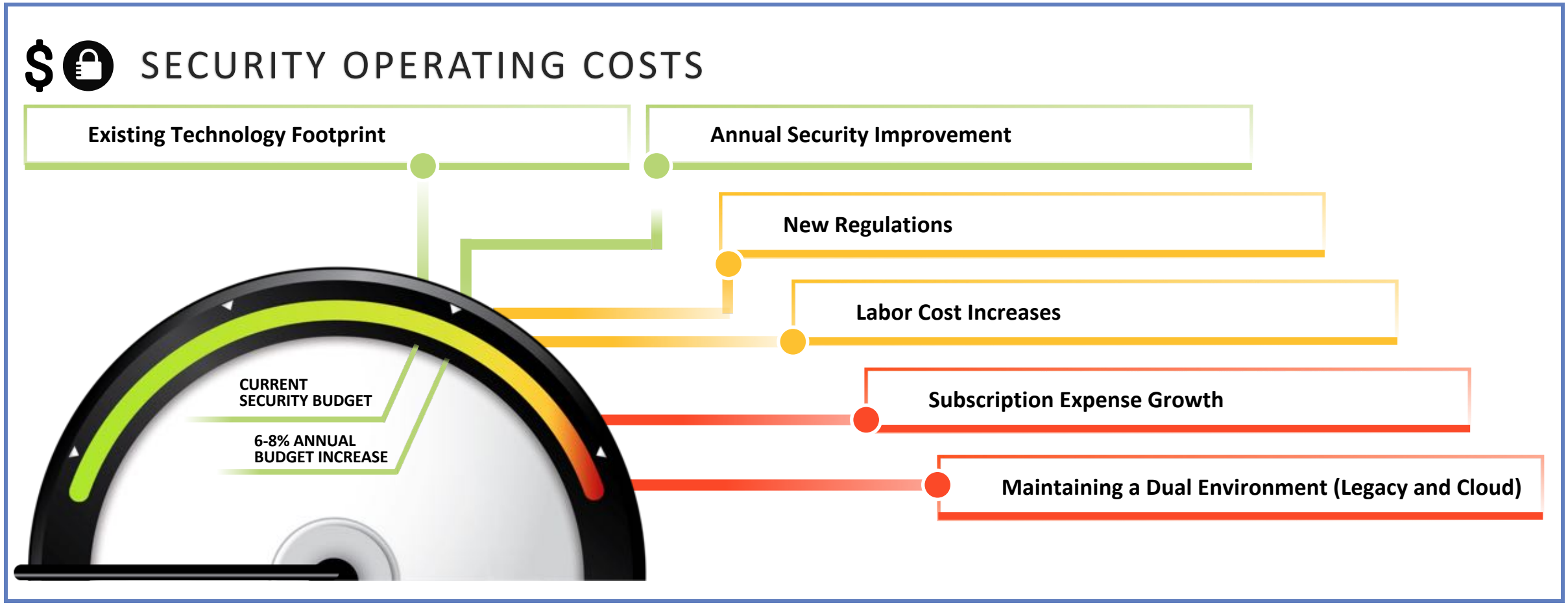
Symantec™

Delivering Integrated Cyber Defense in the Cloud Generation

Fiscal Crisis

The Industry Faces a Looming Fiscal Spending Crisis

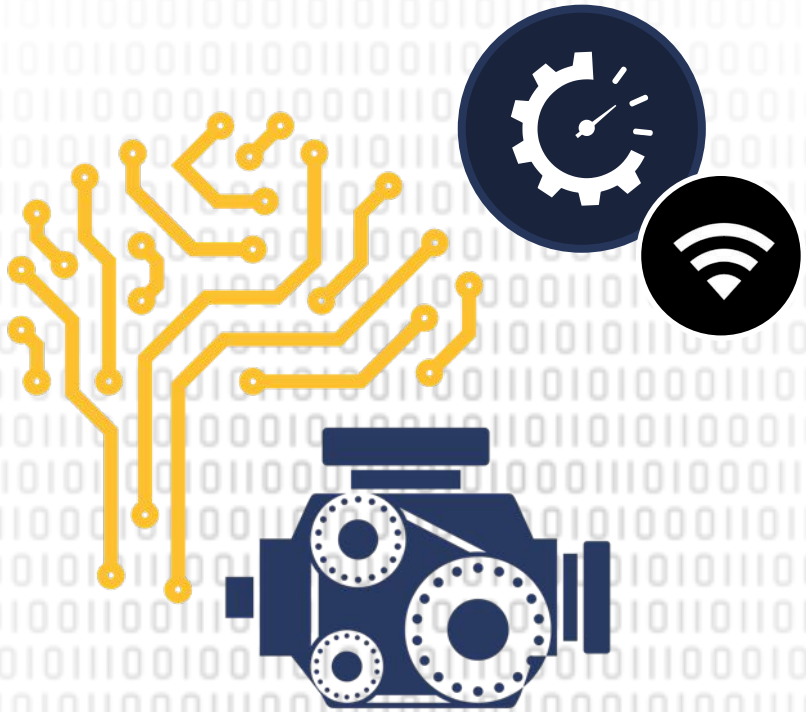


The Cloud Generation Dilemma

A Dark Internet Will Require Presence at Key Termination Points

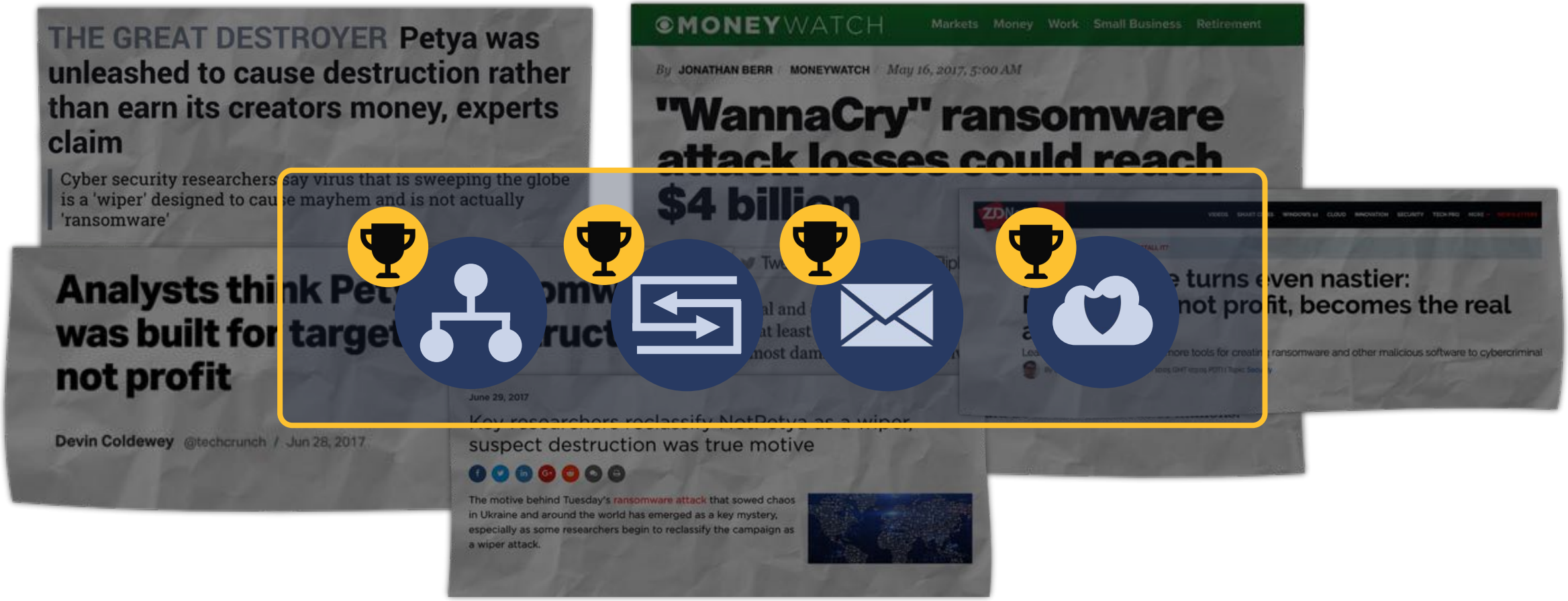
The Cloud Generation Dilemma

Organizations Will Need to Depend on Automatic Security Capabilities



The Cloud Generation Dilemma

Industry Refocused on the Criticality of Prevention



The Cloud Generation Dilemma

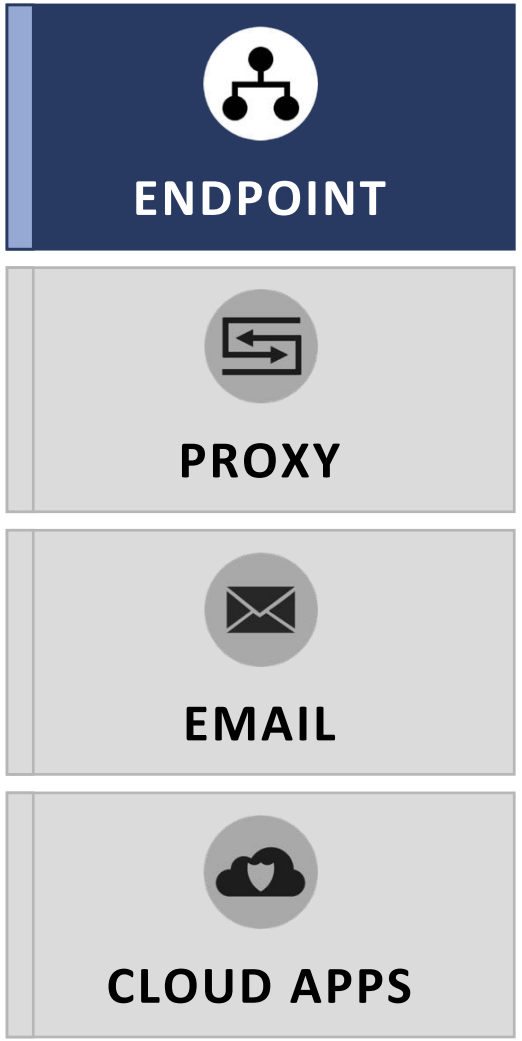
Changing Usage Models Will Mandate Cloud Generation Architecture

The Cloud Generation Dilemma

Changing Usage Models Will Mandate Cloud Generation Architecture

THE COMING FISCAL CRISIS	CLOUD GENERATION ARCHITECTURE & PLATFORMS	A DARK INTERNET
		
DEEP ARTIFICIAL INTELLIGENCE & AUTOMATION		**BEST IN CLASS TERMINATION POINTS & PROTECTION**
		

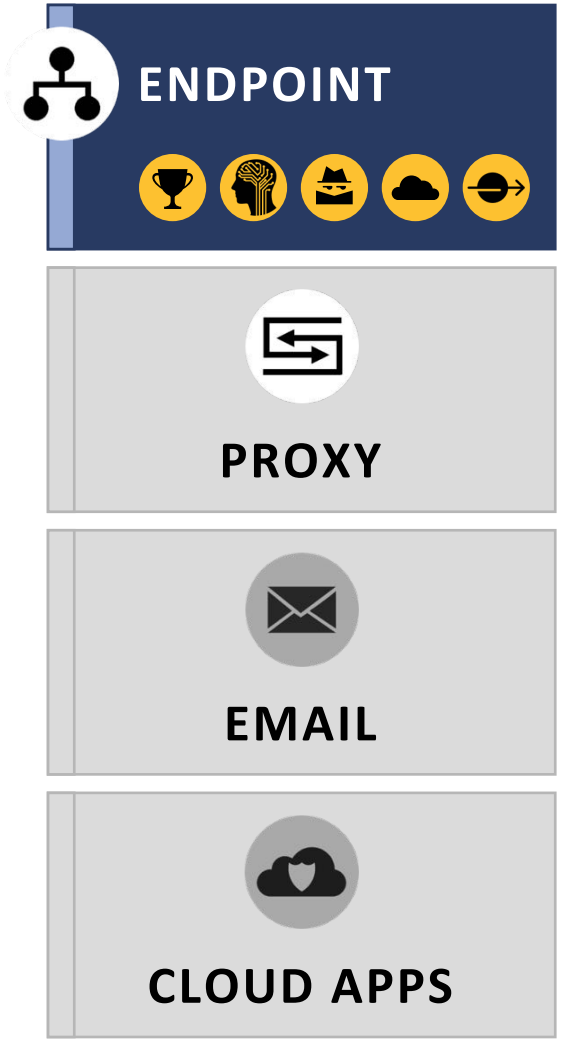
Delivering Protection in The Cloud Generation



Endpoint Requirements

- Best in Class Protection
- Machine Learning / Artificial Intelligence
- Single Agent / Efficient Architecture
- Cloud Aware / Enabled
- Supports all Endpoints

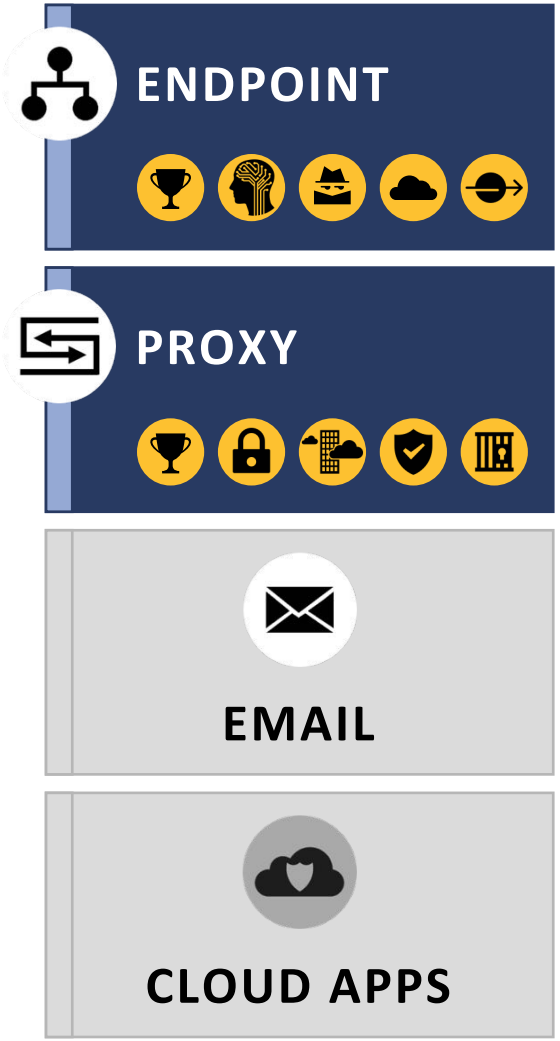
Delivering Protection in The Cloud Generation



Proxy Requirements

- Best in Class
- Strong Encrypted Traffic Management
- Cloud, On-Premise & Virtual Form Factors
- Integrated CASB
- Network Browser Isolation

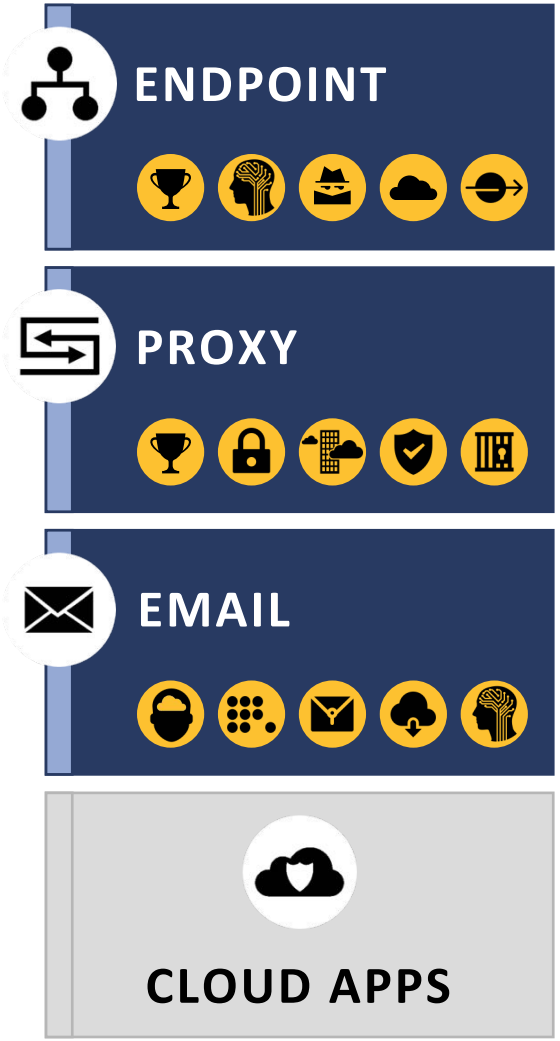
Delivering Protection in The Cloud Generation



Email Requirements

- Best-In-Class Spam and Malware Defense
- Integrated Content Isolation
- Protects Intra-Company, Outbound & Inbound
- Flexible Form Factor
- Machine Learning / Artificial Intelligence

Delivering Protection in The Cloud Generation

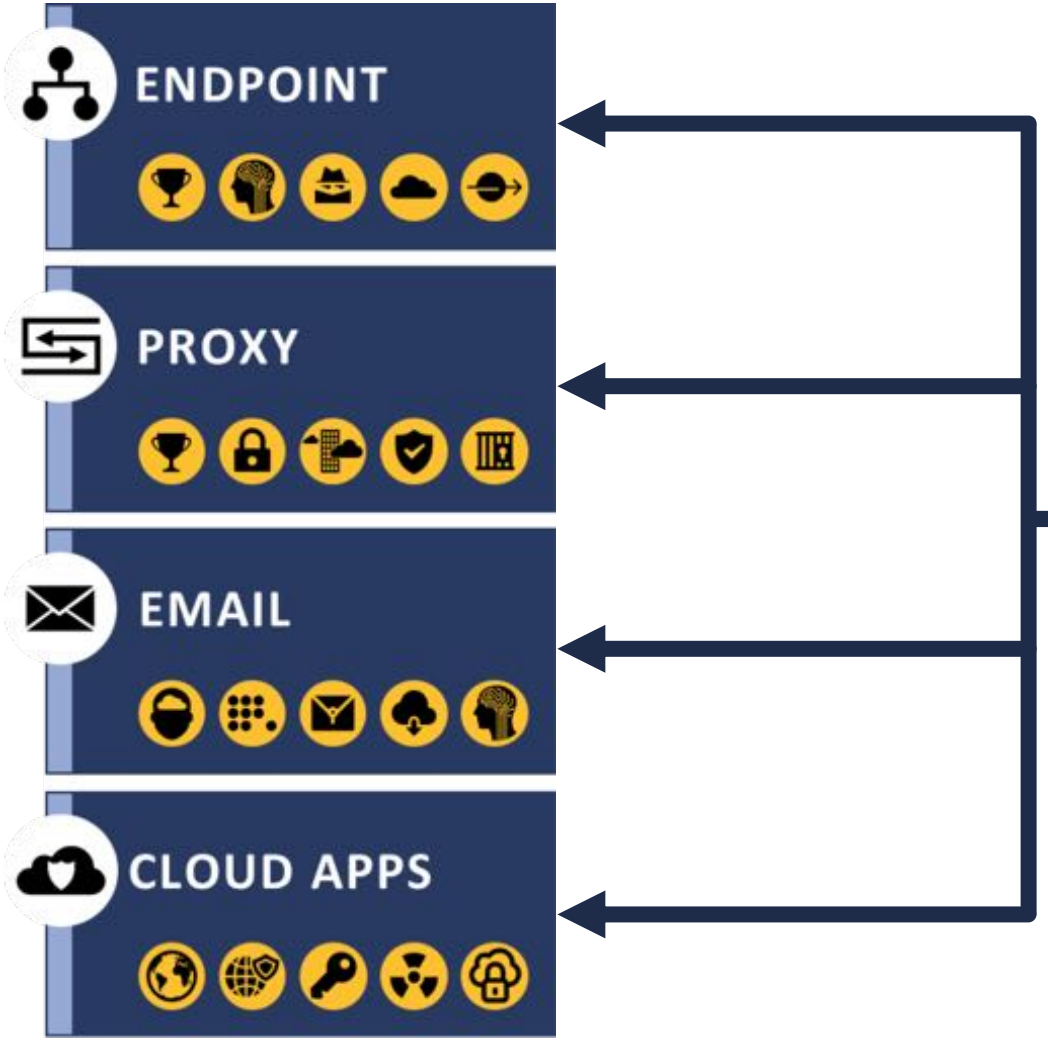


Cloud Application Requirements

- Visibility Over Cloud User Behavior
- Control Across all Cloud Applications
- User and User-Action Based Authentication
- Protections Against Malicious Content
- Extends Data Protection to the Cloud

Delivering Protection in The Cloud Generation

Delivering Protection in The Cloud Generation



API BASED

- One-to-One Integration Mechanics
- Heavy Programmatic Skills
- Support Intensive
- Painful Innovation Consumption

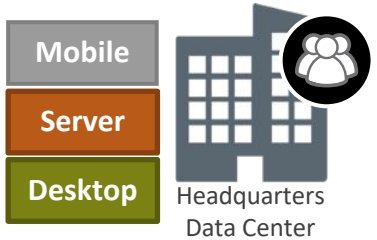
VS

INTEGRATION FABRIC

- Codified Integration Model
- Simple Innovation Consumption
- Enterprise Class Workflows
- Empowers Third Party Participation

Superior ATP Architecture

Better detection and protection for web and mail threats



Headquarters Data Center

SMG — Email (SMTP)

1 Proxy — Web & Cloud (HTTP/HTTPS)

- Decrypt, block web threats
- Extract documents, ICAP to CA

Content Analysis

2 Hash Reputation
Custom user whitelist/blacklist + Risk Scoring
→ Passes acceptable files to user

3 Anti-Malware/Anti-Virus
Combine Symantec, Kaspersky, Sophos or McAfee
→ Signatures evaluated for known bad

4 Predictive File Analysis
Static Code Analysis, Machine Learning
→ Analyzes code for malicious character

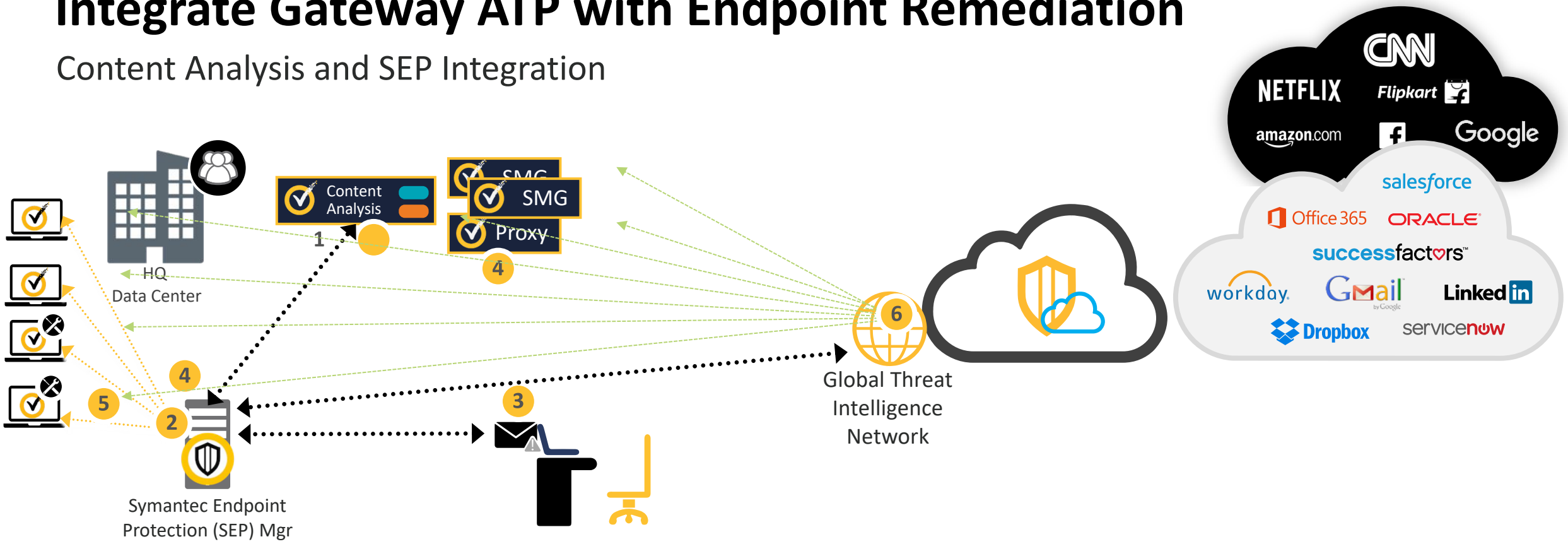
5 Dynamic Sandboxing
Virtual Machine + Emulation Sandboxing
Mobile & Desktop Files
→ Detonates only truly unknown files

- Active, preventative ATP architecture
- Reduce sandbox samples & incidents 99%
- Increase advanced malware detection 4x
- SMG integrates with Content Analysis for advanced malware analysis

Additional Sandbox
On Prem
In Cloud
Malware Analysis Service (MAS)

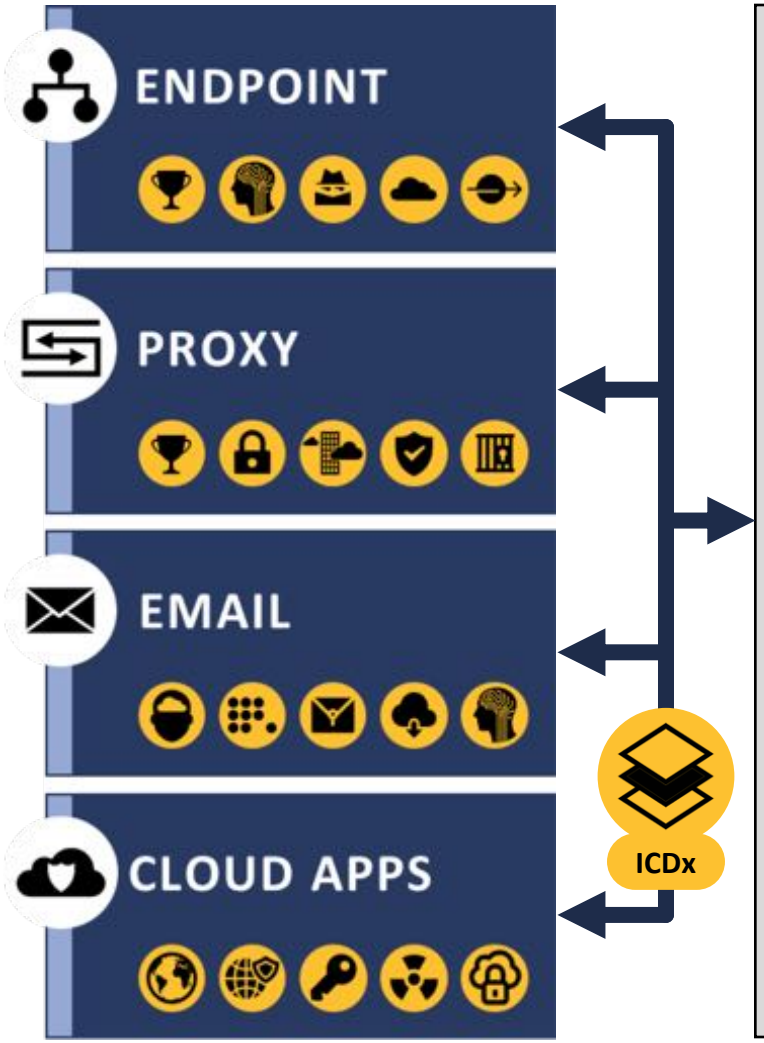
Integrate Gateway ATP with Endpoint Remediation

Content Analysis and SEP Integration



1. Content Analysis discovers a threat downloaded via behavioral detonation – alerts SEP Manager
2. Threat verified on endpoints via Symantec SEPM
3. Alert sent with IoC and infected clients to SOC
4. Blacklist added to SEPM and SWG to stop malware spread
5. Automated remediation and cleanup preformed
6. IoC sent to Global Intelligence Network, updates sent down to all devices

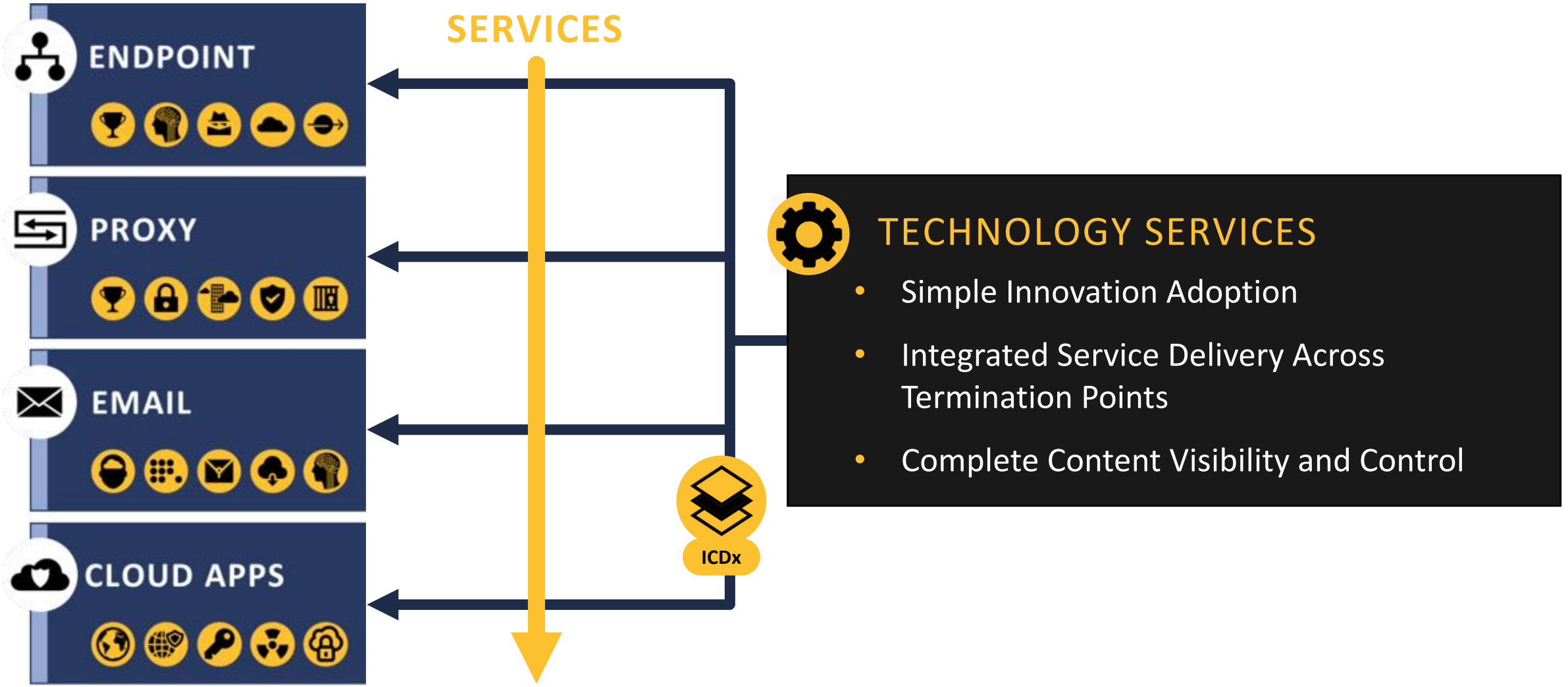
Delivering Protection in The Cloud Generation



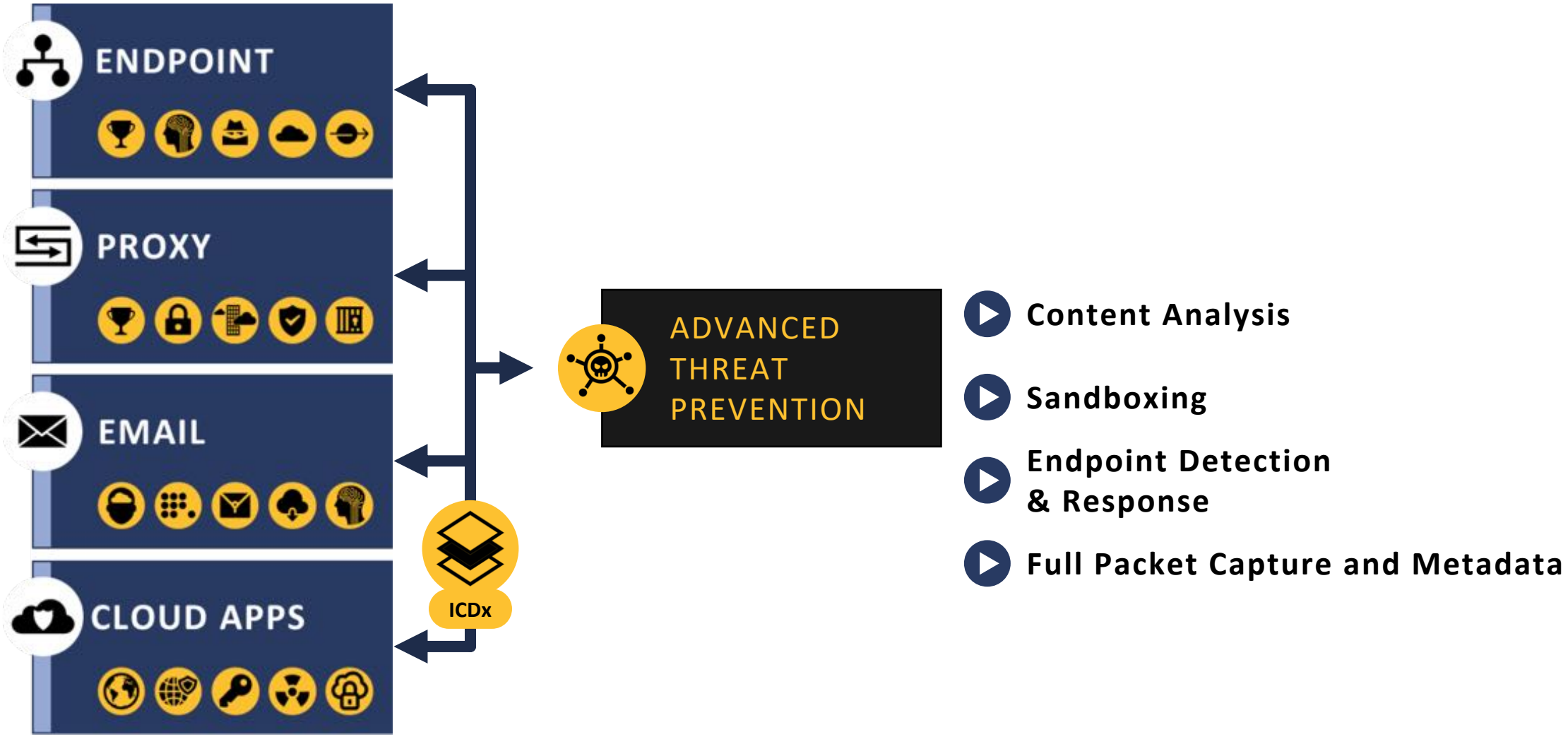
INTEGRATED CYBER DEFENSE EXCHANGE (ICDx)

- Open Interface to Symantec and Third Party Technologies
- Structures and Unifies Telemetry
- Control of Event Information for Regulatory Adherence
- Long-Term Correlation of Event and Telemetry Data
- Provides Automated Actions for Control Points
- Integration Point for External Control Structures
  - MSP
  - Artificial Intelligence / Machine Learning
  - Orchestration

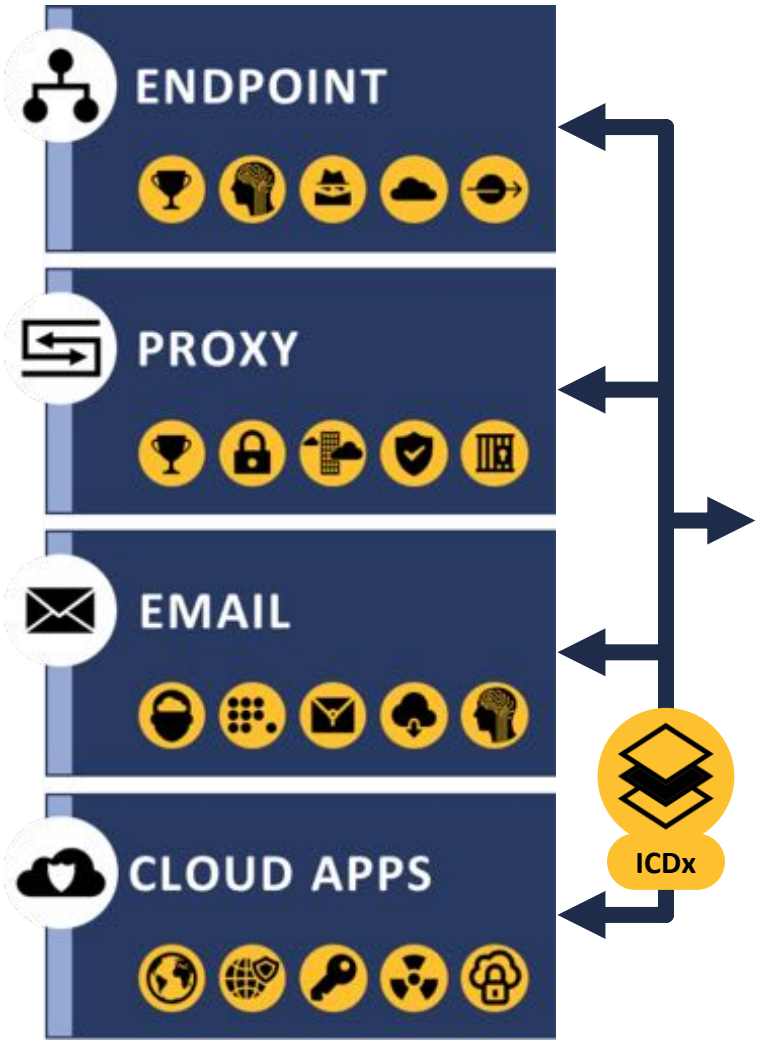
Delivering Technology Services in The Cloud Generation



Delivering Technology Services in The Cloud Generation



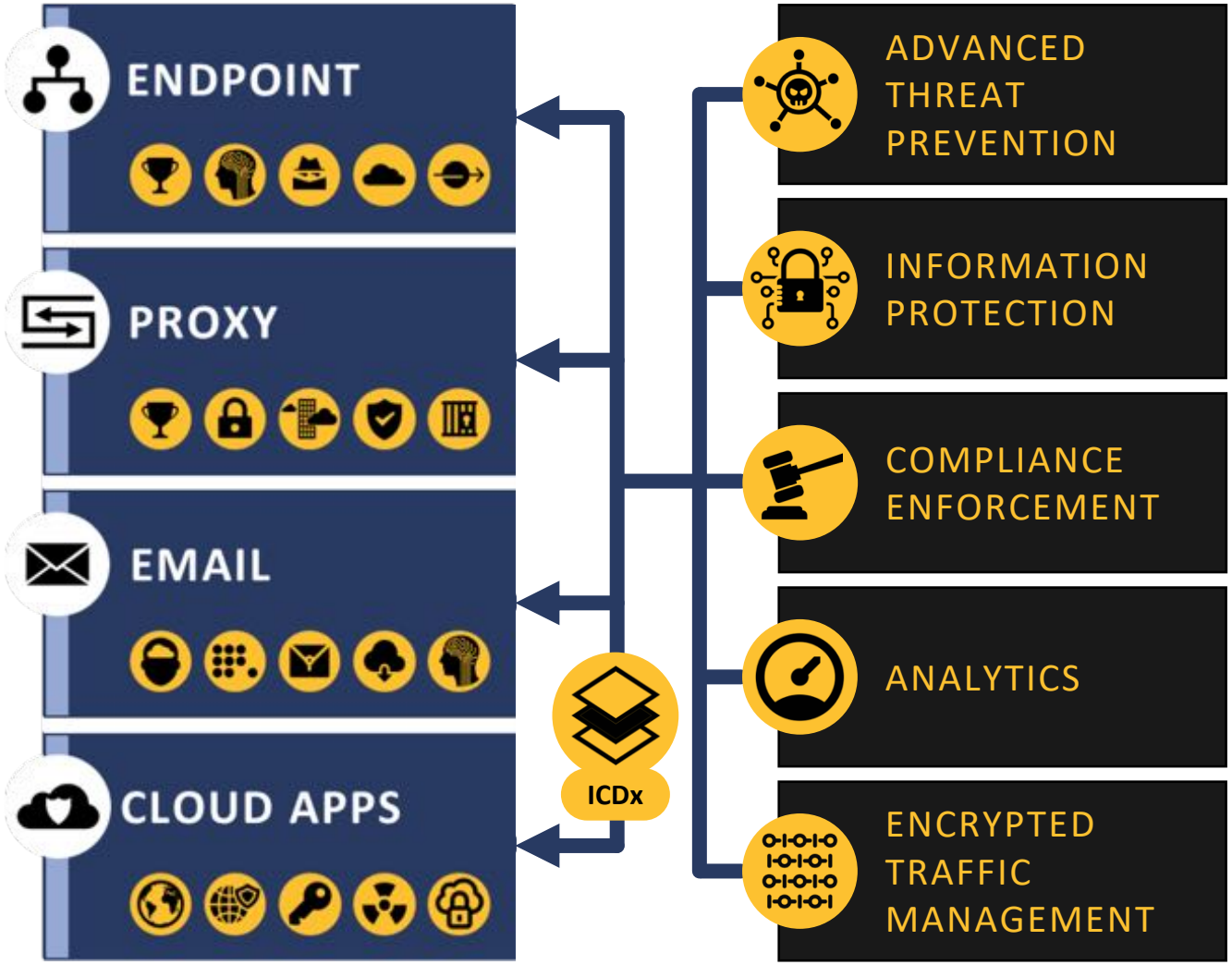
Delivering Technology Services in The Cloud Generation



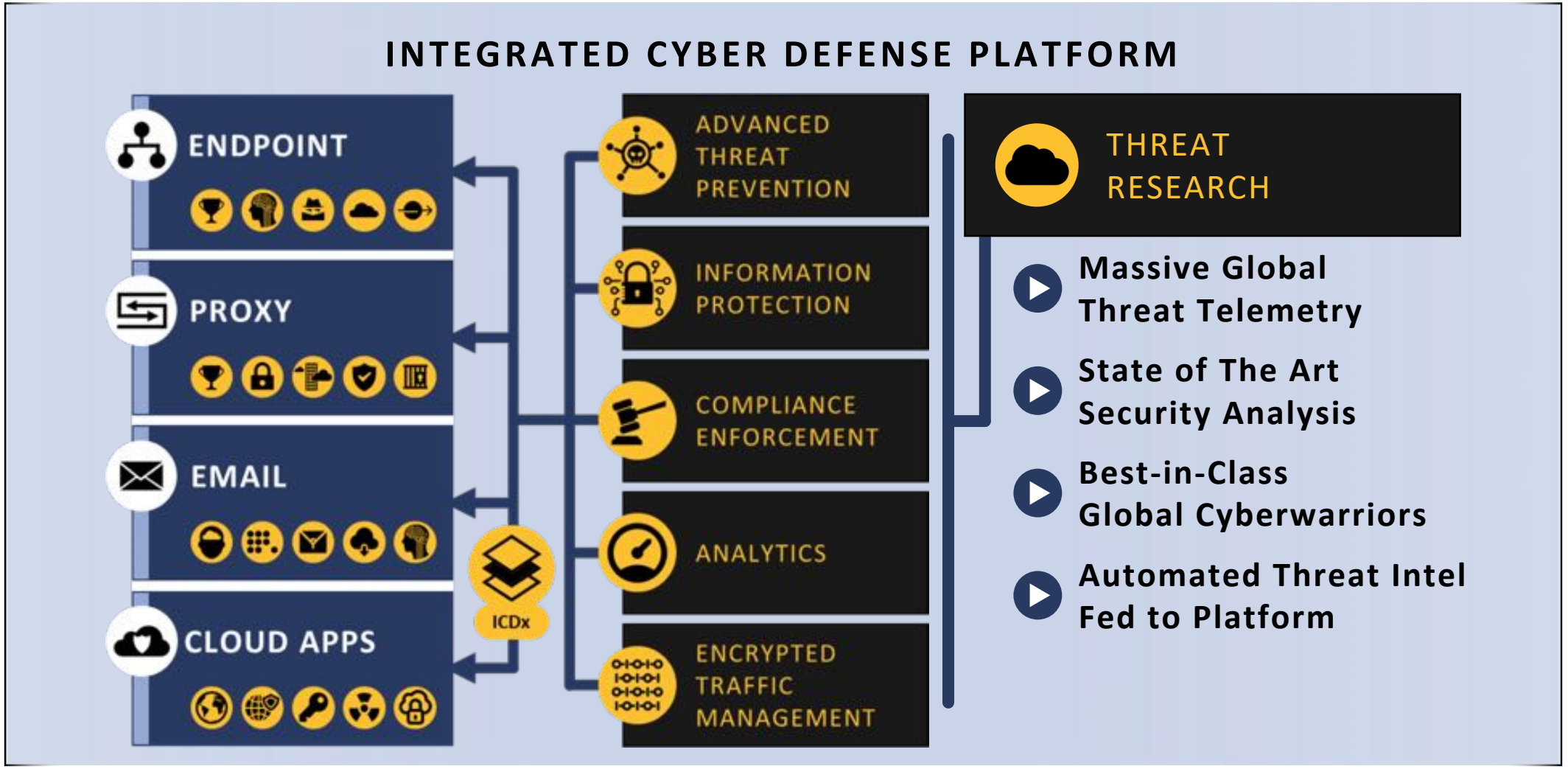
INFORMATION PROTECTION

- DLP
- Multifactor Authentication
- Encryption
- Information Centric Analytics
- Discovery and Compliance

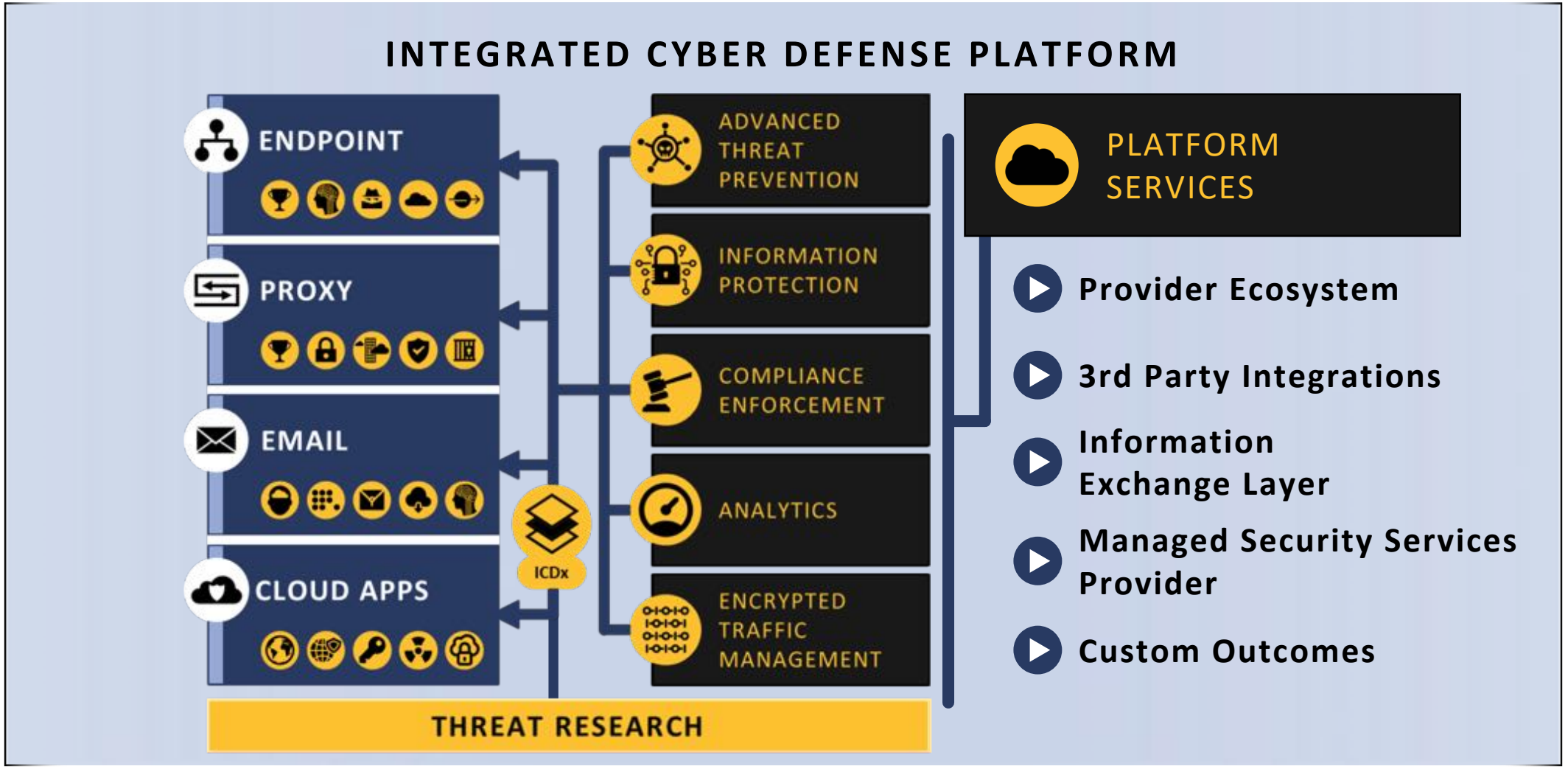
Delivering Protection in The Cloud Generation



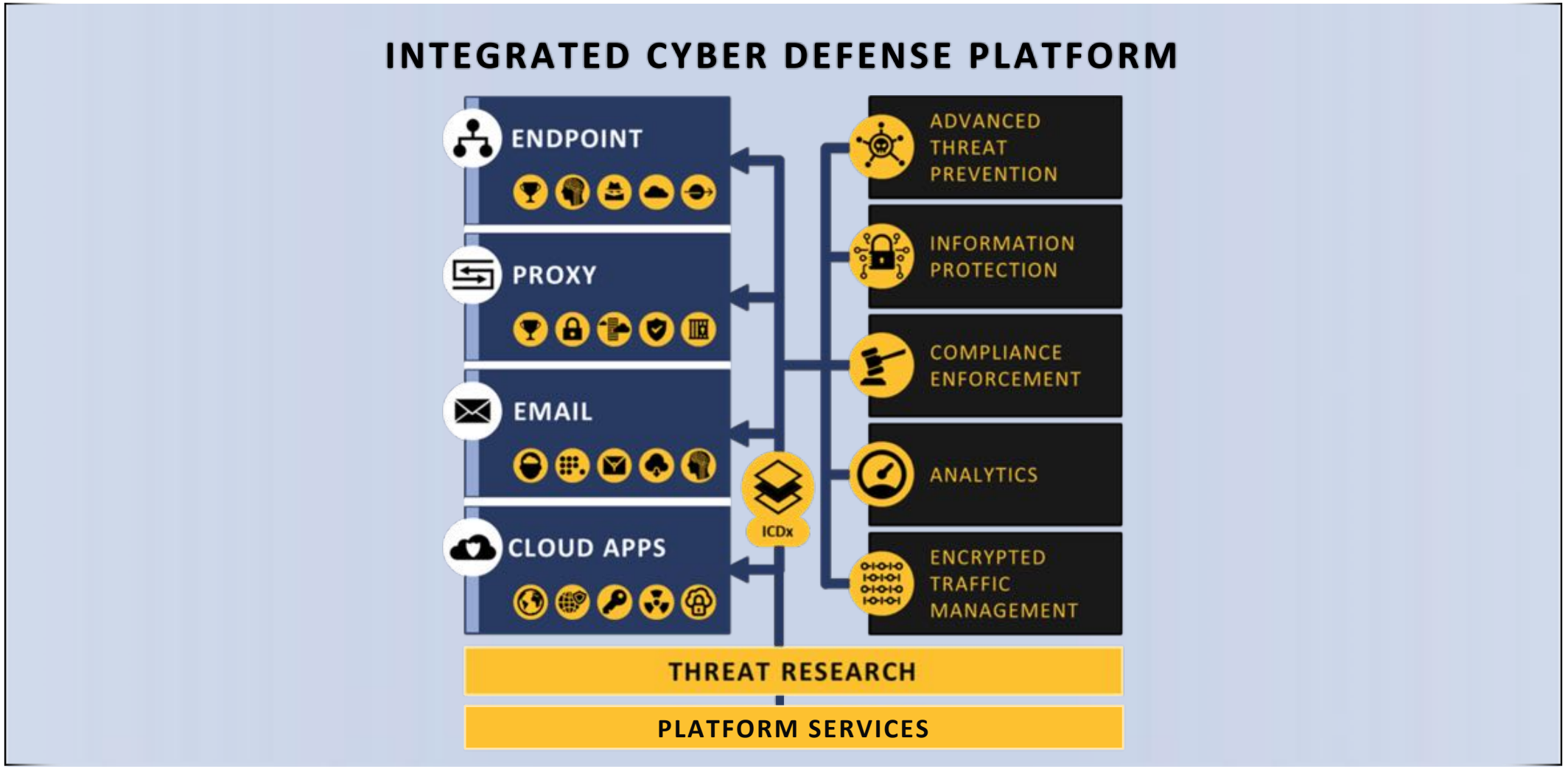
Delivering Protection in The Cloud Generation



Delivering Protection in The Cloud Generation



Delivering Protection in The Cloud Generation

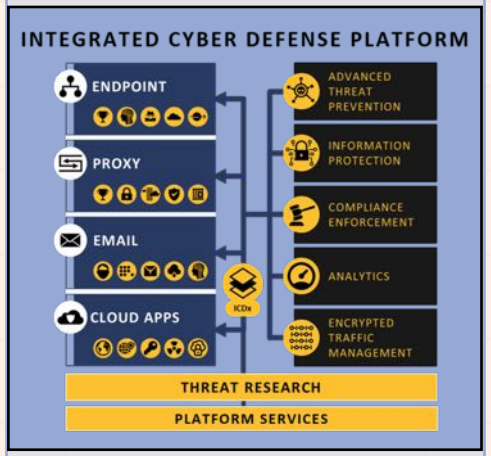


600+ PARTNERS INQUIRIES → **94** TECHNOLOGY PARTNERS → **178** INTEGRATIONS

A10 Networks
AASHTO
Accellion
AGARI
AGAT
Allure
Area 1
Banco de Bogotá
Attivo Networks
boldonjames
Centrify
Compuverde
Citrix
CloudGenix
ctera
cyber observer
cpacket networks
Cybersponse
Cymulate
DB Networks
Dell EMC
docker
Echoworx
exabeam
f5
Fidelis Cybersecurity
Flexera Software
Hitachi
gradian
indeni

Symantec TIP PROGRAM ACCESS

Bay Dynamics
Cisco
CounterTack
Demisto
Dropbox
FireEye
ForeScout
Fortinet
gemalto
Google

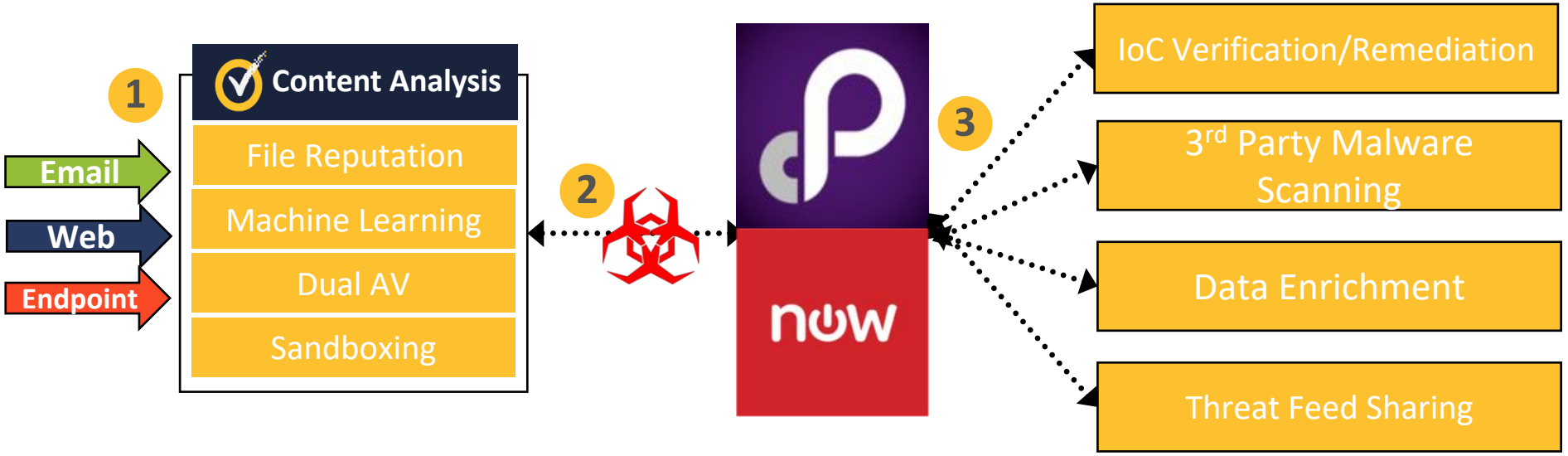


amazon web services
splunk>
servicenow
box
IBM
Microsoft

vmware
VENAFI
REVERSINGLABS
radware
Qualys.
Phantom
ORACLE
lastline
NetApp
MICROFOCUS

Intsights
ipswitch
ixia
LogRhythm
McAfee
MetaNetworks
MobileIron
napatech
NETSCOUT
NCR
NETDIALOG
NUTANIX
opentext
redhat
RSA
Pulse Secure
SAP
salesforce
silverpeak
slack
SOPHOS
SWIMLANE
SYMPHONY
THALES
thycotic
TITUS
tufin
VARONIS
VERSA NETWORKS
yammer

Data Flow – CA / Orchestration Vendor Integration



Symantec

Carbon Black.
Carbon Black Response

Symantec
Symantec Endpoint Protection

FireEye
FireEye

cuckoo
Cuckoo

virustotal
VirusTotal

OPSWAT Metadefender
Metadefender

CROWDSTRIKE
Streaming API

Hewlett Packard Enterprise
ArcSight ESM

200 + Integrations

1. Malicious file is discovered via CA
2. Malicious file/meta is sent to Orchestration Vendor
3. Orchestration Vendor executes on the Symantec Playbook
4. If needed, threat intel shared with Symantec for blacklisting purposes

The Cloud Generation Dilemma

Changing Usage Models Will Mandate Cloud Generation Architecture

Cloud Security Chaos

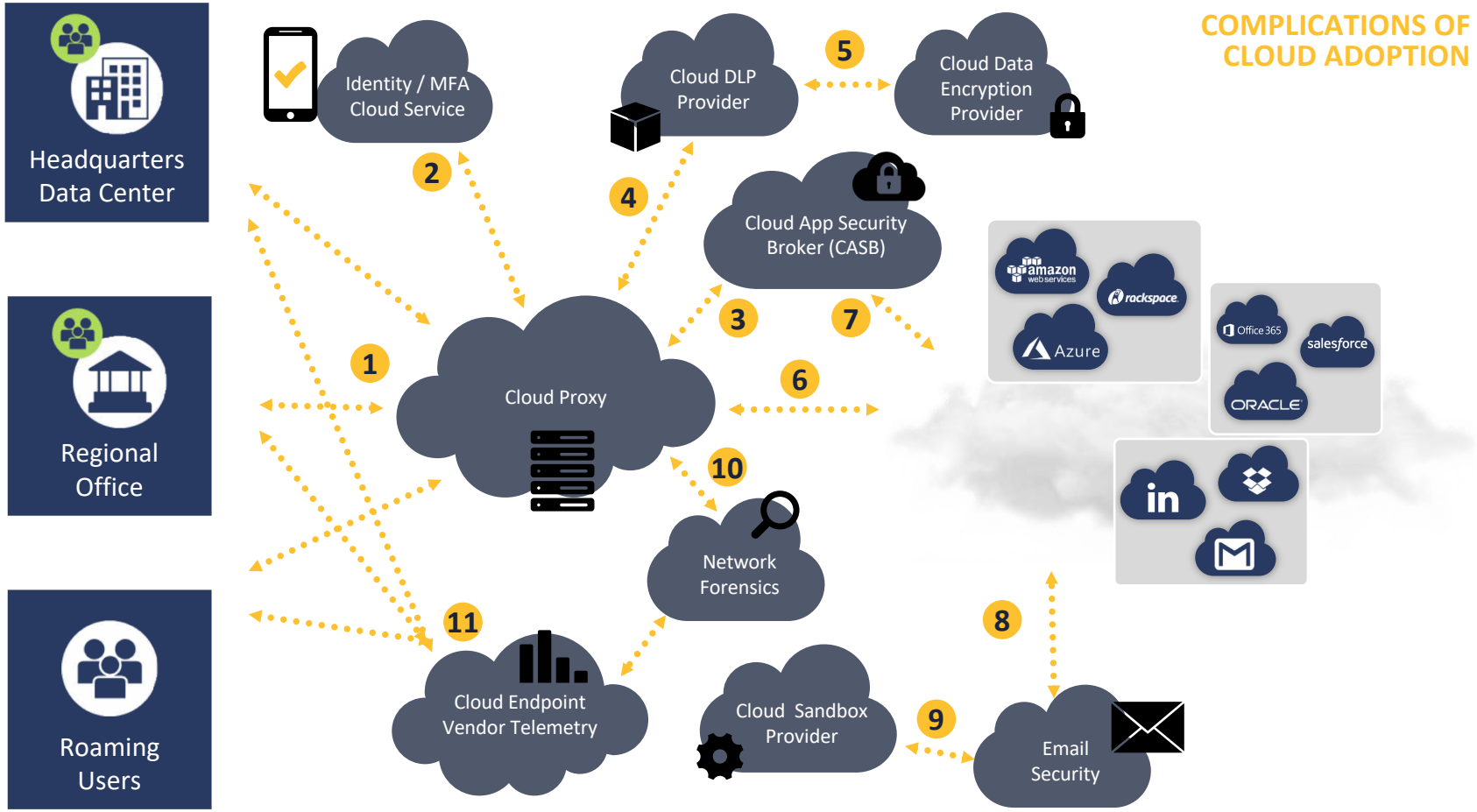
Challenges of Disparate Cloud Security Providers

COMPLICATIONS OF CLOUD ADOPTION

1. Connect to Cloud Proxy
2. Authenticate the connection
3. Validate user access to cloud application
4. Inspect document upload for sensitive material
5. Encrypt document due to sensitivity
6. Document uploaded into cloud app
7. Content is classified and tagged inside of cloud app
8. Email sent to user confirming document receipt
9. Threat inspection performed on email content
10. Full packet capture forensics
11. Endpoint activity telemetry

Cloud Security Chaos

Challenges of Disparate Cloud Security Providers

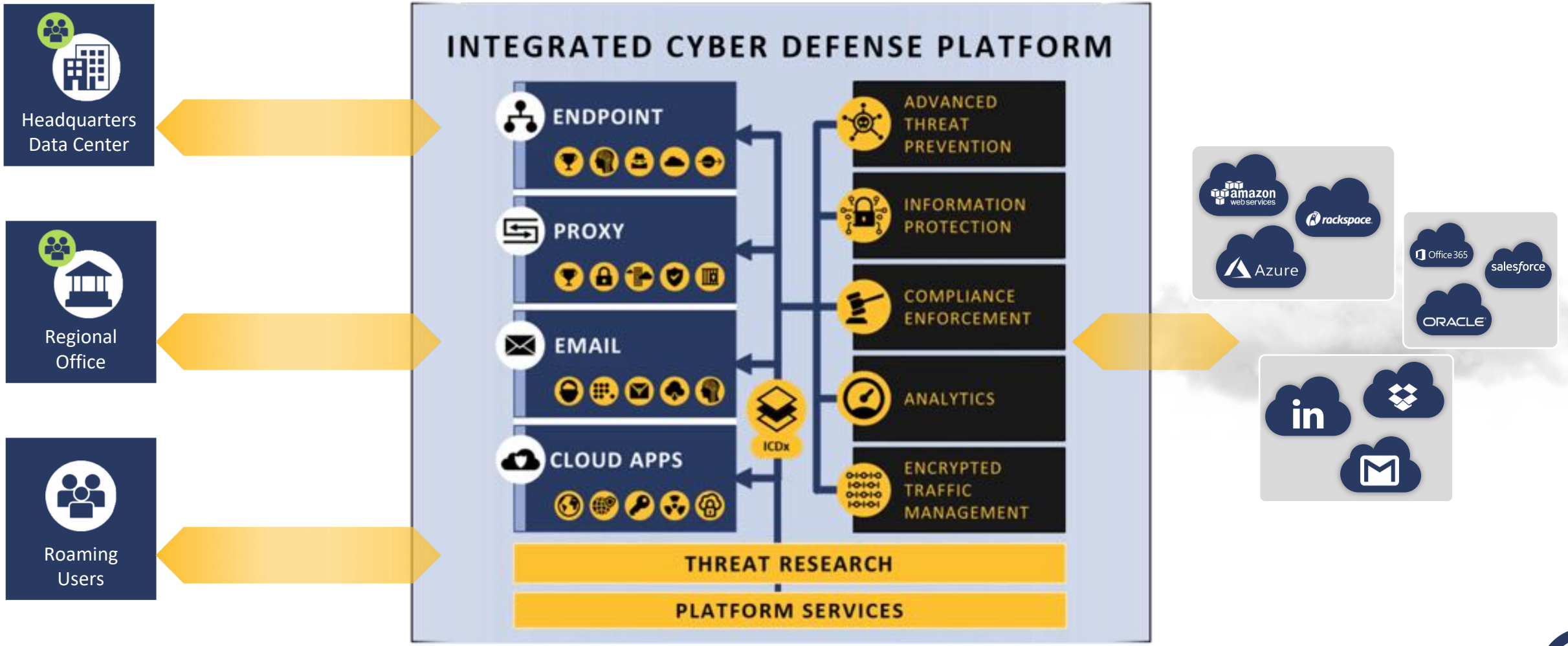


COMPLICATIONS OF CLOUD ADOPTION

- Who Owns the Comprehensive Service Level Agreements?
- Single Pane of Glass?
- Redundancy & High-Availability?
- Vendor Compatibility?

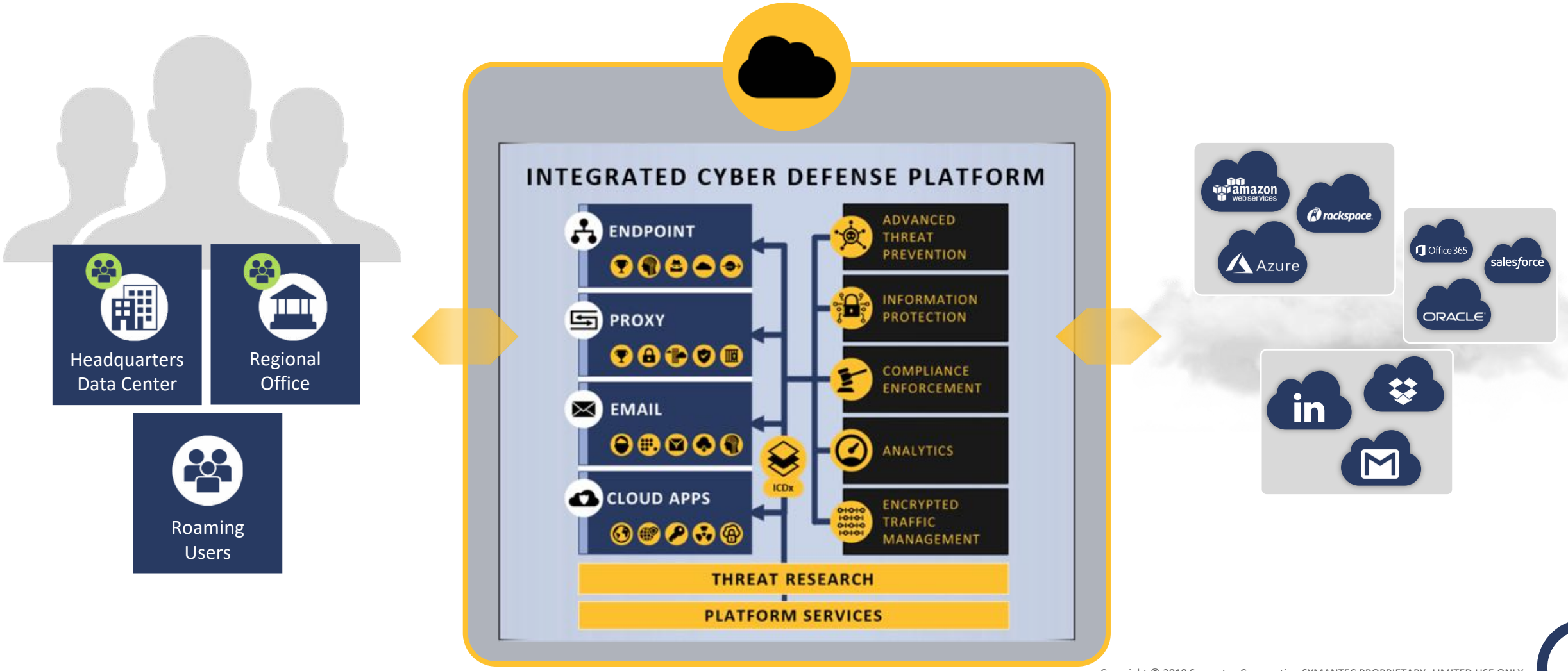
Symantec Integrated Cyber Defense

Delivering a Simplified Security Model for the Cloud Generation



Symantec Integrated Cyber Defense

Delivering a Simplified Security Model for the Cloud Generation




Symantec