SHARE Session 14021

Protecting Critical Data on a z/OS Mainframe: A New Attitude

Paul de Graaff
Chief Strategy Officer

Vanguard Integrity Professionals
www.go2vanguard.com

AGENDA

Introduction

1 This part of the presentation discusses the current threat landscape and how enterprises are dealing with the challenges.

Challenges for z/OS

2 This part of the presentation discusses the challenges enterprises face with interpreting with integrating z/OS into their overall Security Intelligence Architecture and Operations.

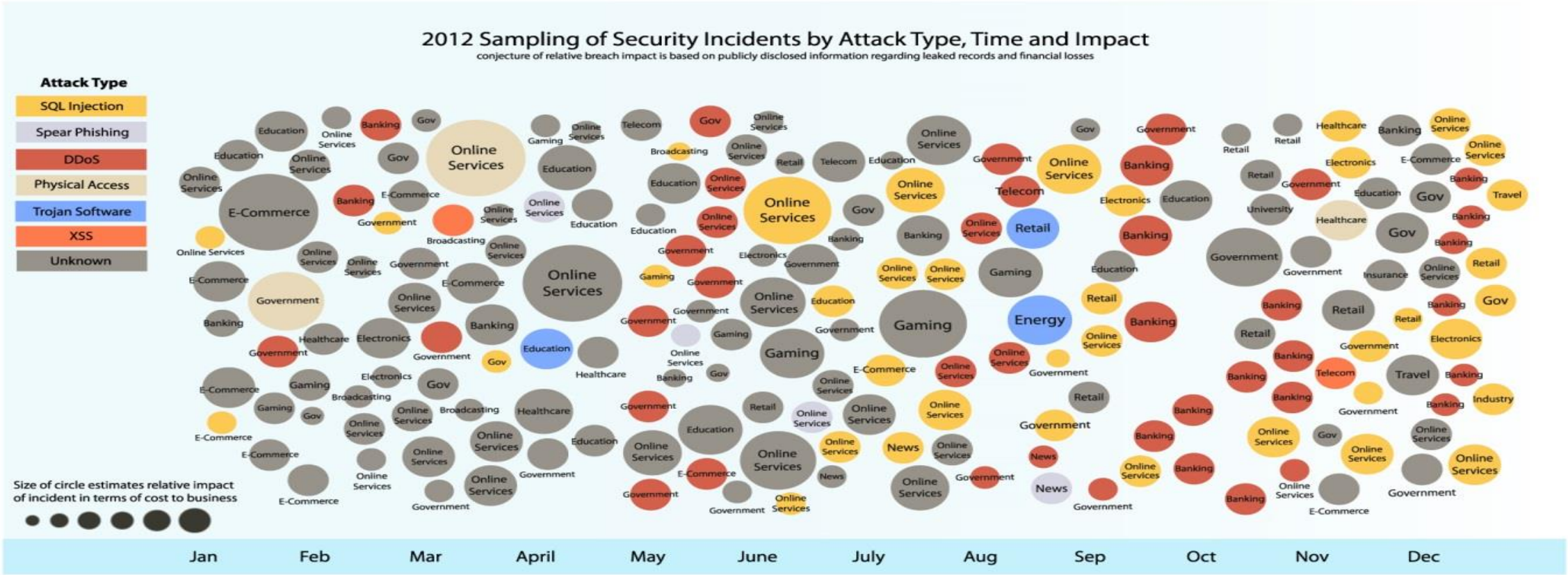
z/OS Security Intelligence Maturity Model

3 This part of the presentation shows how Vanguard looks at security intelligence and a proposal for a framework and maturity model for z/OS Security Intelligence.

Current Threat Landscape

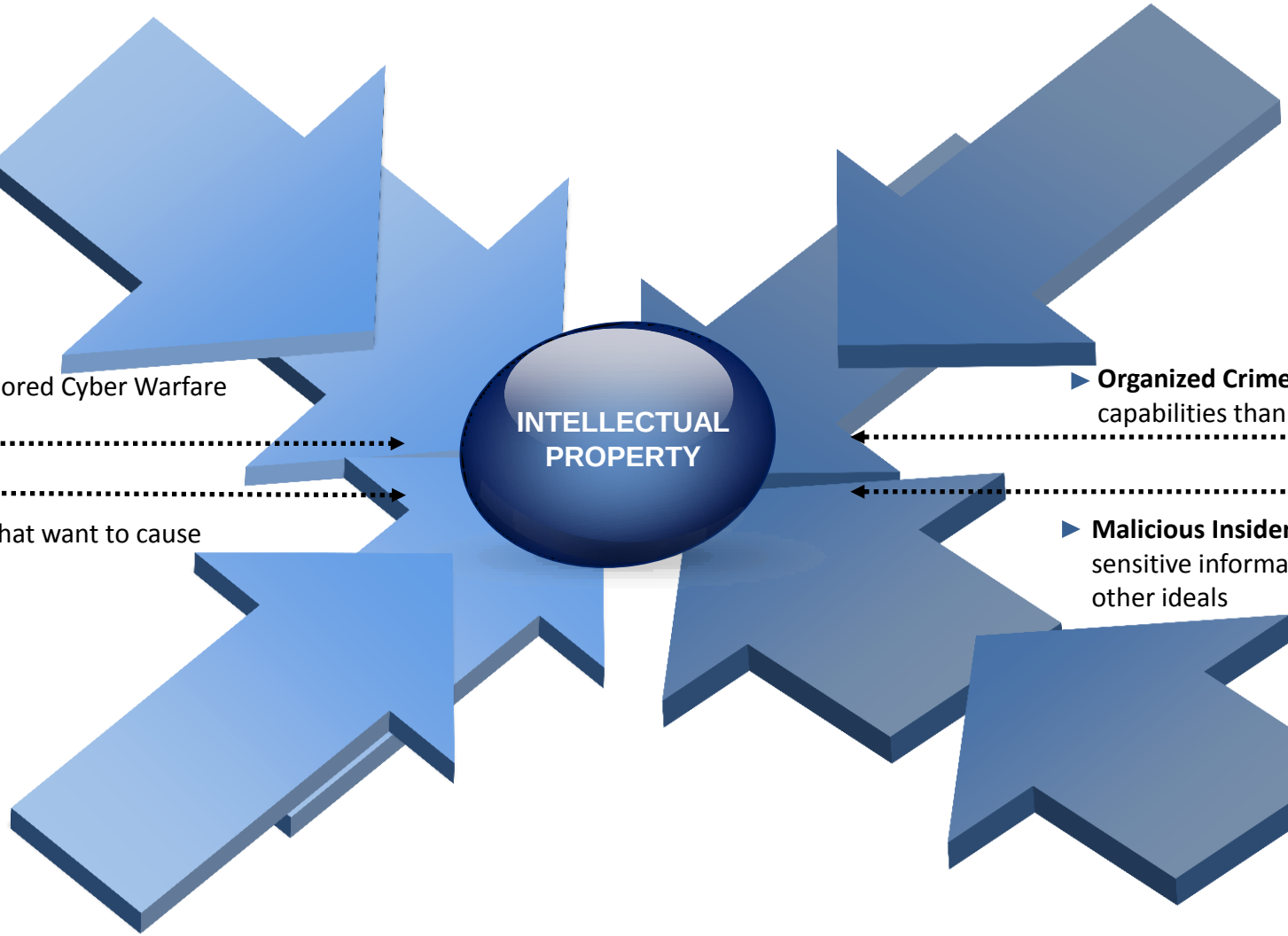
INTRODUCTION

Attack Statistics



Source: IBM X-Force® Research and Development

Threat Actors



- **Nation States:** State sponsored Cyber Warfare
- **"Hacktivism":** Individuals that want to cause harm for social reasons
- **Organized Crime :** less expensive using digital capabilities than physical
- **Malicious Insider:** people with access to sensitive information and using it for profit or other ideals

Sophistication

Low Level

- **Motivation:** Fun, nothing else to do;
- **Target:** anybody
- **Funding**: None

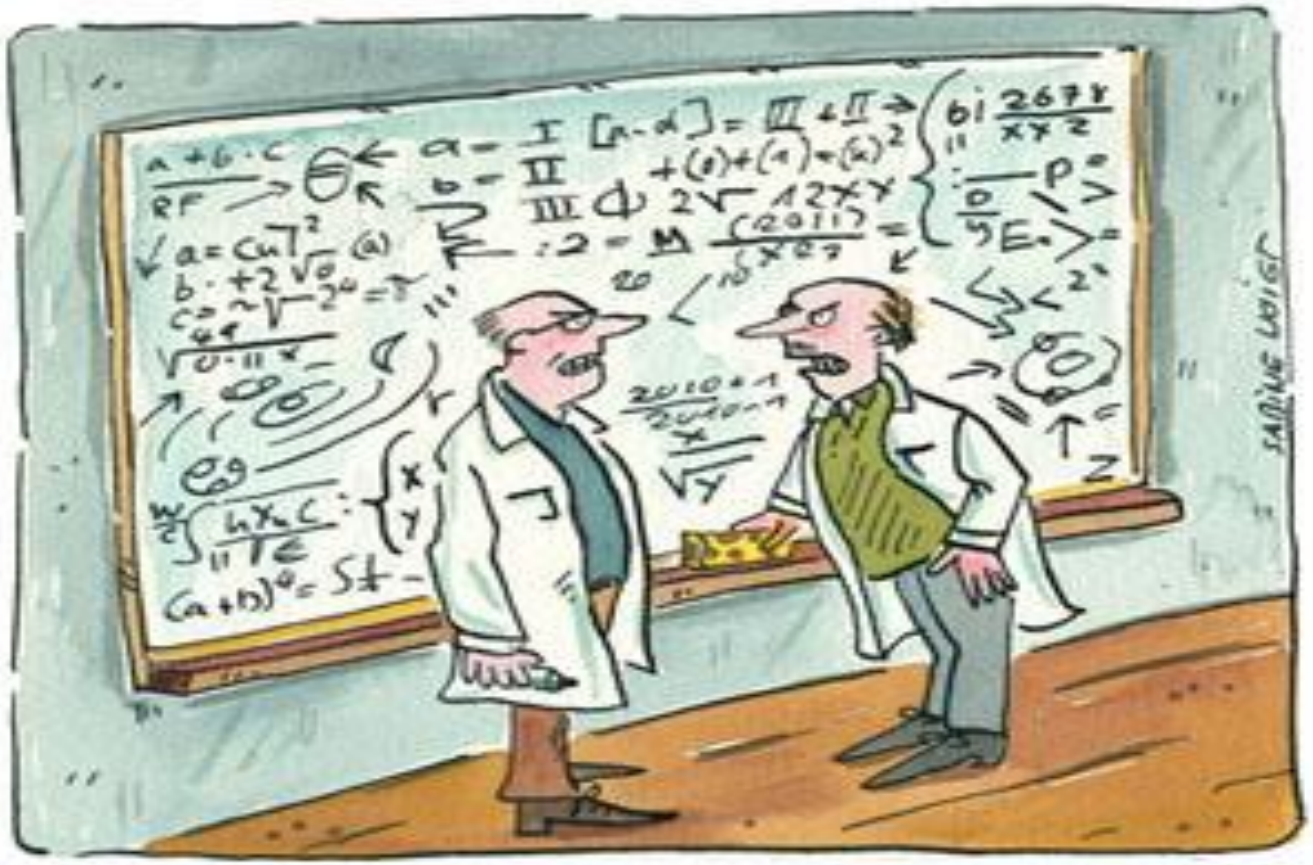
Medium Level

- **Motivation:** Reputation or Social;
- **Target:** Corporations, Governments, High Profile People;
- **Funding**: Limited funds but deep expertise;

High Level

- **Motivation:** Espionage, Influence, Trade Secrets, Inside Information;
- **Target:** Government Agencies, Contractors, Think Tanks, Corporations
- **Funding**: Well funded and deep expertise;

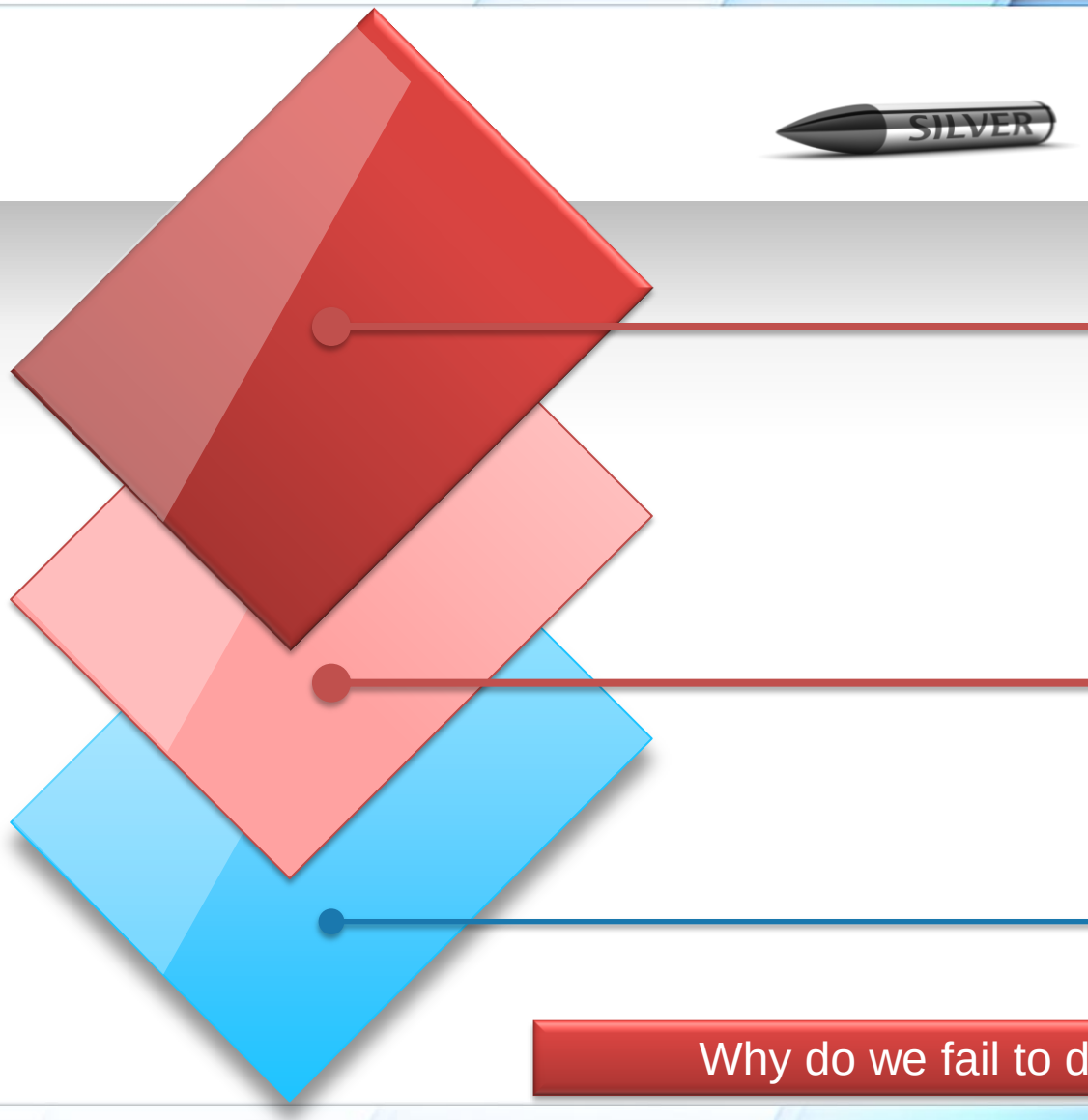
Sophistication



"If you think this is advanced, how do you expect to deal with APT?"

Traditional Security - Set of Layered Defenses

VANGUARD
Integrity Professionals
Enterprise Security Software



Preventive Controls
FW, IPS, WAF, DDoS, Awareness, Training

Detective Controls
IDS, AV, SIM, VA, etc

Corrective Controls / Response Procedures
IR Plans, BCP, DDoS

Why do we fail to detect / prevent APT type attacks?

Verizon Data Breach Report 2013

- Recommendations:
  - ***Ensure essential controls are met; regularly check that they remain so;***
  - Collect, analyze and share incident data to create a rich data source that can drive security program effectiveness;
  - Collect, analyze, and share tactical threat intelligence, especially Indicators of Compromise (IOCs), that can greatly aid defense and detection;
  - ***Without deemphasizing prevention, focus on better and faster detection through a blend of people, processes, and technology.***
  - Evaluate the threat landscape to prioritize a treatment strategy. Don't buy into a "one-size fits all" approach to security.
  - If you're a target of espionage, don't underestimate the tenacity of your adversary. ***Nor should you underestimate the intelligence and tools at your disposal***.

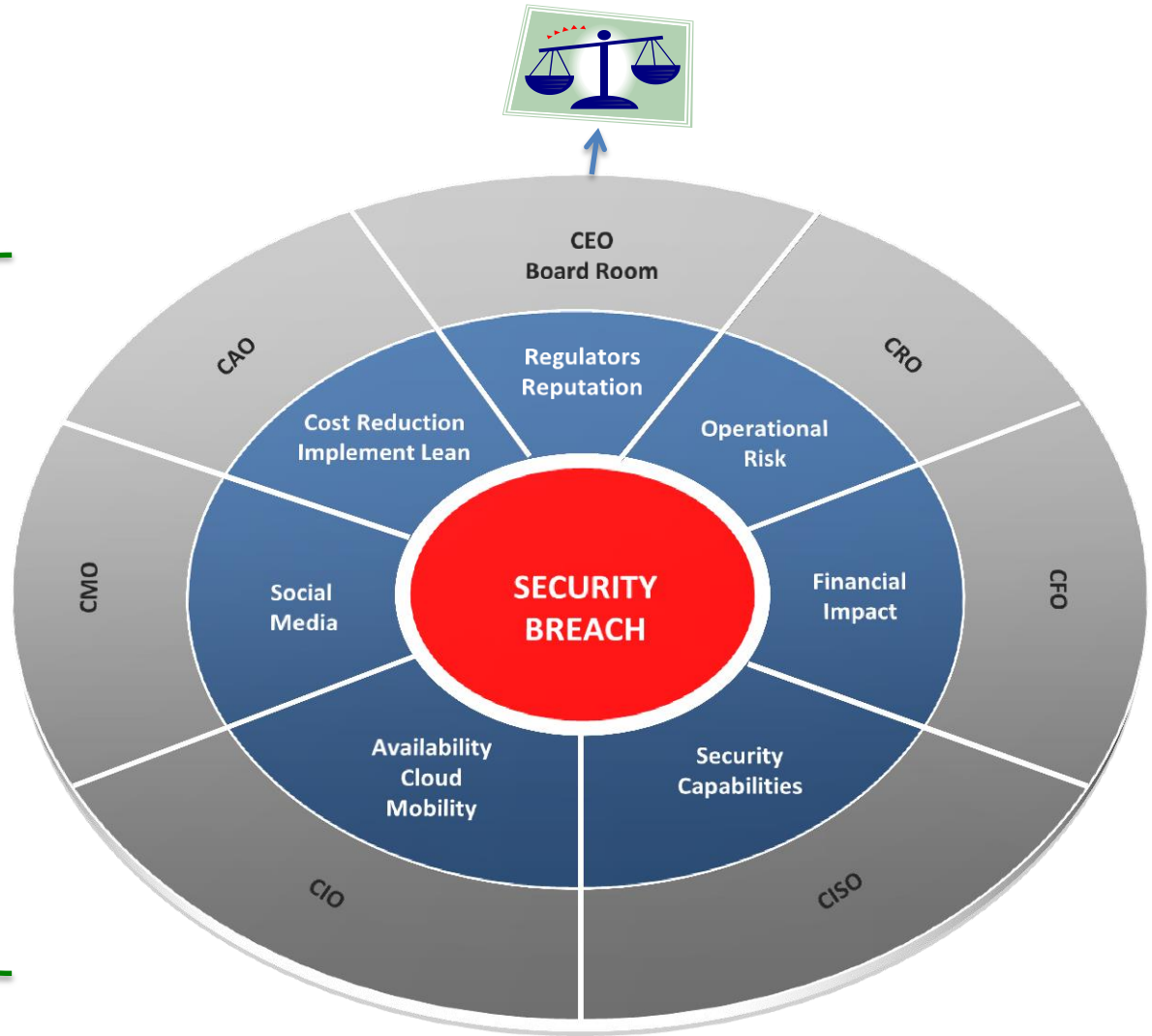
Note: subset of all recommendations

Security Intelligence and the z/OS Platform

ENTERPRISE CHALLENGES

Enterprise Challenges

Changes



Impacts

Security Challenges

VANGUARD
Integrity Professionals
Enterprise Security Software

Virtualization/Cloud
- Dynamic Workloads
- Cloud Bursting
- Elasticity

Security Intelligence
- Who wants to harm me
- What are they after?
- What methods are used?

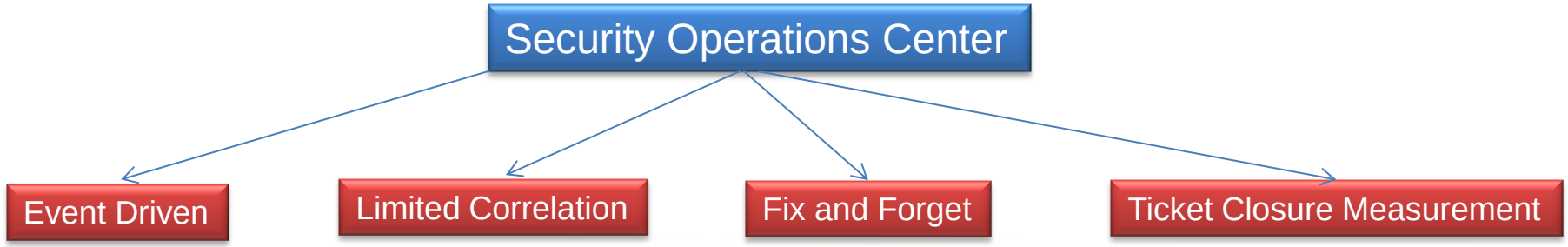
Mobility/BYOD
- Explosion mobile devices
- BYOD seen as cost saver
- Data Loss inevitable

Impact
- Where is my “data”?
- Requires *Dynamic* Security Controls
- High Audit Requirements

Impact
- Where is my IP?
- How is it protected and monitored ?
- Data Loss Prevention (DLP)

Impact
- Requires different set of IT services;
- Accelerates Cloud Adoption (Dropbox etc.)

Security Operations versus Security Intelligence (1)



Security Operations versus Security Intelligence (2)

VANGUARD
Integrity Professionals
Enterprise Security Software

SECURITY INTELLIGENCE .COM

sec•ur•ity in•tell•i•gence

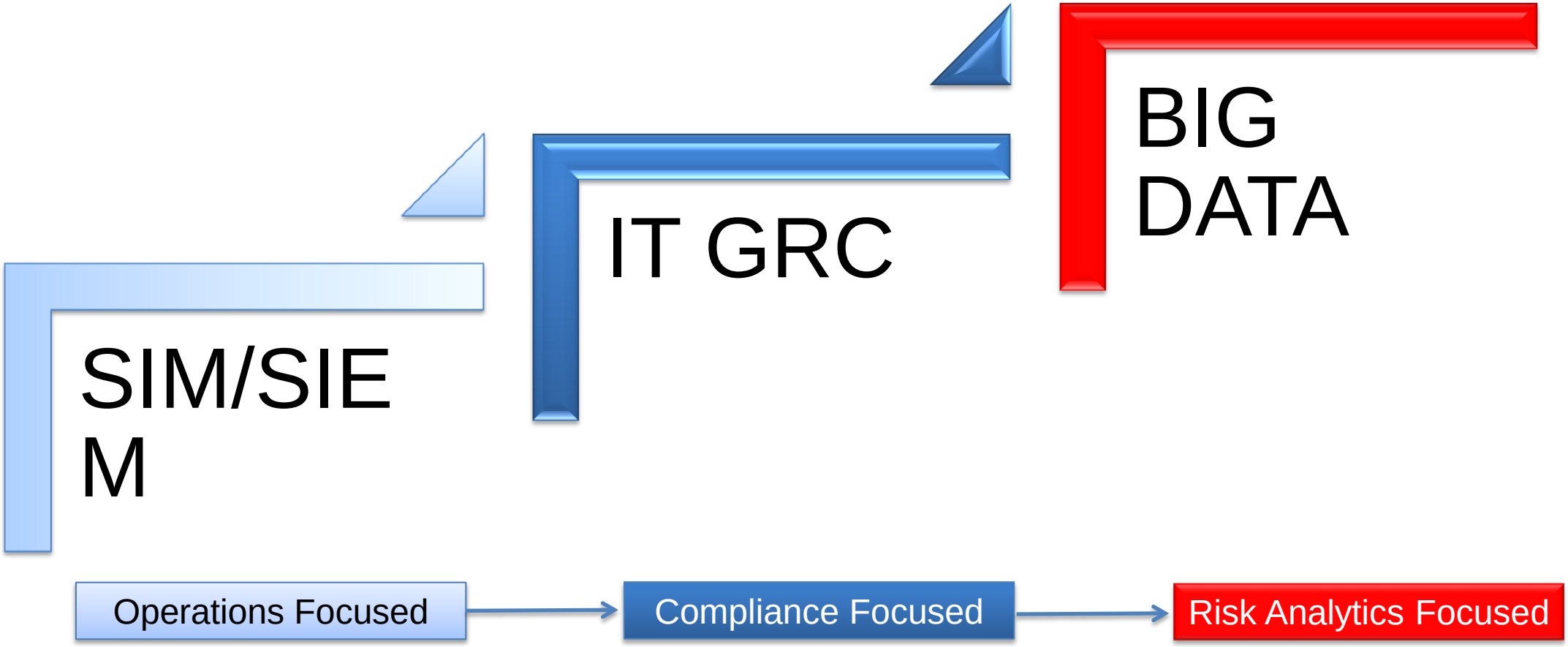
–noun 1. The real-time collection, normalization and alalytics of the data generaeted by users, applcations and infastructre that impacts the IT security and risk posture of an enterprise.

- Networks
- *Mainframes* & Servers
- Databases
- Applications
- Users & Identities
- Cloud
- Mobile

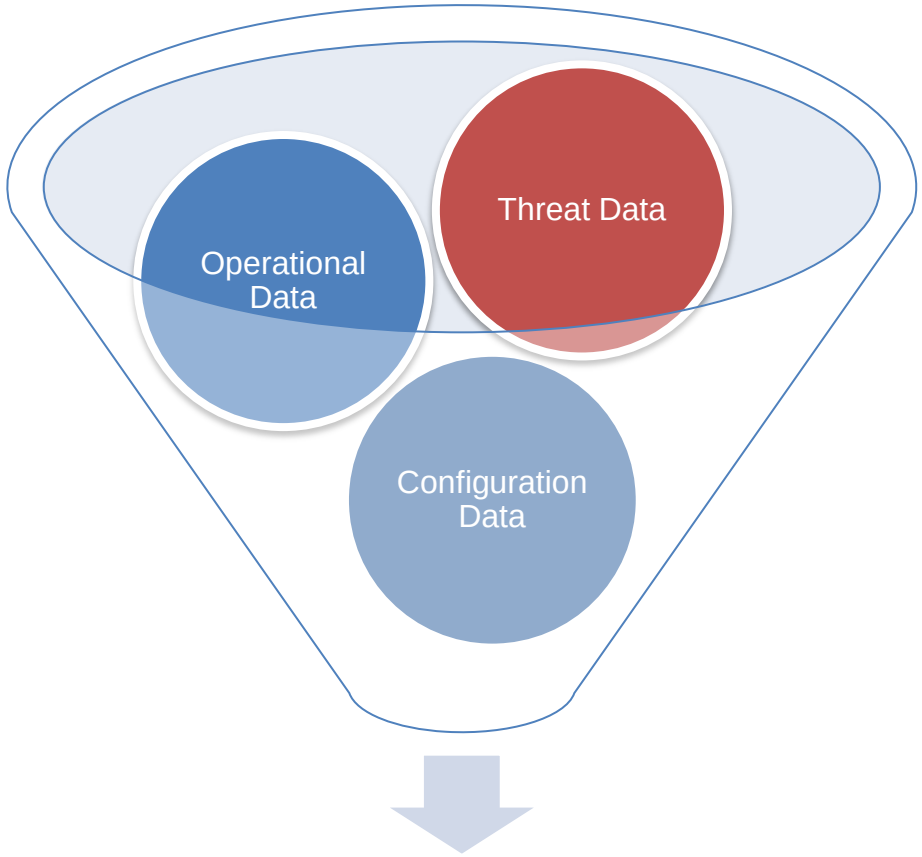
Security Intelligence:

- Contextual aware;
- Correlated and aggregated event;
- Isolate and understand attack behavior;

Security Operations versus Security Intelligence (3)



Security Intelligence

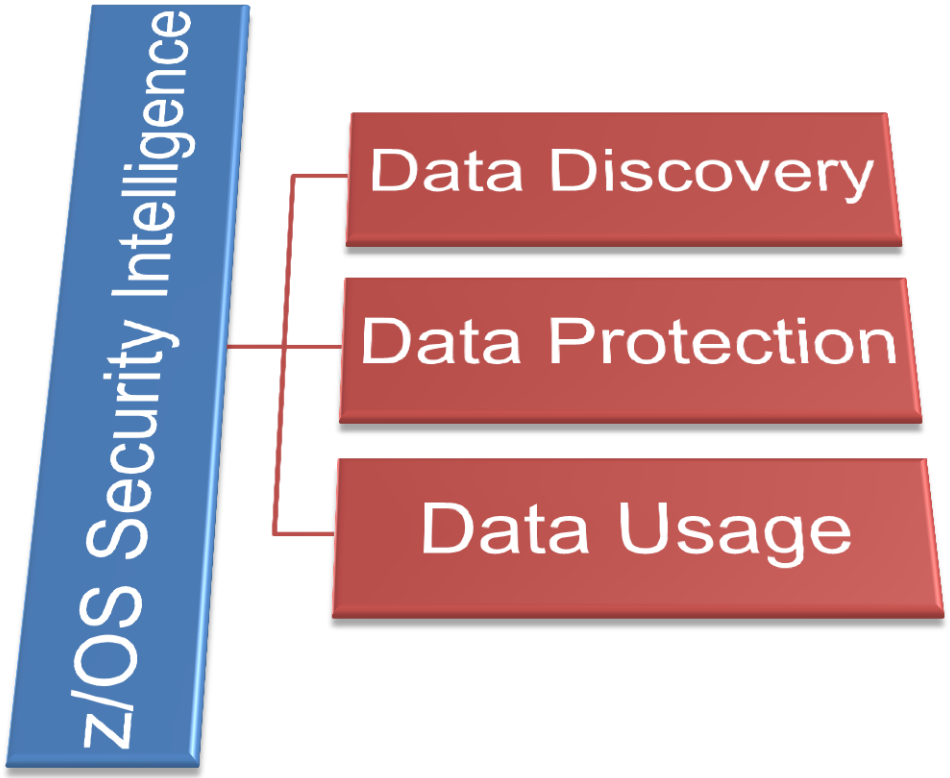


Security Intelligence

Framework and Maturity Model

Z/OS SECURITY INTELLIGENCE

Security Intelligence and z/OS – How do they fit together?

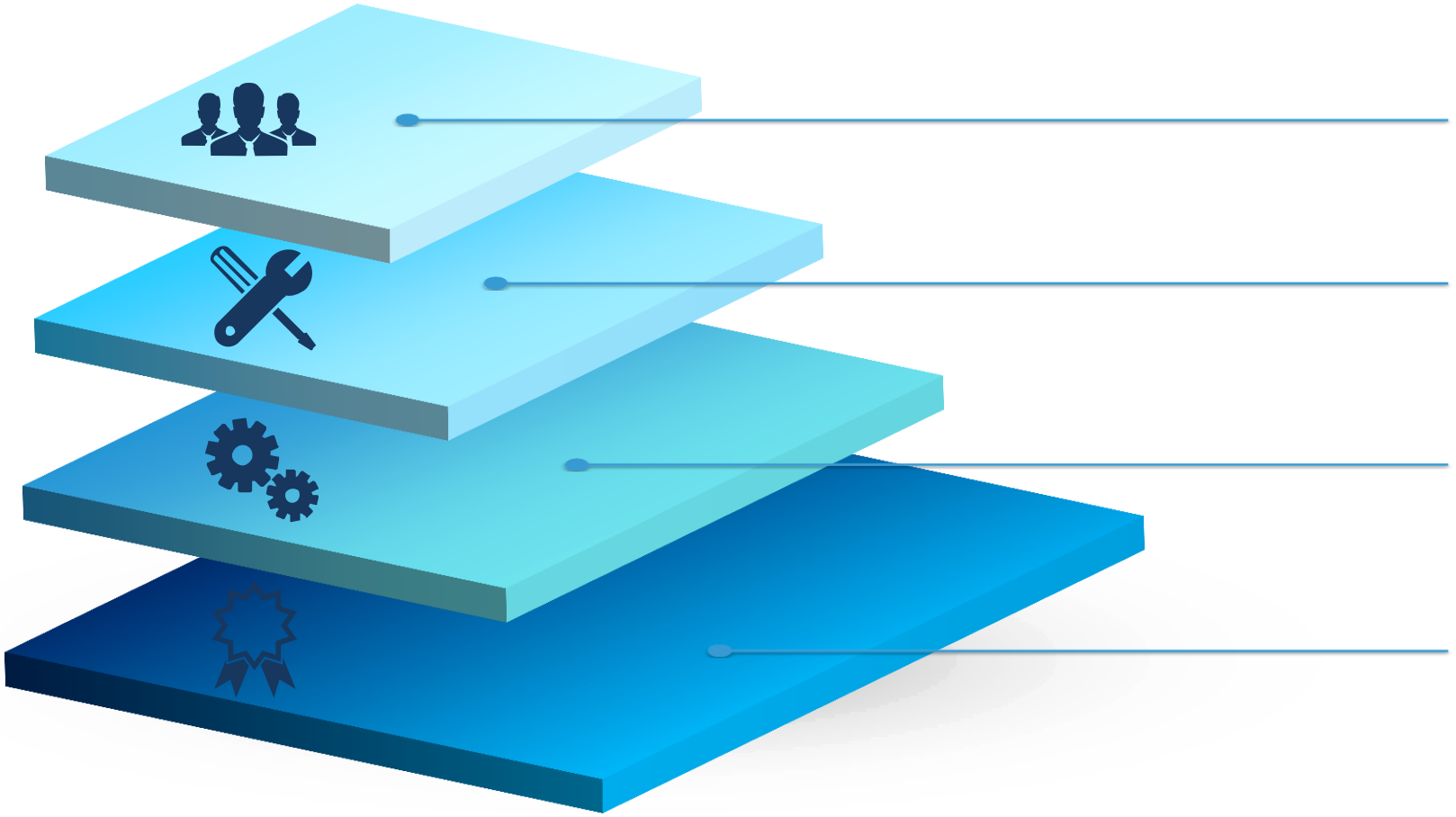


Do you know where you sensitive data is stored ?

Do you know how your sensitive data is protected and stays protected ?

Do you know who is accessing your sensitive data ?

z/OS Security Intelligence Framework



(1) Security Operations Staff

(2) Data Discovery Tools

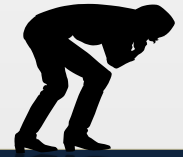
(3) Policy Enforcement

(4) Provenance

z/OS Security Intelligence Maturity Model

Productivity

First step in the z/OS Security Intelligence Maturity Model is establishing an I&AM framework to properly provison and deprovision access to z/OS resources and enhance the productivity of the oragnization through Role Based Access models.



Monitor

Second step in the z/OS Security Intelligence Maturity Model is establishing a security operations monitoring framework that effectively monitors the z/OS environment for intrusions and misuse of resources.

Integrity

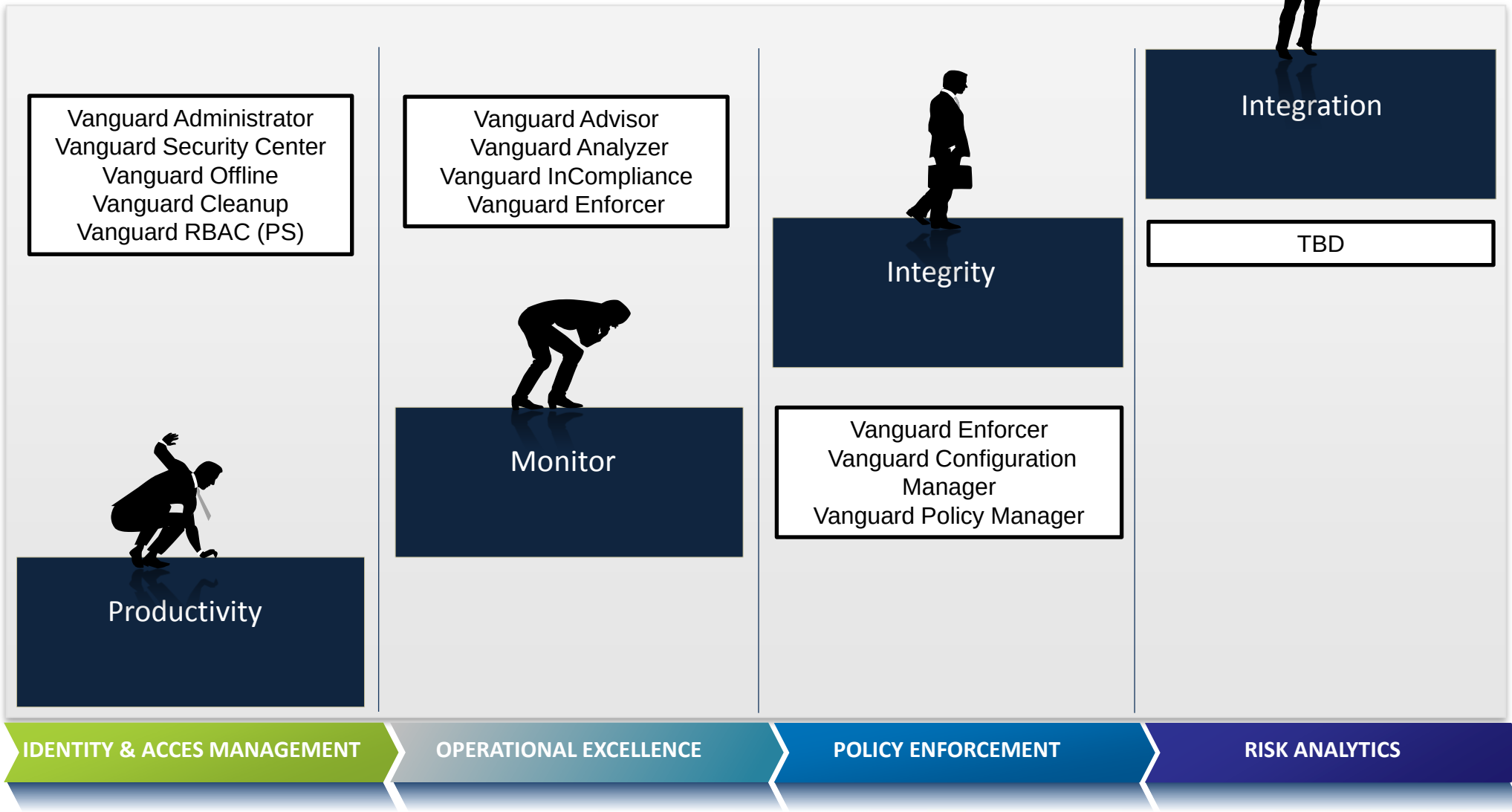
Third step in the z/OS Security Intelligence Maturity Model is establishing a security policy for z/OS and ensuring the policy is enforced at all times to ensure the integrity of the z/OS platform.

Integration

Fourth step in the z/OS Security Intelligence Maturity Model is establishing integration the data security wharehouse where risk analysis is performed to determine unusual data usage patterns that may be an indication of a security breach or fraud.

IDENTITY & ACCES MANAGEMENT | OPERATIONAL EXCELLENCE | POLICY ENFORCEMENT | RISK ANALYTICS

z/OS Security Intelligence Maturity Model versus Vanguard Solutions



New attitude

- The Mainframe is NOT an island > Integrate
- Understand where you data is (or was)
- Bad things happen to mainframes too !
- Understand the key (security) events on a mainframe
- Mobile will have major impact how data is accessed

Thank You
Call us at 800-794-0014 or email us at info@go2vanguard.com