RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SPO1-W04

Get Your Head in the Cloud: A Practical Model for Enterprise Cloud Security

Nicolas Popp

SVP Information Protection

Symantec Corp

#RSAC

Cloud security – Only five years ago!

From Love to Trust…

Certainly not a fad

Office 365

2015 Revenue
~ 0.7 Billion

amazon web services

2015 Revenue
~$ 9 Billion

Why it this happening?

AGILITY®

What cloud security is about

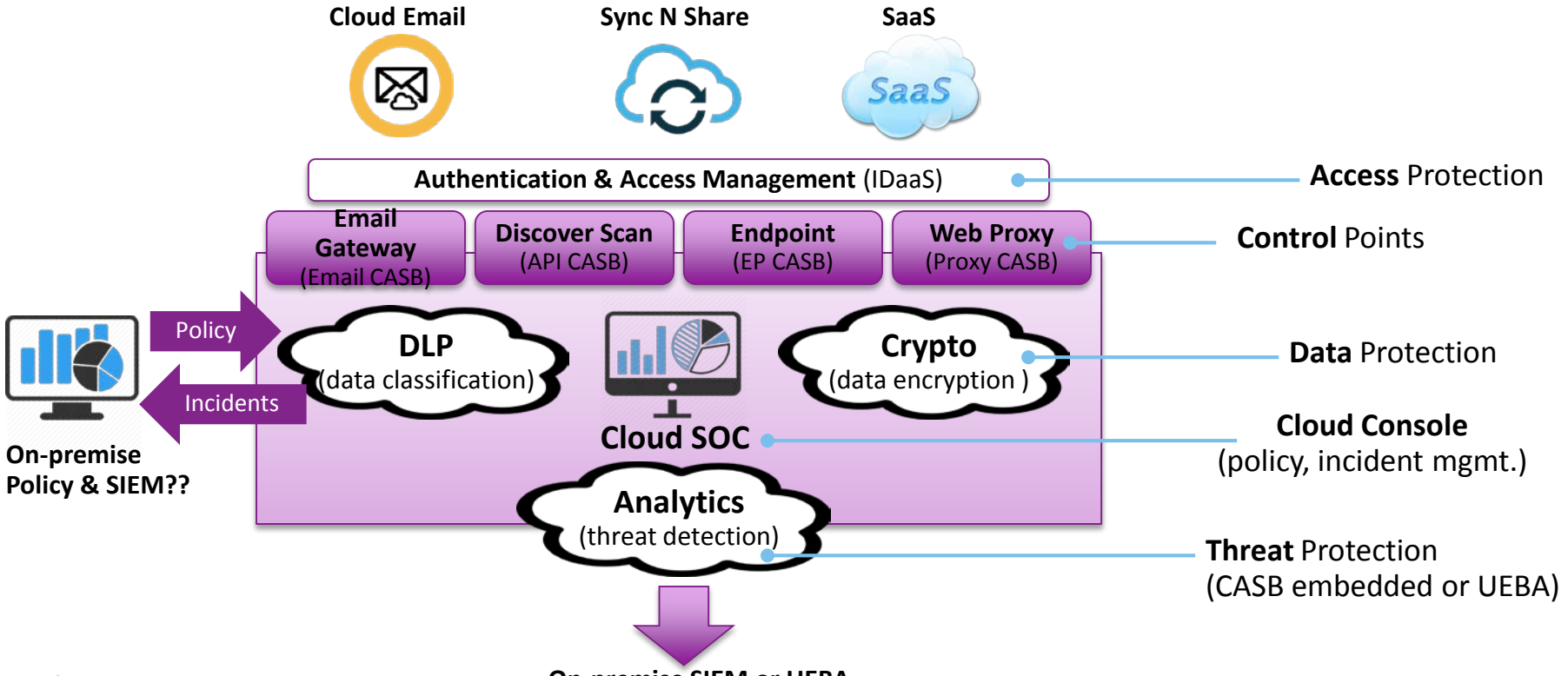
SECURITY FOR CLOUD APPS (CLOUD ACCESS SECURITY BROKER)	SECURITY FOR CLOUD INFRASTRUCTURE (CLOUD DATA-CENTER SECURITY)	MANGING SECURITY FROM THE CLOUD (CLOUD SOC)
Sensitive data is stored in SaaS apps – authorized as well as unauthorized apps, sometimes beyond the visibility or control by IT	Native security offered by IaaS vendors is inadequate: Shared responsibility model for security	Managing security has become complicated by multiple solutions and need for frequent updates.

Use Cases: SaaS Security is about the data (not the network)

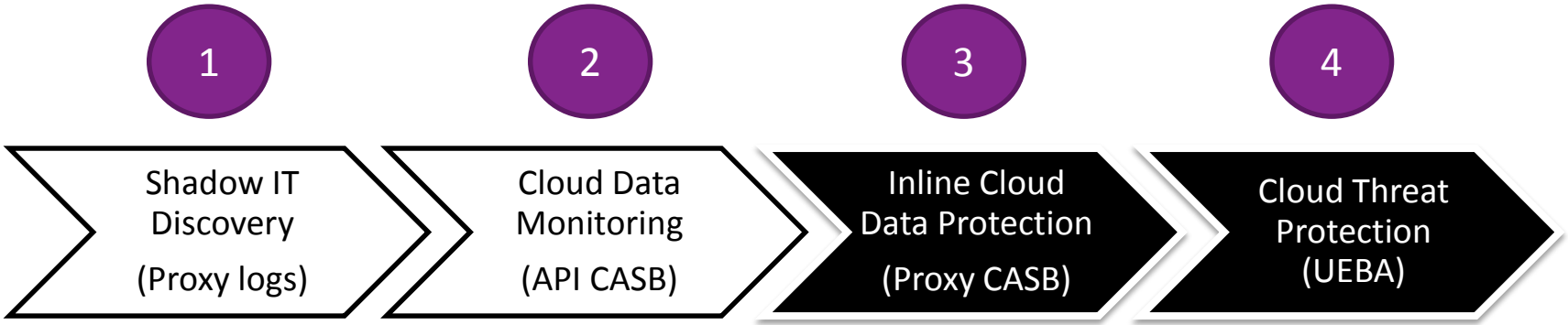
"SaaS security is identity an data centric not network centric"

- **Identity & shadow IT**
  - How do I authenticate, provision , de-provision users ?
  - What unauthorized risky cloud service are being?
- **Data Protection**
  - **What** are my users storing in the cloud?
  - **What** are they downloading from the cloud?
  - **What** are they sharing in the cloud?
  - How can I protect my critical cloud?
- **Threat protection**
  - How do I detect and prevent threat activity in the cloud?

SaaS Security: The Cloud Access Security Broker



Deployment phases & technologies



Seeing is believing

- Email CASB

Inline protection of outbound messages from O365 Exchange using cloud DLP and cloud encryption

- API CASB

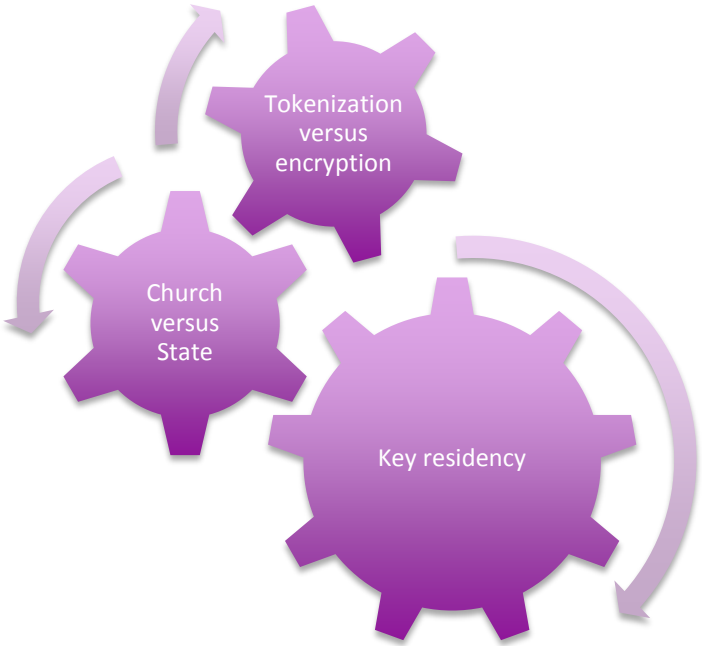
Discovery of confidential data at Box by scanning data at rest through the BOX APIs

The CASB contenders

CSP	CASB	DLP/Web Sec	Network Sec
You do not need one. I will provide all the security for my cloud (Amazon, SFDC) and beyond (MSFT)	The security guys cannot execute. You need a brand new control point for the cloud	The perimeter is dead. Simply extend traditional DLP and web security controls to the cloud	The firewall (NG) remains the control point, just VPN back home or deploy virtually in the cloud

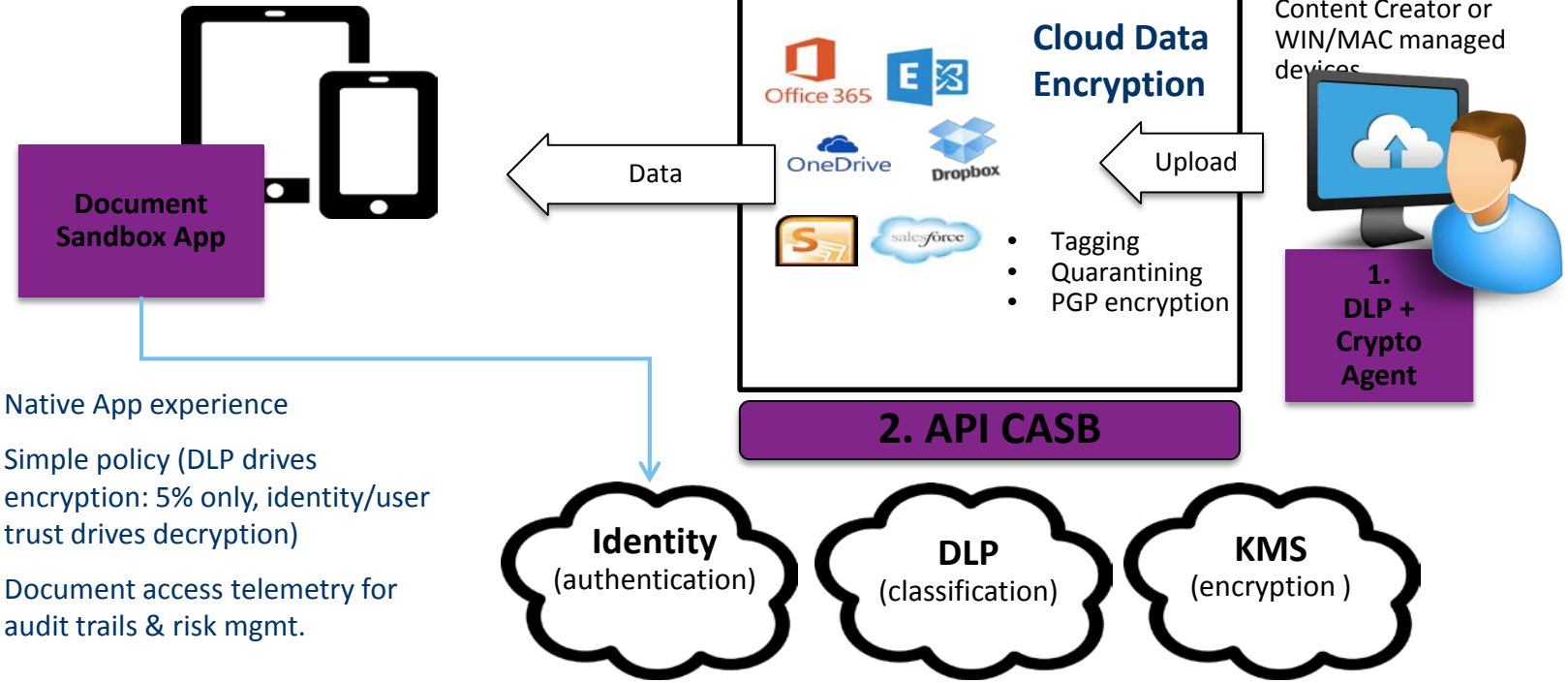
CloudProvider

Encryption: cryptic crypto key issues



- **Guiding principles**
  - Structured data belongs to the app, external encryption or tokenization is an “unnatural act”
  - Files travel across apps and are best served by external encryption (except for DAR)
- **Structured data encryption**
  - Compliance: let the CSP encrypt and enforce access policy
  - Data residency: the CSP should allow regional deployment
  - Trust: CSP should allow you to externally control the keys
- **Unstructured data encryption**
  - Key challenge: the data is more “mobile”
  - DRM versus Adaptive Encryption

Beyond DRM: adaptive encryption



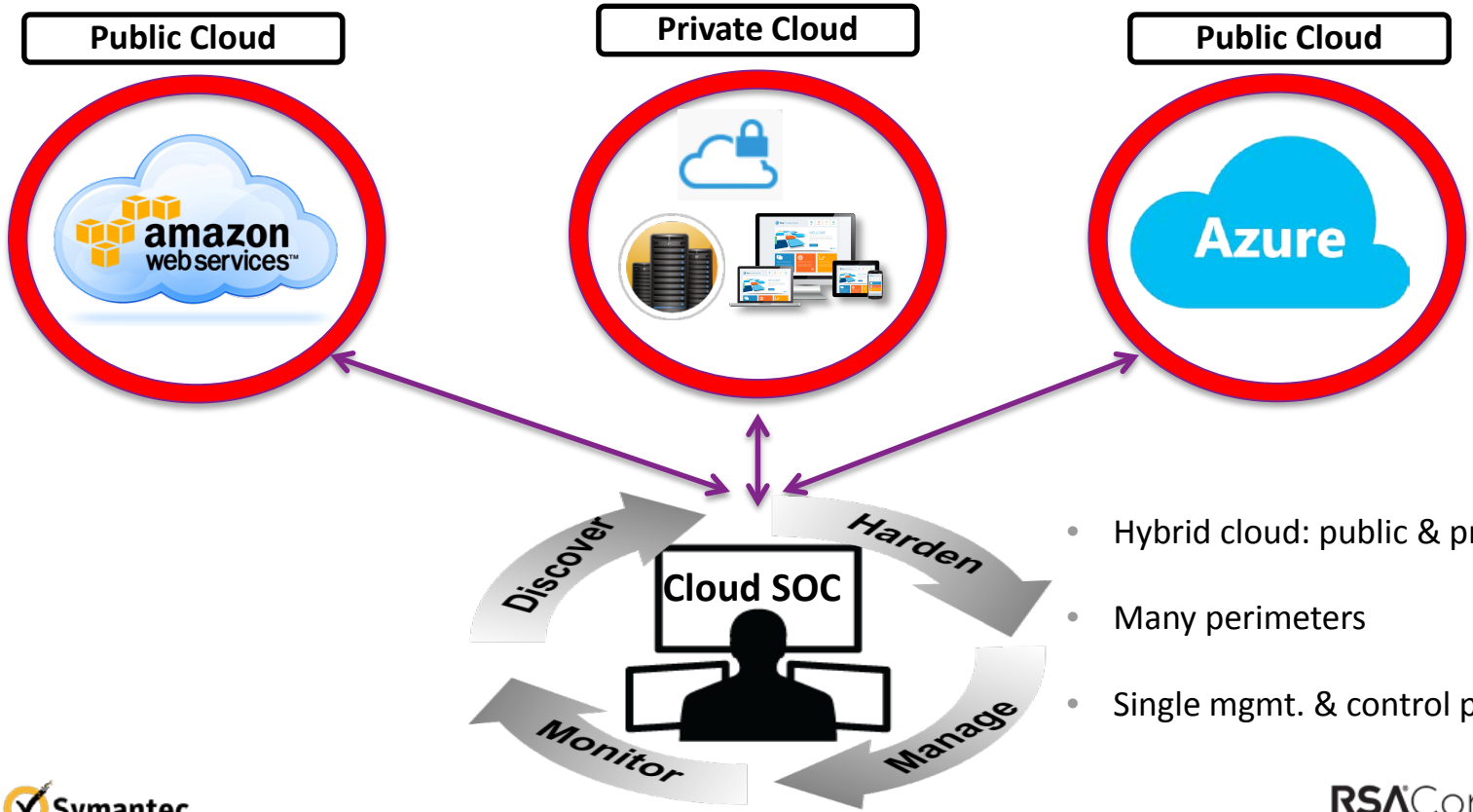
- Native App experience
- Simple policy (DLP drives encryption: 5% only, identity/user trust drives decryption)
- Document access telemetry for audit trails & risk mgmt.

Seeing is believing

- Cloud KMS & Encryption for Dropbox

Selective (content-aware) file-encryption in the cloud and mobile access by an external user, with transparent decryption based on authentication policy

IaaS: Protecting workloads across clouds



- Hybrid cloud: public & private
- Many perimeters
- Single mgmt. & control plane

Use Cases: Workload & network Centric

WORKLOAD PROTECTION

- What workloads are running in the cloud? What technology stack?
- How do I harden these workloads?
- How do I protect against vulnerability (patching)?

NETWORK PROTECTION

- How do I protect a multi-workloads system (EW segmentation)?
- How do I lock down my IaaS perimeters?

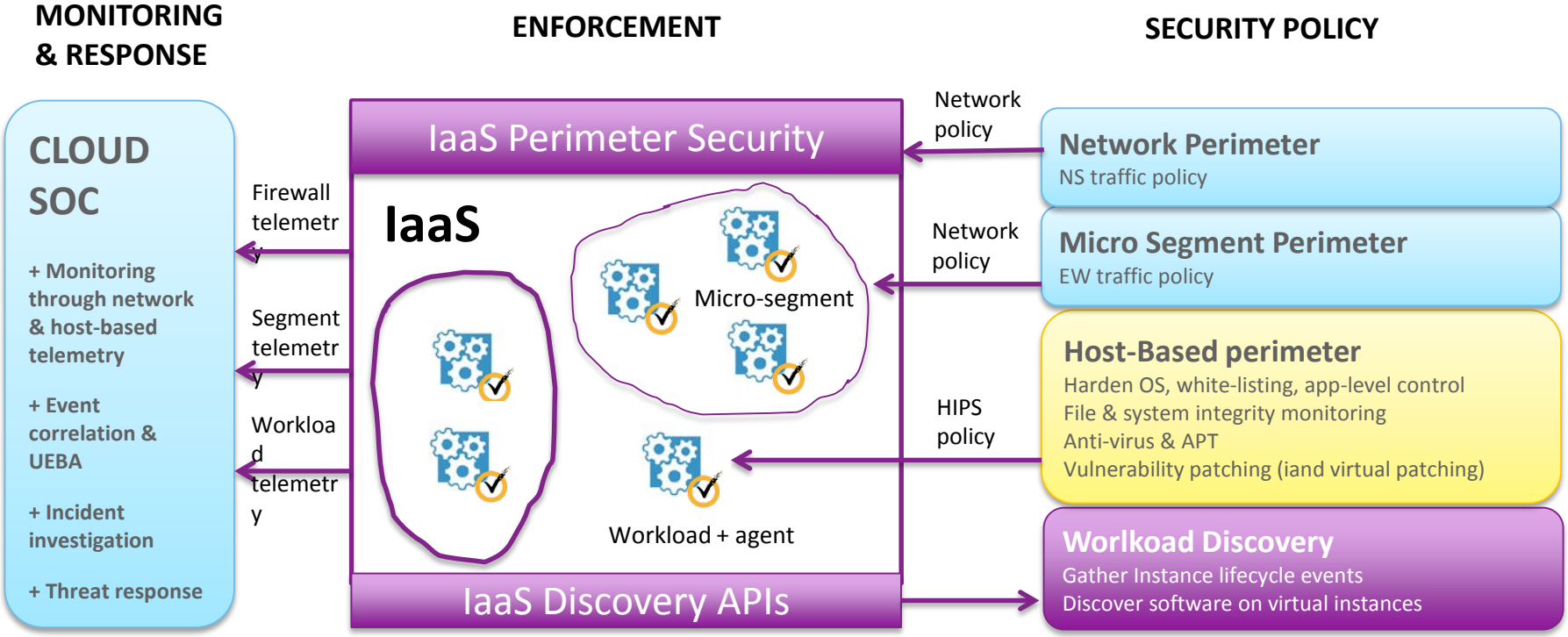
SOC MONITORING & RESPONSE

- How do I monitor all layers (workloads, segments, IaaS)?
- How do I detect threats from monitoring?

Automation (DevOps Integration)

- Workloads are templated and built
- Velocity of deployments (3 pushes a day to 100s of pushes a day)
- Security agents are part of orchestration
- Policy are suggested based on workload and workload interactions

The new perimeters

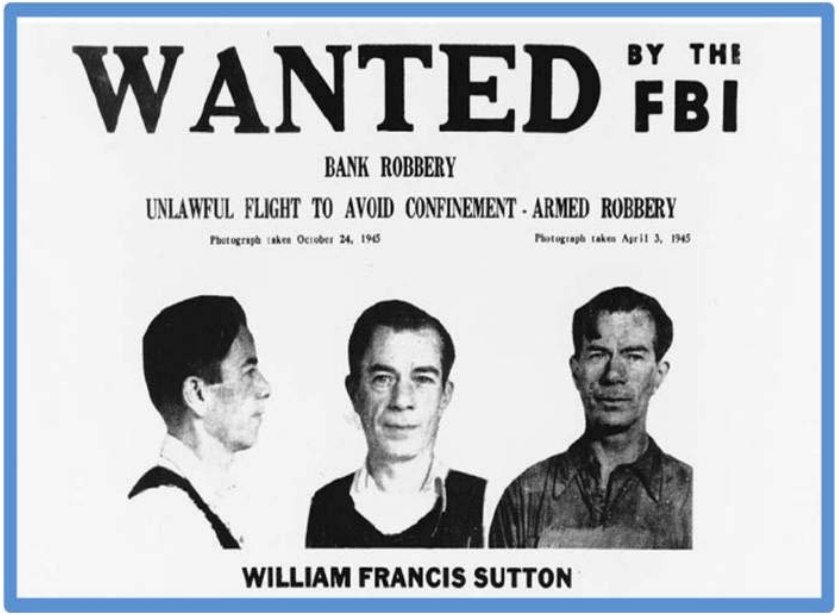


Seeing is believing

- Amazon Workloads Security

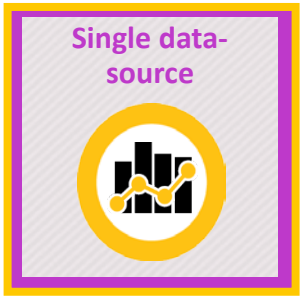
Discovering you amazon workloads and applying host and application level controls to protect them

The need for security analytics (UEBA)



- **Identity & data as new threat planes**
  - SaaS networks are opaque
  - From detecting bad IP addresses to bad users!
  - From netflow to data flow
- **Physical Scaling: SIEM versus Big Data**
  - Telemetry explosion
  - Open source architectures (Hadoop, Spark,…)
- **Logical Scaling: SIEM versus ML**
  - SIEM & Correlation rules: building a haystack
  - ML: finding the needles

UEBA: key concepts



User Entity Behavioral Analytics

- The **user** is the entity to **profile** and **risk-score**
- Refine risk score based on user **behavioral change**
- Refine risk score based on **peer comparison**
- **Correlate** across all user activity and behavioral anomalies

UEBA: Cloud threat detection example

12/9 Workday

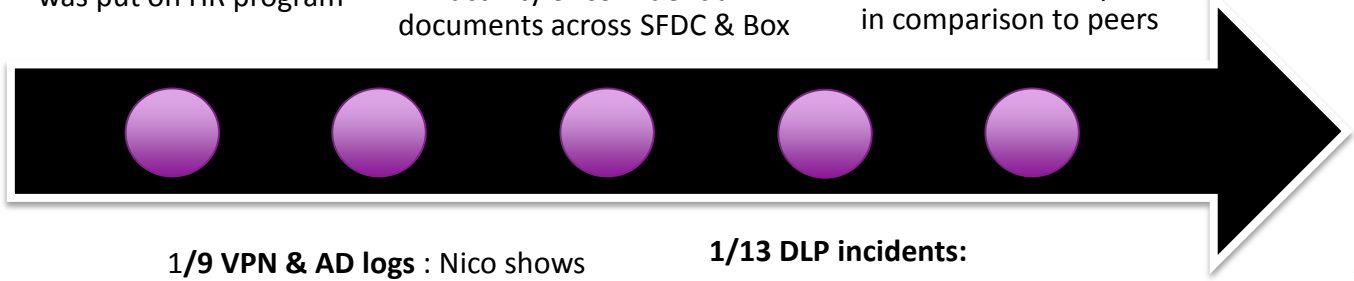
Nico had a bad review and was put on HR program

1/12 SaaS activity APIs:

Nico shows increased download activity of confidential documents across SFDC & Box

1/15: Firewall logs:

Nico shows abnormal bandwidth consumption in comparison to peers



Potential malicious insider

1/9 VPN & AD logs : Nico shows increased login activity and abnormal hours access (self & peer) across SFDC, Box, Workday

1/13 DLP incidents:

DLP incidents shows changed and abnormal data movements (print, personal email, removable media)

Will IaaS & SaaS security mgmt. converge?

Identity
(user & SaaS access)

Cloud Activity
(SaaS -level activity)

API CASB
(data at rest)

Proxy/EP CASB
(data in motion & use)

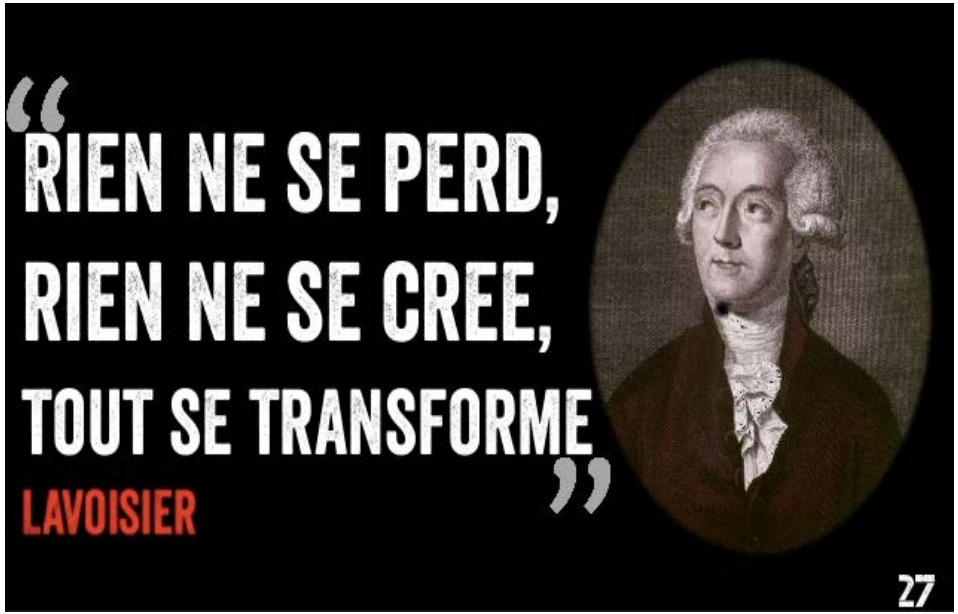
Privileged access events

Vulnerability & Threat intelligence

Virtualized workload activity

Virtualized network activity

Conclusion: cloud security is an evolution



- **From network to identity & data-centric security**
  - Says the DLP guy!
- **From one BIG to many smaller perimeters**
  - More perimeters with smaller diameters (containers, workloads,, micro-segments + user, device/app sandboxing, data encryption…)
- **From SIEM to Big Data security analytics**
  - The explosion and complexity of security telemetry drive the need for big data and machine learning in the SOC

Applying what you have learned

- **Develop a holistic cloud security strategy that includes:**
  - The protection of corporate SaaS applications
  - The protection of corporate workloads and systems running in public or private IaaS
  - New security management & monitoring services in the cloud
- **Plan for a Cloud Access Security Broker**
  - Evaluate a phased approach (access & discovery first)
  - Plan for active controls (DLP, encryption), understand implementation options (API, proxy, EP)
- **Understand IaaS workloads security**
  - The workload and SDN-centric security controls that compliance and security will require
- **Consider big data security analytics**
  - Integrate big data architectures & machine learning as part of your SIEM/SOC strategy