data Protection Impact Assessments (DPIAs)?	<u>No</u>	<u>Unsure</u>	<u>To some extent</u>	<u>To a large extent</u>	<u>Absolutely</u>
2.10 P	30	Do you document your activities involving the processing of personal data?	<u>No</u>	<u>Unsure</u>	<u>To some extent</u>	<u>To a large extent</u>	<u>Absolutely</u>

Symantec Elastica - DB 1

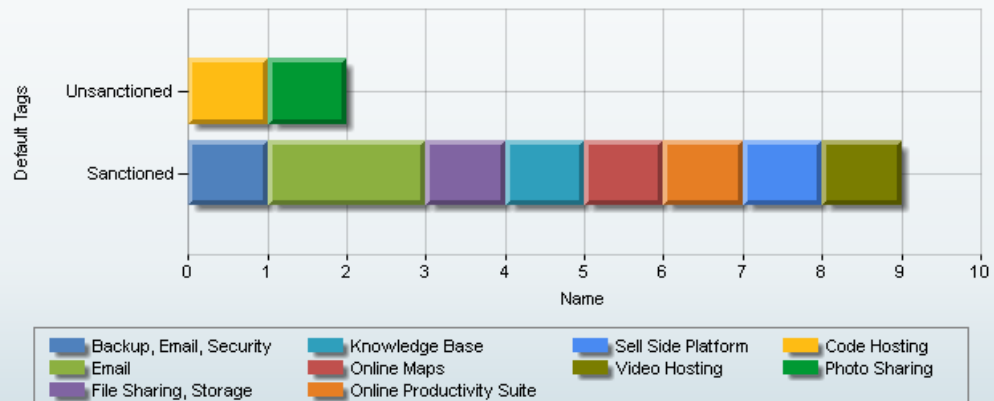
Elastica - Rating for Sanctioned Apps



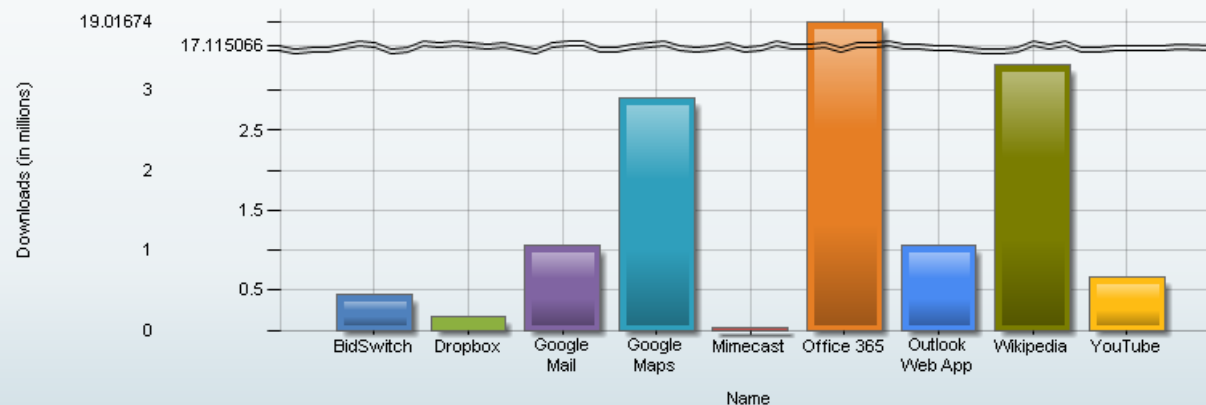
Elastica - Uploads to Sanctioned Apps



Elastica - Sanctioned Apps by Category



Elastica - Downloads from Sanctioned Apps



RE^EEVOLUTION





The Art of DECEPTION



MONTGOMERY'S HOTEL
INDIAN STREET BLADE

Handwritten text in a cursive script, likely a signature or name, rendered in a dotted format for tracing or learning. The text is arranged in two lines. The top line contains the word "Mama" followed by a flourish. The bottom line contains the word "Mama" followed by a flourish.



Success
Failure



Sir Isaac Newton, 1642 - 1727

**‘If I have seen further it is
by standing on the
shoulder of giants’**

Is. Newton

point of view.

Trust [trʌst] n

confidence in

dependance v

contingent a

WE ARE SYMANTEC



THANK YOU

New threats from a changing security landscape. Symantec insights from ISTR

Ramsés Gallego

**CISM, CGEIT, CISSP, SCPM, CCSK, ITIL, COBIT, Six Sigma Black Belt
Strategist & Evangelist, Symantec - Office of the CTO**



Past International Vice President, ISACA, Board of Directors

Immediate Past President, ISACA Barcelona Chapter

Executive Vice President, Quantum World Association

Privacy by Design Ambassador, Government of Ontario, Canada

ramses_gallego@symantec.com



@ramsesgallego