RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

# Castles in the Air:
# Data Protection in the Consumer Age

SESSION ID: DSP-W03

Jason Clark
Chief Strategy and Security Officer
Accuvant
@CSOinFL

John Johnson
Global Security Strategist
John Deere
@JohnDJohnson

# Agenda

- Technology Trends: Making Security a Key Enabler
- The Changing Perimeter: Implications for Data Protection
- Risk-Based Security Solutions
- A Data-Centric Approach
- Aligning Strategy
- Capabilities and Maturity
- A Vision for the Future

# Defending The Castle

# The Castle Model of Defense

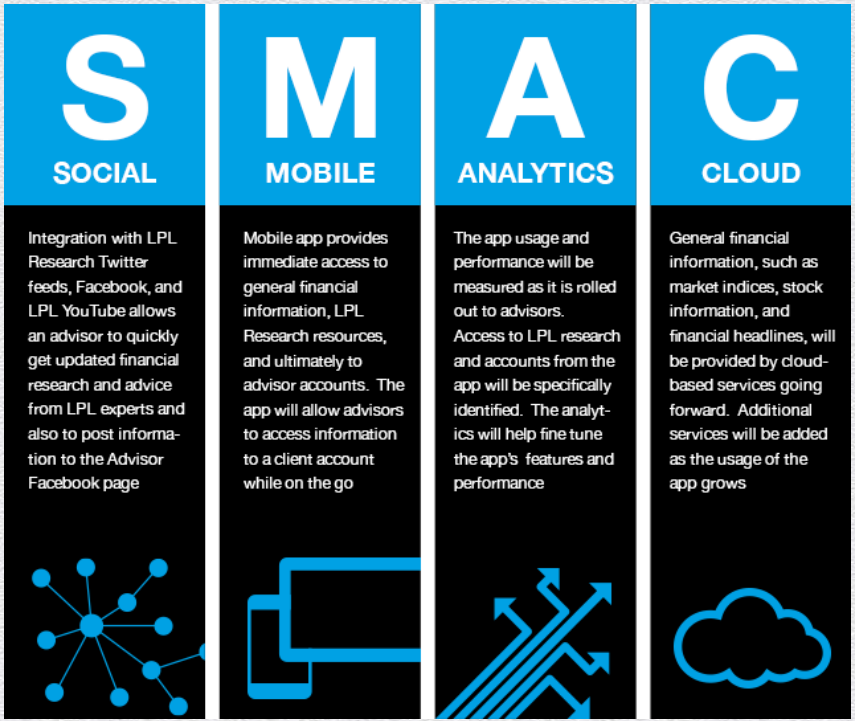
**What is the advantage of a castle?**

- The castle is built on high ground
- The castle has visibility to see enemies approaching far away
- The castle has thick, impervious walls
- Guards watch everyone coming and going
- It is very difficult and expensive for enemies to breach a castle

**Why is our enterprise not a castle?**

- The Internet has no high ground
- We don’t have good visibility to threats
- We have lots of holes in our walls
- We don’t inspect all the traffic coming and going
- **The Asymmetric problem:** It is expensive to defend, but the adversary only needs to find one hole to breach the enterprise

# Let's Talk SMAC

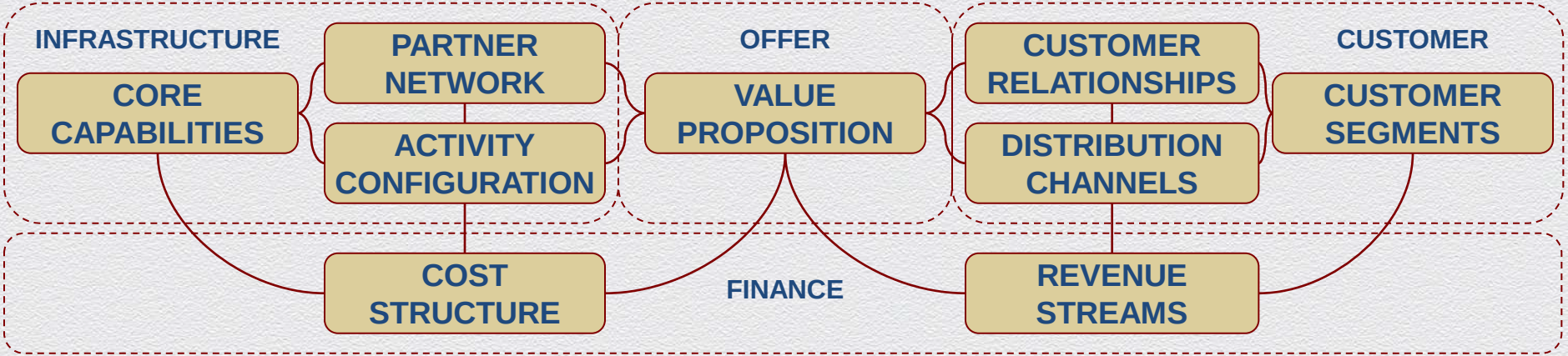



*The SMAC Stack*

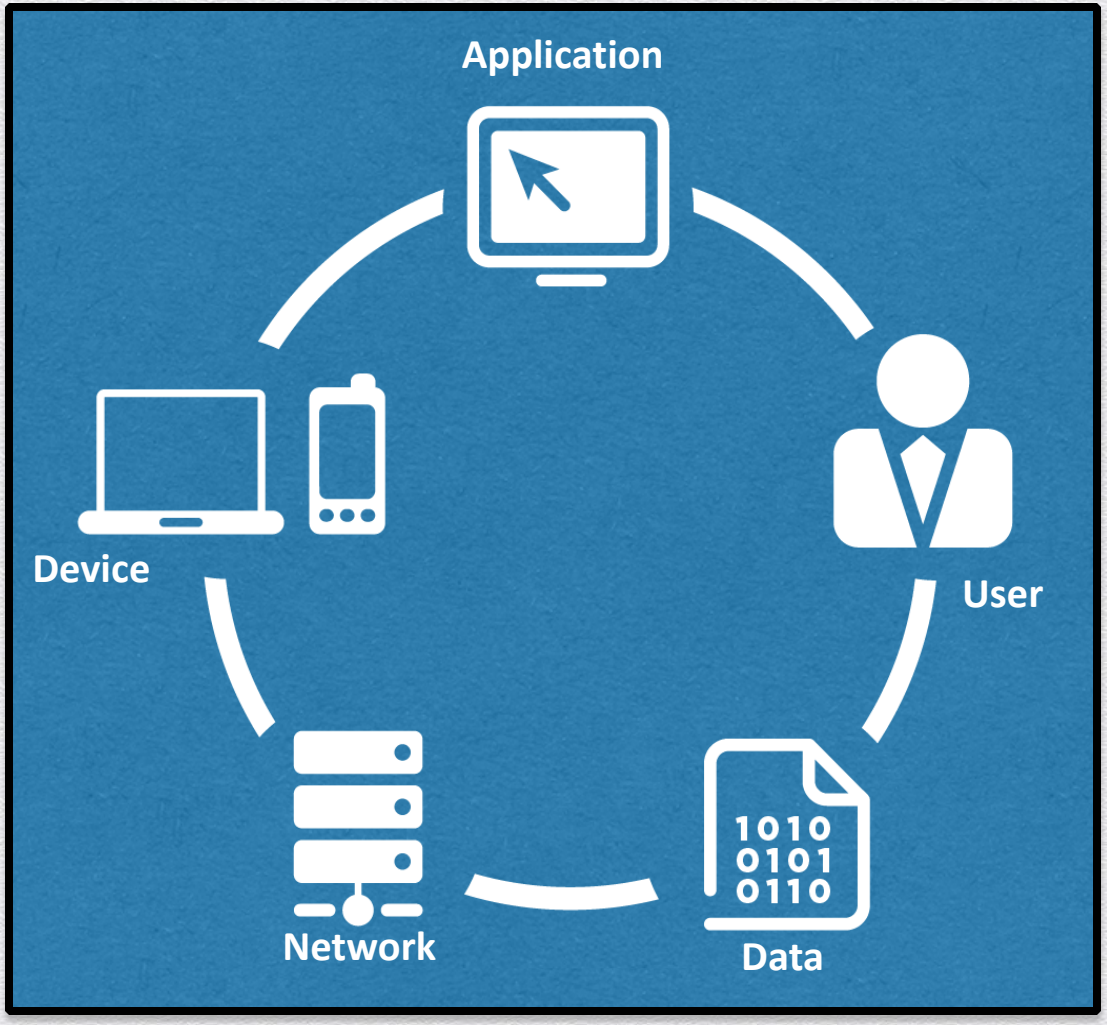
# Consumerization: Threats & Opportunities

- Security can be seen as a key enabler or a barrier to success
- It will happen: don’t throw yourself in front of the train to stop it
- The solutions that worked in the past will not serve us in the future
  - We need the right mix of people, processes and technology to secure these transformative technologies
  - The perimeter is evolving away from “castle model”
  - It is easier than ever to have important data leak; we inherently have less visibility and control over data that leaves our environment

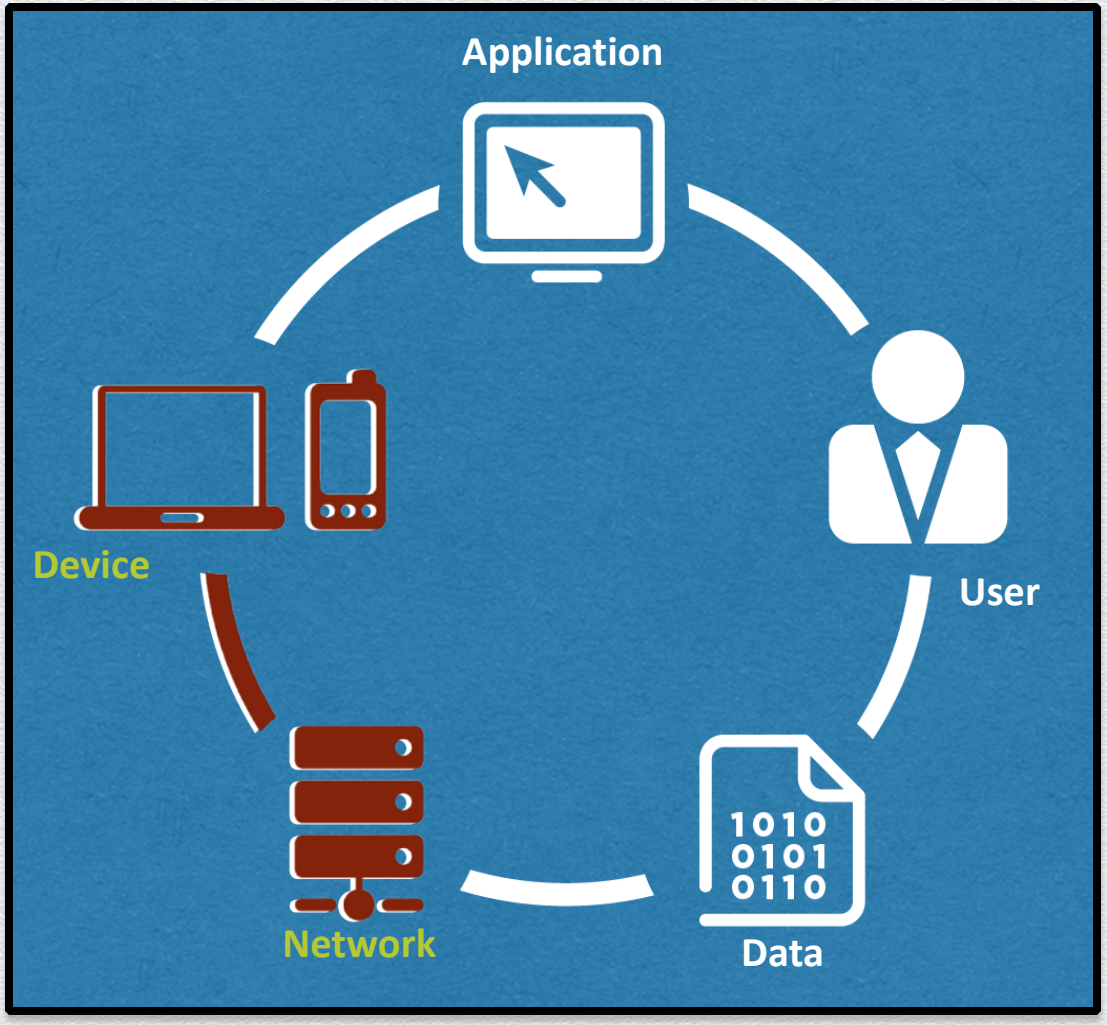
# Business Model Framework




a business model describes the value an organization offers to various customers and portrays the capabilities and partners required for creating, marketing, and delivering this value and relationship capital with the goal of generating profitable and sustainable revenue streams

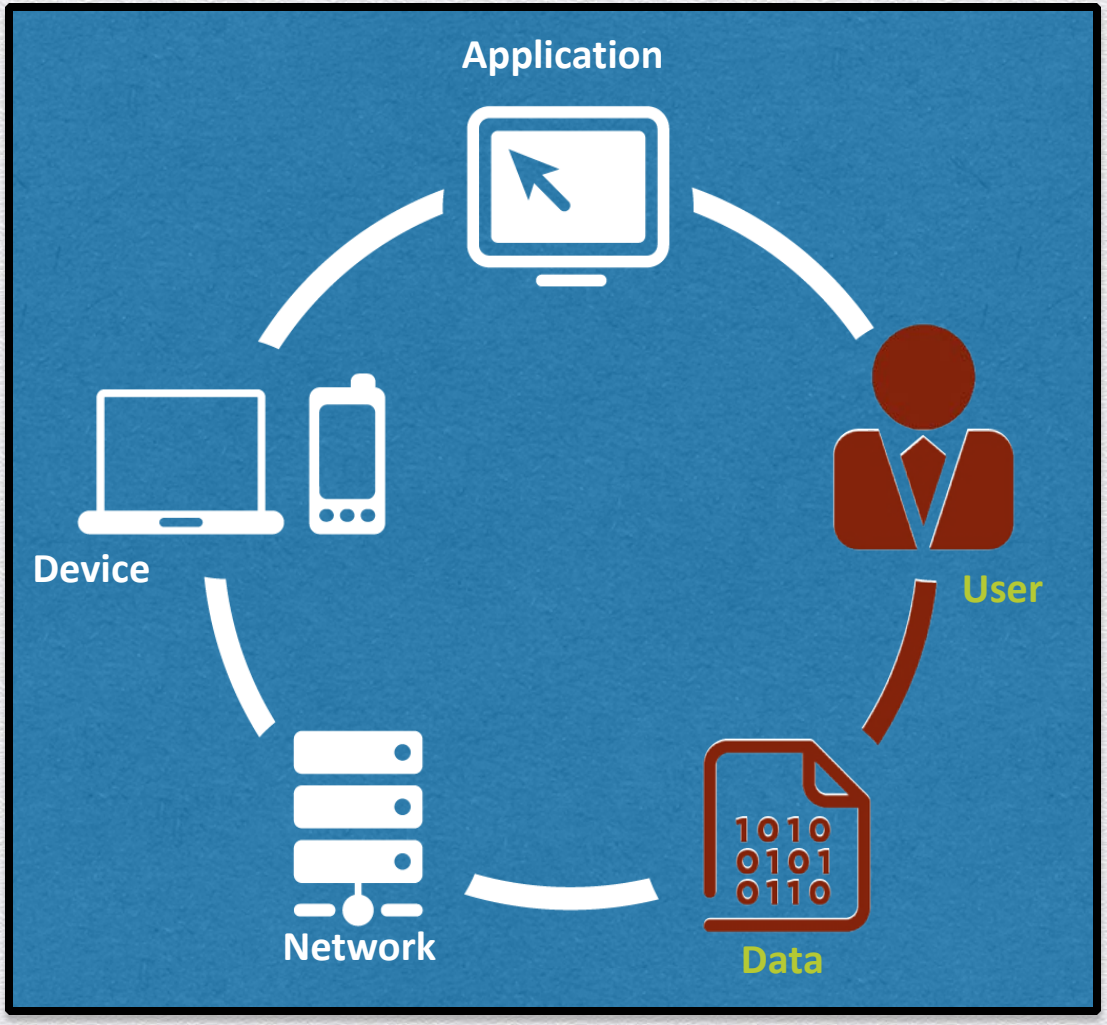



# HOW WE SECURE THE PERIMETER TODAY




# HOW WE SECURE THE PERIMETER TODAY

**MAJORITY OF THE SECURITY SPEND HAS BEEN FOCUSED ON STOPPING OR DETECTING THE THREATS ON THE NETWORK OR DEVICE.**




# HOW WE SECURE THE PERIMETER TODAY

**IN COMPARISON LITTLE SPEND HAS BEEN PUT TOWARDS USER ACTIVITY AND DATA PROTECTION. MOST ORGANIZATIONS ARE IMMATURE IN UNDERSTANDING USER AND DATA BEHAVIOR.**

# ACTORS AND MOTIVATIONS

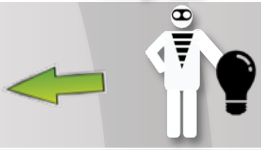
From Outside

From Insiders

**From Outsiders via Insiders!**

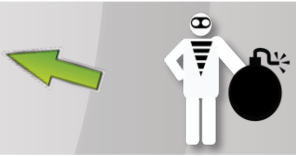
**INDIVIDUALS**

**ORGANIZED CRIME**



**INDUSTRIAL**

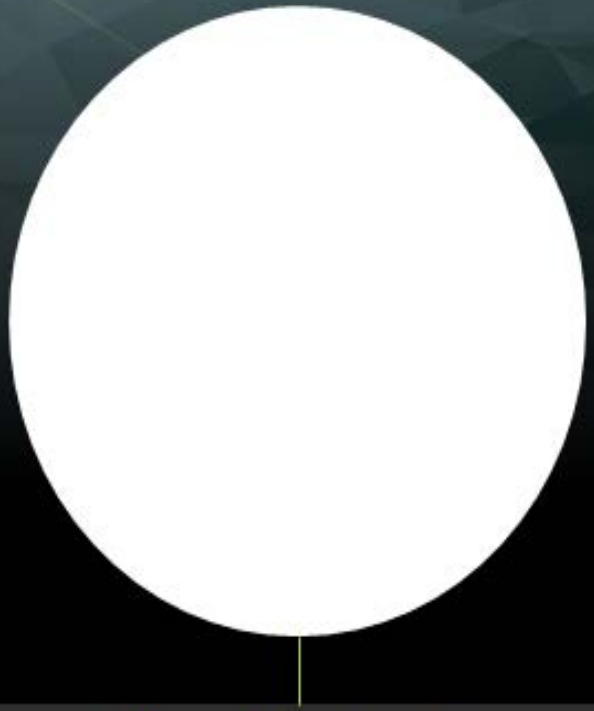
**HACKTIVISTS**



**TERRORISTS**

**NATION STATES**

# SECURITY SPEND

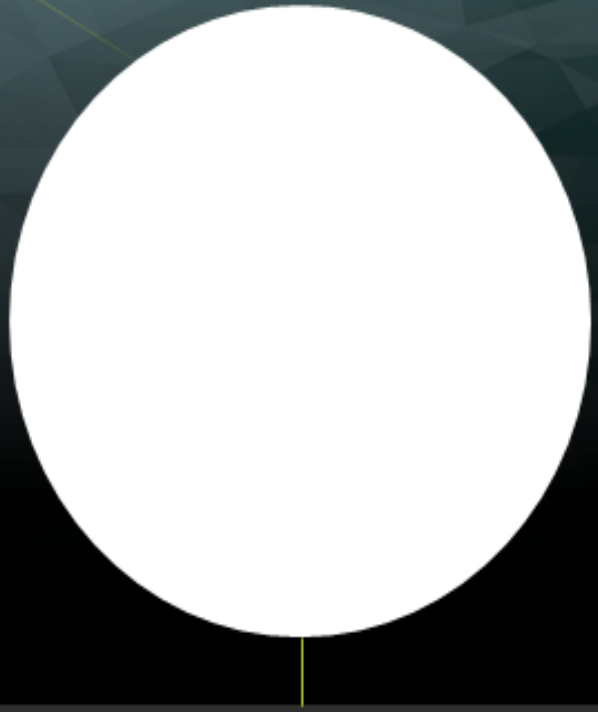


Your Company's Revenue

IT Budget

Infosec Budget

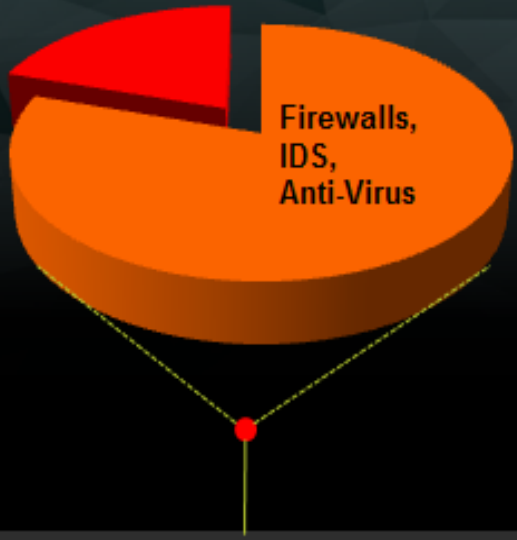
# SECURITY SPEND



Your Company's Revenue

*80% OF THE SPEND IS 30% EFFECTIVE AT SECURING THE BUSINESS.*

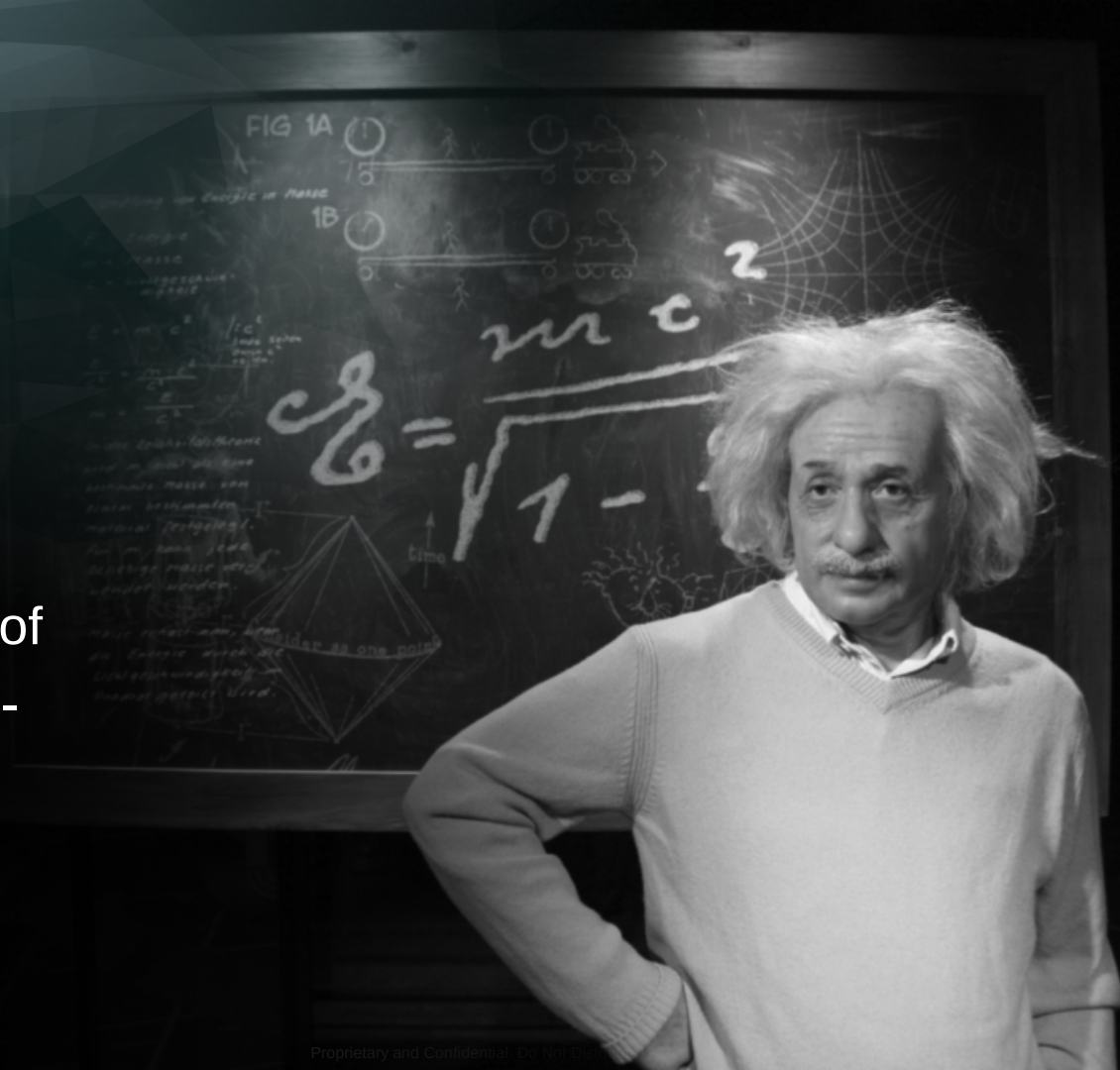
IT Budget




Infosec Budget

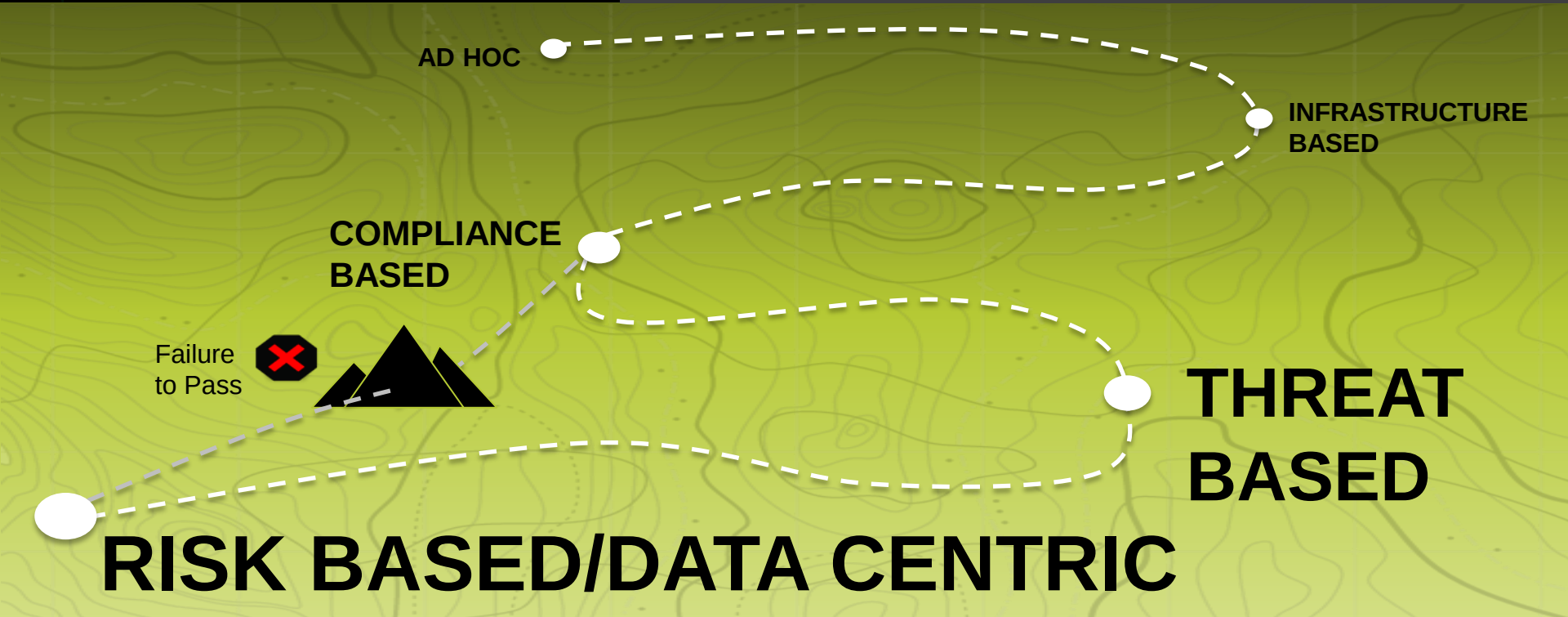
# WHAT IS THE DEFINITION OF INSANITY?

Continuing to Put 80% of Our Spend on Firewalls, Anti-virus and IPS and Not Changing Our Security Strategy/Tactics



# The Security Journey

Ultimate Goal is Risk Based/Data Centric with Threat Modeling



# A Risk-Based Approach

- Work with the business, don’t operate in a vacuum
- Figure out who owns the risk and who the decision makers are
- Identify the data/assets that you most want to protect
- Assess threats in consistent way
- Develop meaningful risk metrics
- Start with most significant business risk and prioritize
- Identify new technical security controls and apply P/P/T to architect solutions that enable SMAC: Layered, Synergistic, Agile

# CISO View of the World

COMPLEX JOB

Make Our Business Better

COORDINATED APPROACH TO RISK

Business Drivers and Initiatives | Risks | Frameworks | Approach | Risk & Security Coverage | Oversight

EXECUTIVE MANAGEMENT

BUSINESS STRATEGY

- Asset and Capital Management
- Earnings and Operating Margins
- Revenue and Market Share
- Reputation and Brand

Risks

- Strategic
- Operations
- Financial
- Compliance

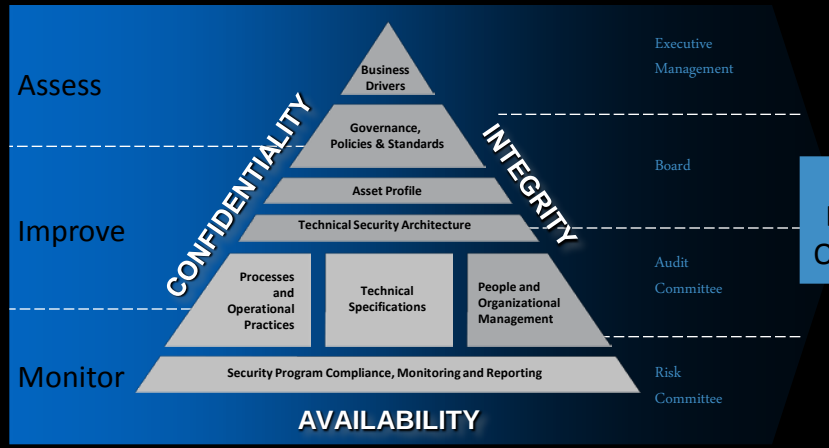
Frameworks

- COSO
- COBIT
- ITIL
- ISO 17799

Regulations

- Patriot Act
- GLBA
- SOX
- Other Regulations

Assess / Improve / Monitor




Executive Management

Board

Audit Committee

Risk Committee

Achieve Business Objectives

ALIGNED TO BUSINESS DRIVERS



Keep Us Out of Trouble

# Data Protection Stewards

Security is responsible for recommending and overseeing the controls that ensure protection stewardship extends beyond IT into the enterprise and beyond the perimeter into the cloud.

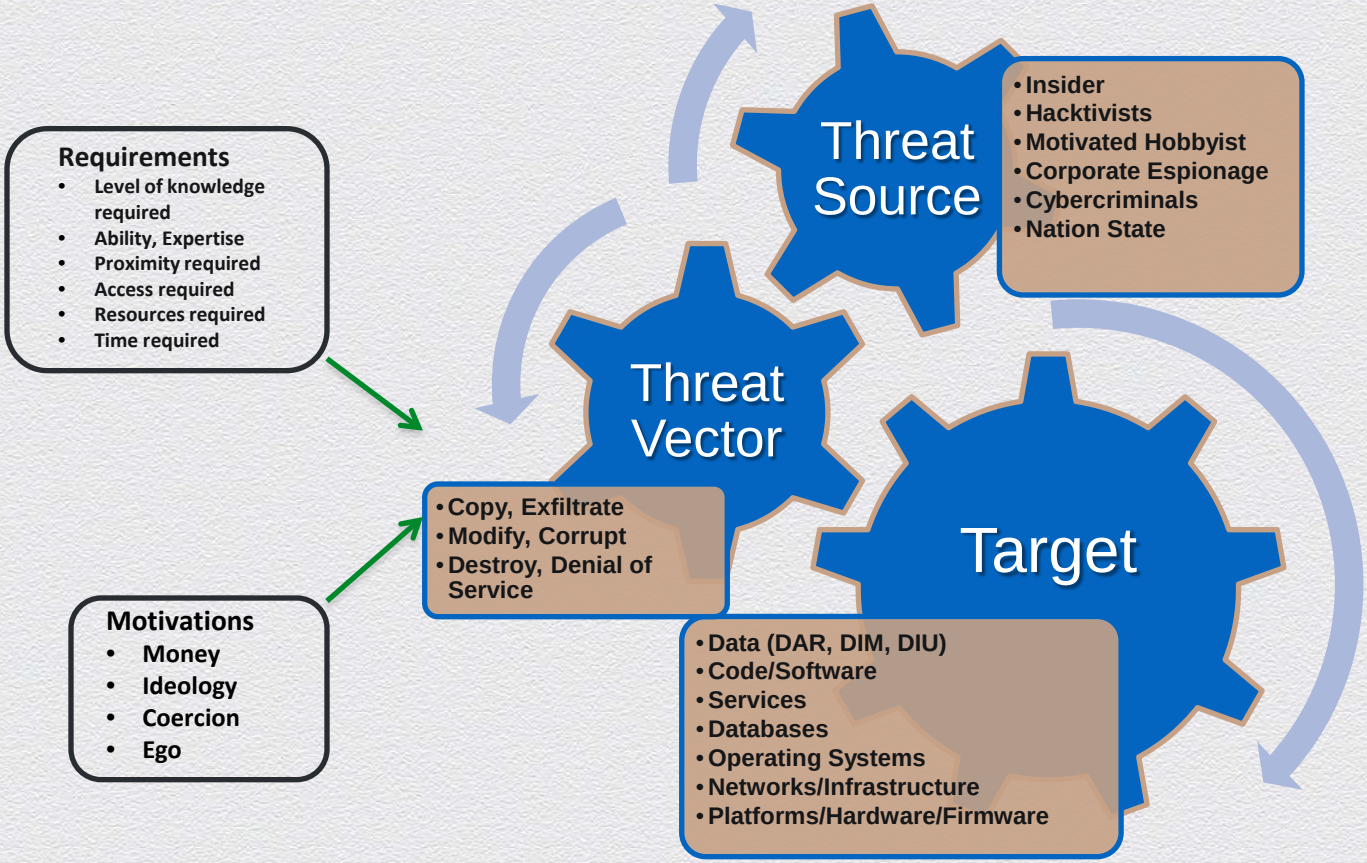
- Support Organization Mission & Business Objectives
- Protect Organization Reputation
- Confidentiality of Information
- Integrity of Information
- Availability of Information

"Integration Theory", Information Security, July 2008, http://searchSecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1321706,00.html

# Data-Centric Security

- Identify the data that you most want to protect
  - Sensitive IP, Regulated, High Value
- Mark the data; don’t try to classify everything
- Perform threat modeling and scoring
- Identify security controls that can be applied at boundary layers
- When possible, automate (intelligent) decision-making
  - If you can’t block, log/alert and educate end user on appropriate use
- Evolve with threats: Reduce adversaries’ operating surface

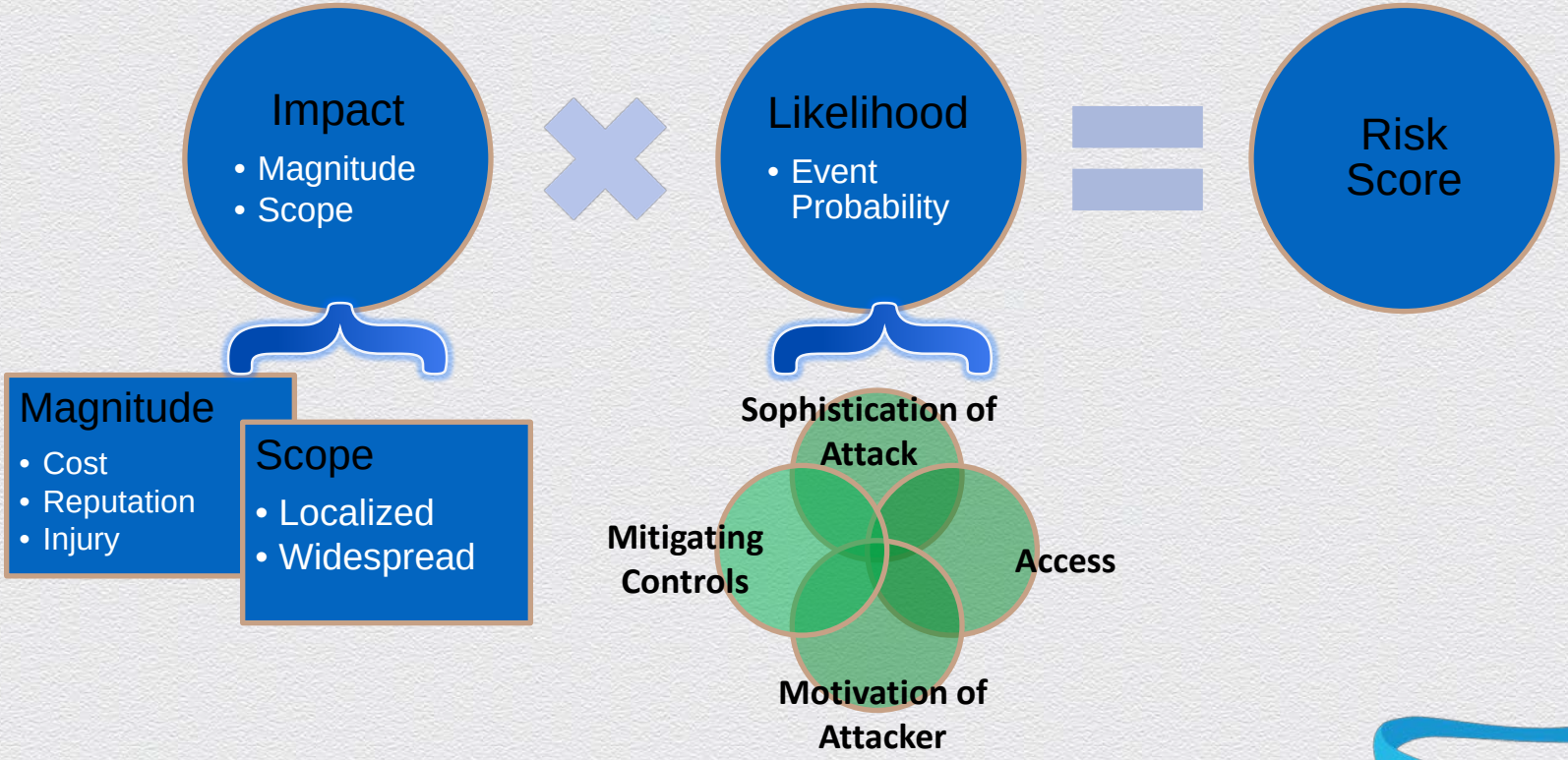
# Cyber Risk Analysis: Threat Modeling



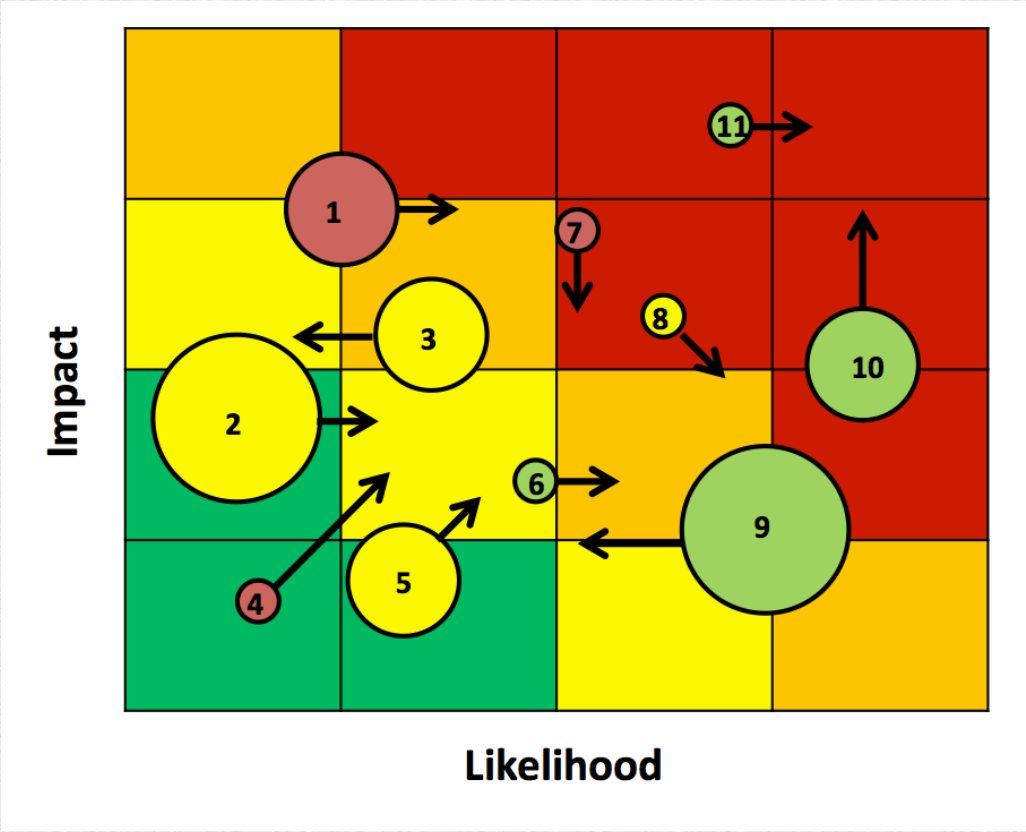

{ RISK

Risk can be mitigated; threat landscape remains unchanged.

# Risk Scoring



# Develop Prioritized Mitigation Strategy Based on Greatest Threat



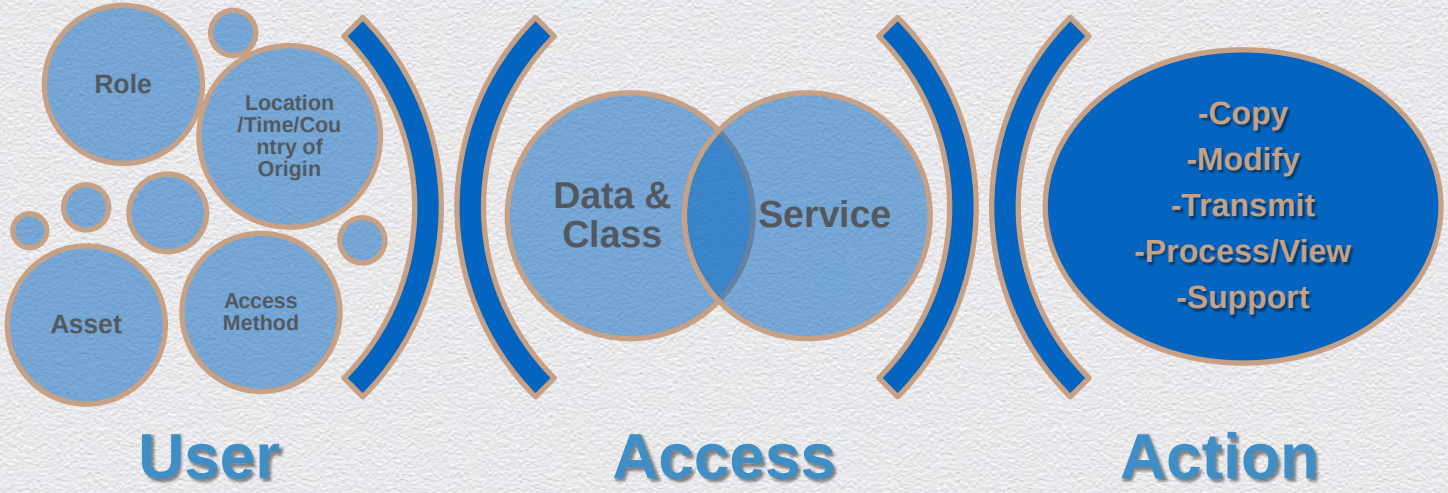
# Security Controls

## PEOPLE, PROCESSES, TOOLS

**Policies, Awareness, Processes, SLA, Contracts…**
**Find enabling technologies:** *mature, interoperable, extensible, offering fine-grained rules.*

- **Device-Centric:** EPP, Client DLP, Mobile Proxy, DRM, MDM, Advanced Threat Detection/Mitigation, VDI, Patch Mgmt, Group Policy, Software Inventory, …
- **Network-Centric:** Segmentation, Network Knowledge, Non-Compliant VLANs, Network/Cloud Content Mgmt (AV, DLP), FW, Proxies, APT Detection, IDS/IPS, SIEM, Threat Intelligence, Rogue Detection, Next Gen Network, Fraud Detection, Vuln Mgmt, Network Forensics, Authentication, Federation…
- **Data-Centric:** Classification Policy, Awareness, Discovery, DRM, DLP…

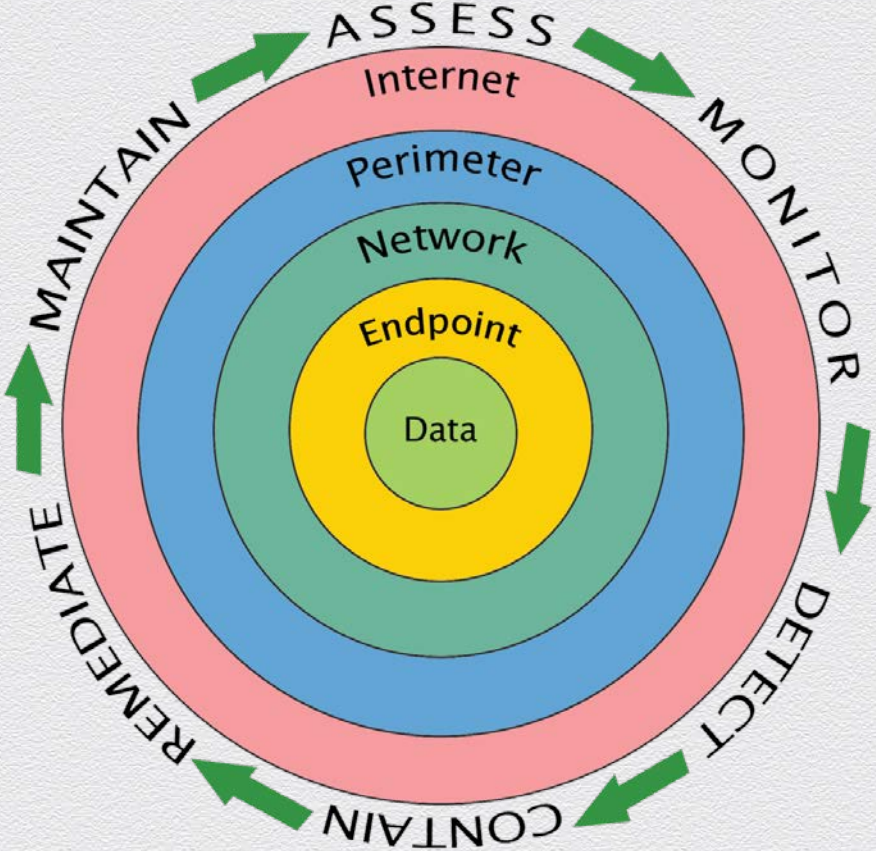
# Apply Security Rules Based on Risk Scoring




Security controls are applied to mitigate risk, based on a number of factors. Develop solutions with technology that makes intelligent decisions at boundaries and automates actions (when possible), to ensure policy compliance.

# This is an ineffective security control

# Layered Security Controls

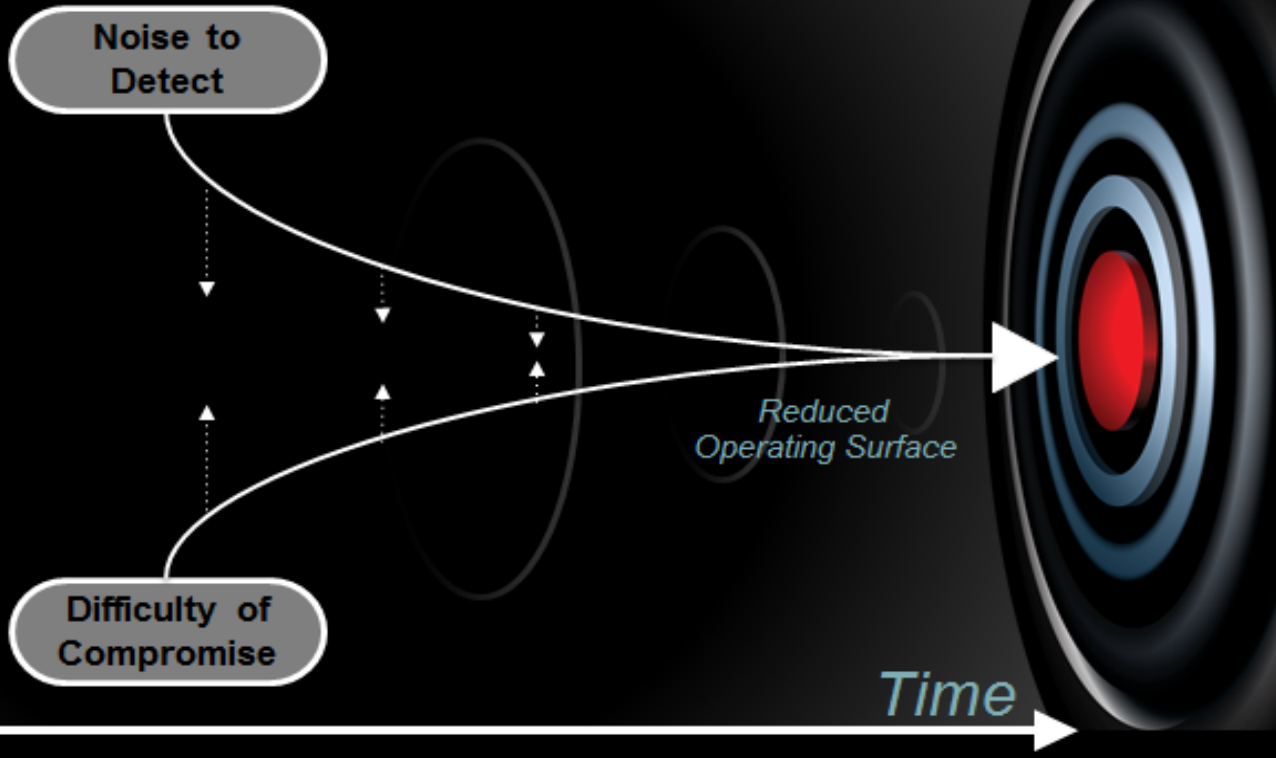


# IP Data and Context Centric Security


Use cases help identify risk and select security controls/rules to mitigate risk (DLP example)

# HOW DO WE EVOLVE WITH THE THREATS?

*Reduce the Adversaries' Operating Surface*




## Reduce the Noise to Detect

- Minimize "Dwell Time"
- Intelligence and Sharing
- Monitoring of Key Data
- Enhanced Monitoring

## Increase the Difficulty of Compromise

- "Secure By Design" Approach
- Internal Compliance
- Improved Access Controls
- Continuous Testing and Improvement

# What should be our focus?

# STRATEGY

Making the Move from Reactive Strategy to Fully Integrated Strategy Aligned with Your Business Strategy

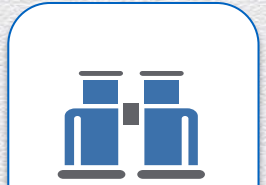
# RISK

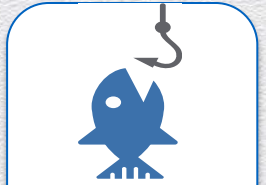
Vulnerability X Threats X Assets

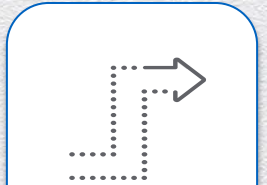
# ASSETS

- Data Protection
- Data Analytics
- Insider Threats
- Mergers and Acquisitions

# Kill Chain Mapping and Threat Modeling

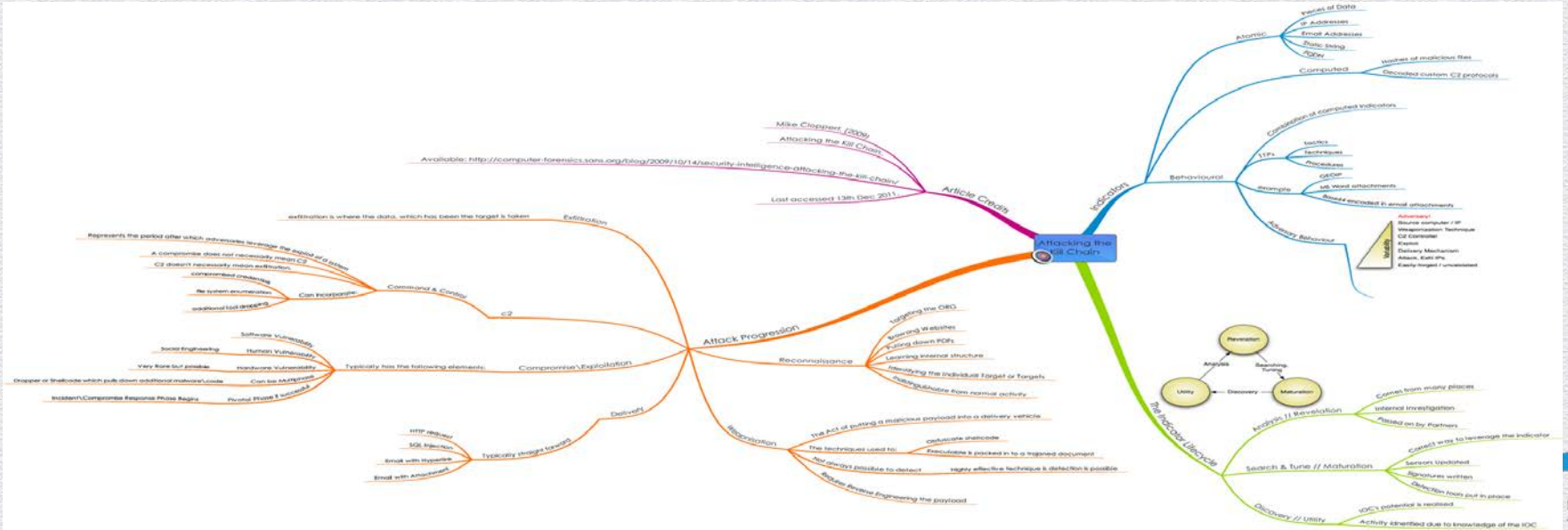


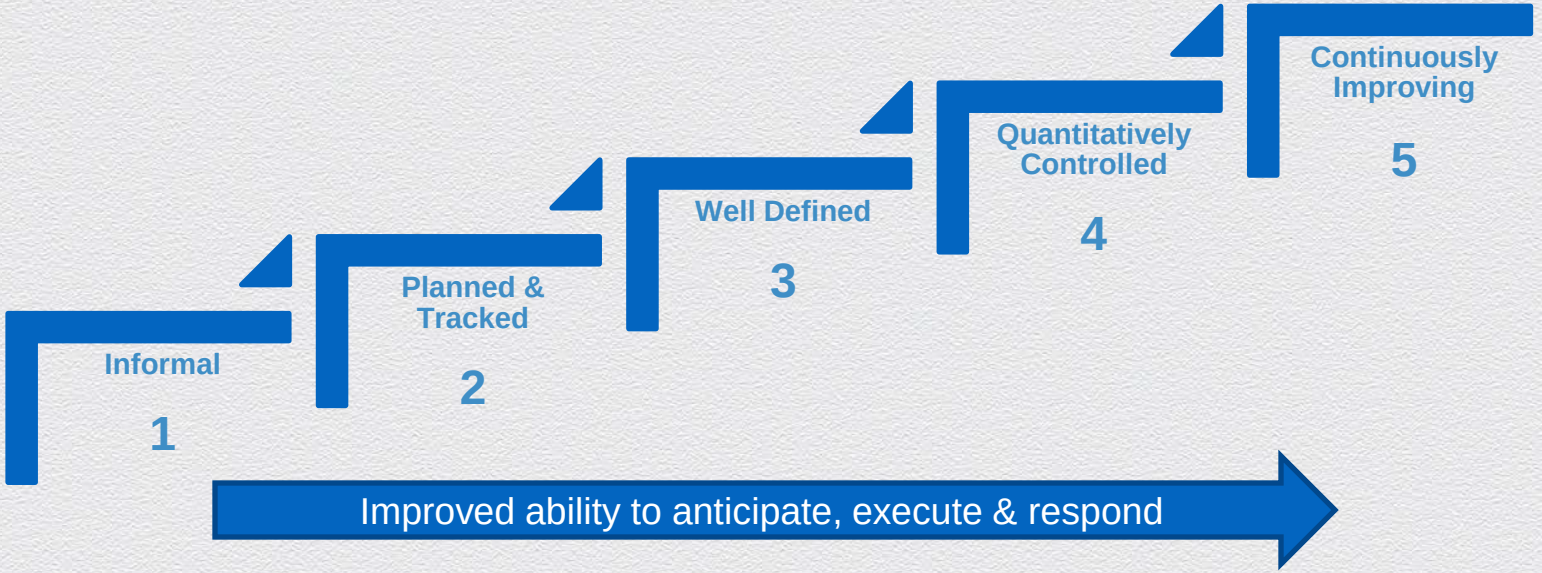




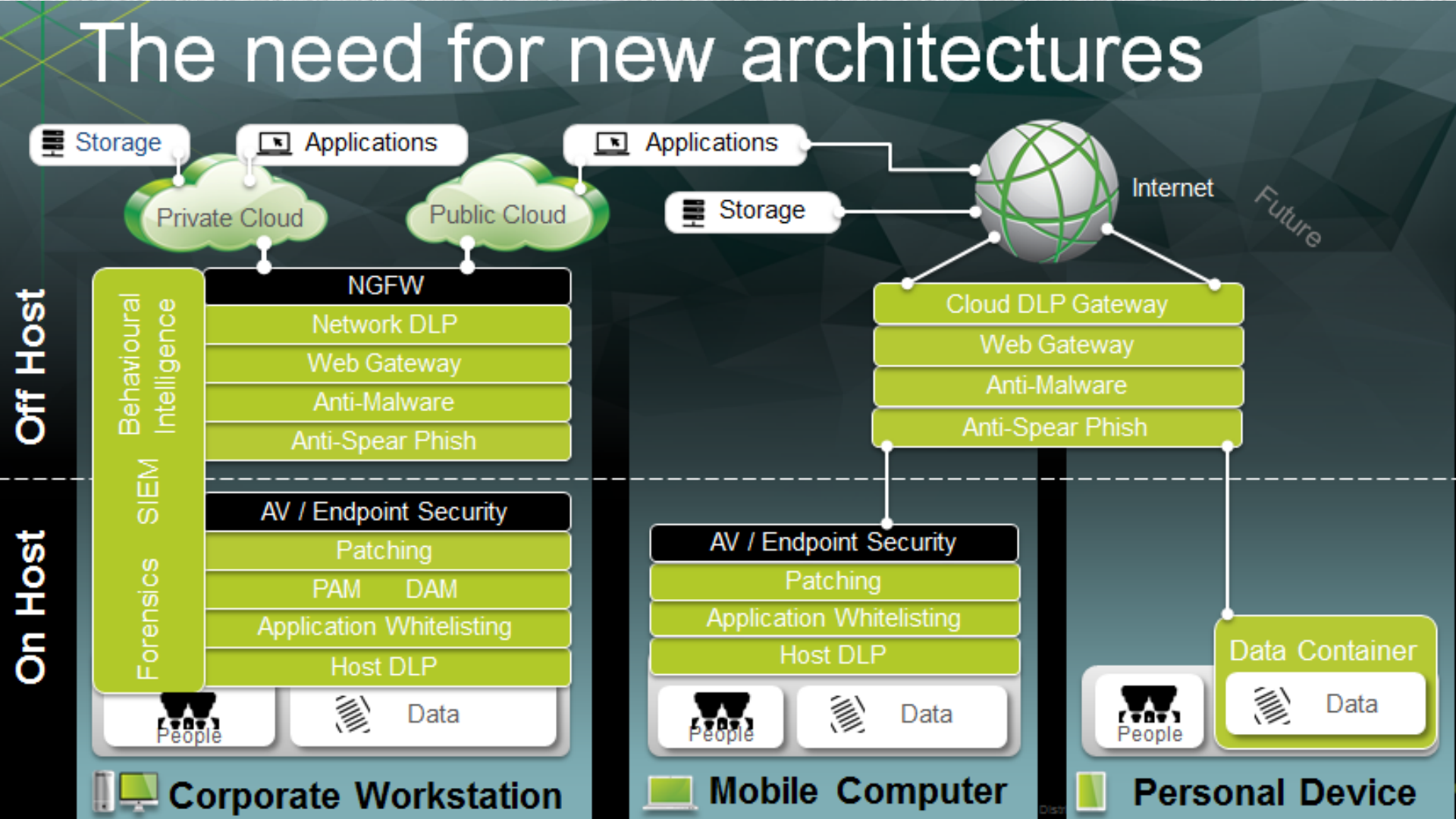



# Security Capability Maturity Model

As the security program matures, more fundamental pieces will be in place to support advanced toolsets and capabilities necessary to protect against more advanced threats and respond faster to attacks



# The need for new architectures

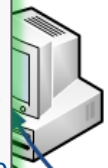


# Data Protection on Endpoint

**Email Threats** (Defenses)
- **Malware** (Anti-Malware)
- **Spam/Phishing** (Adv Threat Protection)
- **Data Loss** (DLP, Encryption)
- **Legal** (eDiscovery, Legal Hold)

**Application Threats** (Defenses)
- **Inappropriate Access** (Access Controls)
- **Attacks** (Adv Threat Protection, Harden Server, Patch Mgmt, Pen Testing, EPP, Application Security Framework, Fraud Detection, WAF, Code Signing, PKI, Web Auth, ADFS)
- **Data Loss** (Data Classification, DRM, DLP,

**Storage Threats** (Defenses)
- **Malware** (AV)
- **Inappropriate Access** (Access Controls, DRM)
- **Data Loss & Exposure** (DRM, DLP, Ent File Sync, Secure File Transfer, Encryption, Backups)



**Web Threats** (Defenses)
- **Malware** (Anti-Malware)
- **Malicious Sites** (Proxy Blocking)
- **Data Loss** (DLP)
- **Adv Threats** (Adv Threat Protection)

**Endpoint Threats** (Defenses)
- **Malware & Exploits** (Software Inventory, EPP, Apex, Patch Mgmt)
- **Data Loss** (DRM, DLP, Encryption, Backups, Forensics)
- **Attacks** (HIPS, Adv Threat Protection, Software Firewall, Patch Mgmt)

**Network Threats** (Defenses)
- **Waterhole** (GPO, VPN)
- **Hacking** (Firewall, Rogue Detection)
- **Advanced Threats** (Edge Devices, IDS, Anomaly Detection, DDoS Mitigation)
- **Data Loss** (Access Controls, NGN, Non-Compliant VLANs)

**General Defenses**
- Policies & Standards
- Monitor & IR (SIEM, logs)
- Audit & Assessments
- Training & Awareness

# Data Protection on Mobile Device

**Email Threats** (Defenses)
- **Malware** (Anti-Malware)
- **Spam/Phishing** (Adv Threat Protection)
- **Data Loss** (DLP, Encryption)
- **Legal** (eDiscovery, Legal Hold)

**Application Threats** (Defenses)
- **Inappropriate Access** (Access Controls)
- **Attacks** (Adv Threat Protection, Harden Server, Patch Mgmt, Pen Testing, EPP, Application Security Framework, Fraud Detection, WAF, Code Signing, PKI, Web Auth, ADFS, Sandbox Apps)
- **Data Loss** (Data Classification, DRM, DLP, Backups, Encryption)

**Storage Threats** (Defenses)
- **Malware** (AV)
- **Inappropriate Access** (Access Controls, DRM)
- **Data Loss & Exposure** (DRM, DLP, Ent File Sync, Secure File Transfer, Encryption, Backups)

**Web Threats** (Defenses)
- **Malware** (Anti-Malware)
- **Malicious Sites** (Proxy Blocking)
- **Data Loss** (DLP)

**Endpoint Threats** (Defenses)
- **Malware & Exploits** (Software Inventory, EPP, Patch Mgmt)
- **Data Loss** (DRM, DLP, Encryption, Backups, Forensics, MDM)
- **Attacks** (Adv Threat Protection, Patch Mgmt,

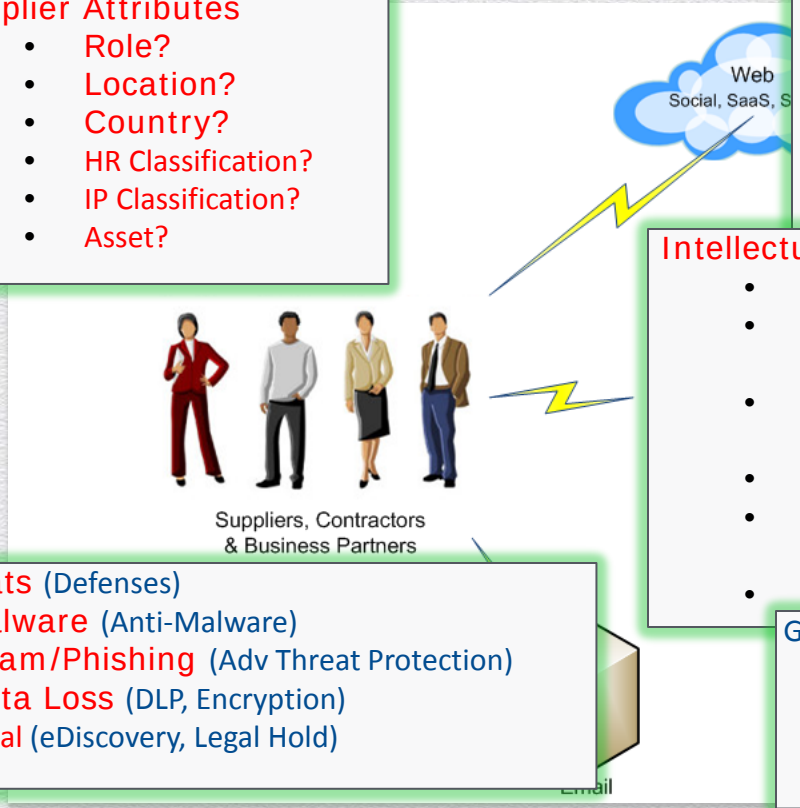
**Network Threats** (Defenses)
- **Waterhole** (GPO, VPN, EODINET)
- **Hacking** (Firewall, Rogue Detection)
- **Advanced Threats** (Edge Devices, IDS, Anomaly Detection, DDoS Mitigation)
- **Data Loss** (Access Controls, NGN, Non-Compliant VLANs)

**General Defenses**
- Policies & Standards
- Monitor & IR (SIEM, logs)
- Audit & Assessments
- Training & Awareness

# Data Protection for Suppliers

**Supplier Attributes**
- Role?
- Location?
- Country?
- HR Classification?
- IP Classification?
- Asset?

**Web Threats** (Defenses)
- Malware (Anti-Malware)
- Malicious Sites (Proxy Blocking)
- Data Loss (DLP)
- Adv Threats (Adv Threat Protection)
- Policy Abuse (Packet Inspection)
- Authentication (ADFS, Web Auth, OTP)

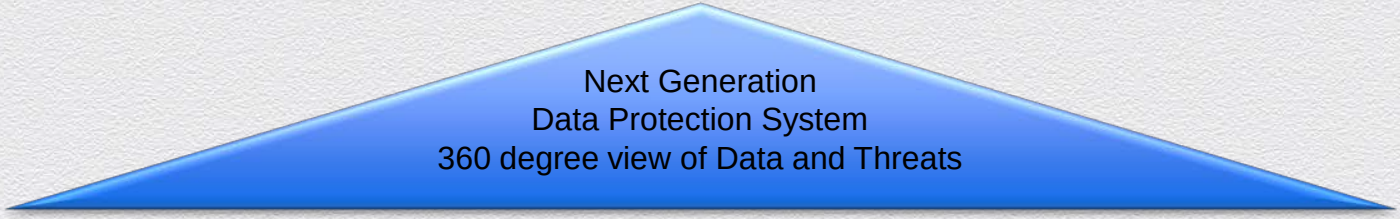



**Intellectual Property Threats** (Defenses)
- Malware & Exploits (Apex)
- Data Loss (DRM, DLP, Encryption, User Monitoring, Logging, Deere Campus)
- Attacks (IDS, Firewall Rules, TPAM, Security Policy, NGN, Contractor Build)
- Remote Access (VDI, VPN, Citrix, OTP)
- Inappropriate Access (Access Controls, EDAC, Fraud Detection, OTP, IPP-SC)
- Contractual (BPT, SLA, MA)

**Email Threats** (Defenses)
- Malware (Anti-Malware)
- Spam/Phishing (Adv Threat Protection)
- Data Loss (DLP, Encryption)
- Legal (eDiscovery, Legal Hold)

**General Defenses**
- Policies & Standards
- Monitor & IR (SIEM, logs)
- Audit & Assessments
- Training & Awareness

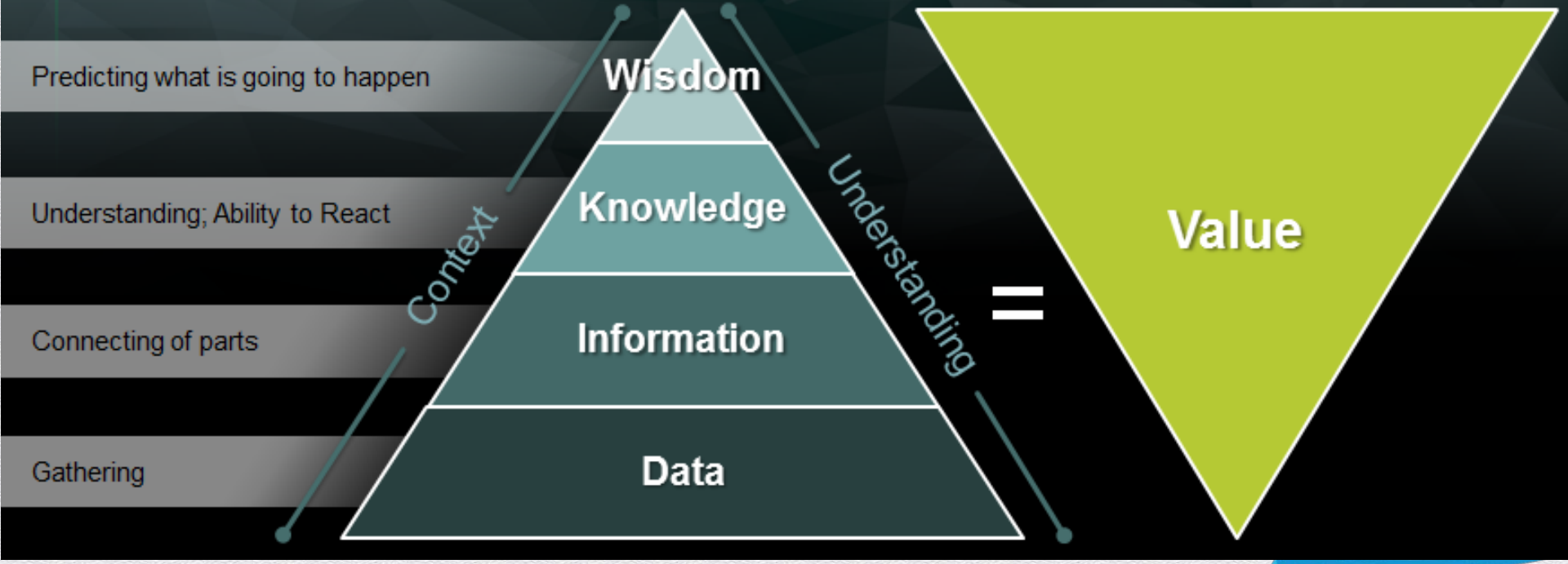
# Behavior Analytics Risk Intelligence




| Threat Focused | User Focused | Data Focused |
|---|---|---|
| IPS / Firewall | Privileged Account Monitoring | Email DLP |
| Proxy | Authentication | Web DLP |
| Anti Malware | Access | Endpoint DLP |
| SIEM | | DRM |

# OPERATIONS TO INTELLIGENCE

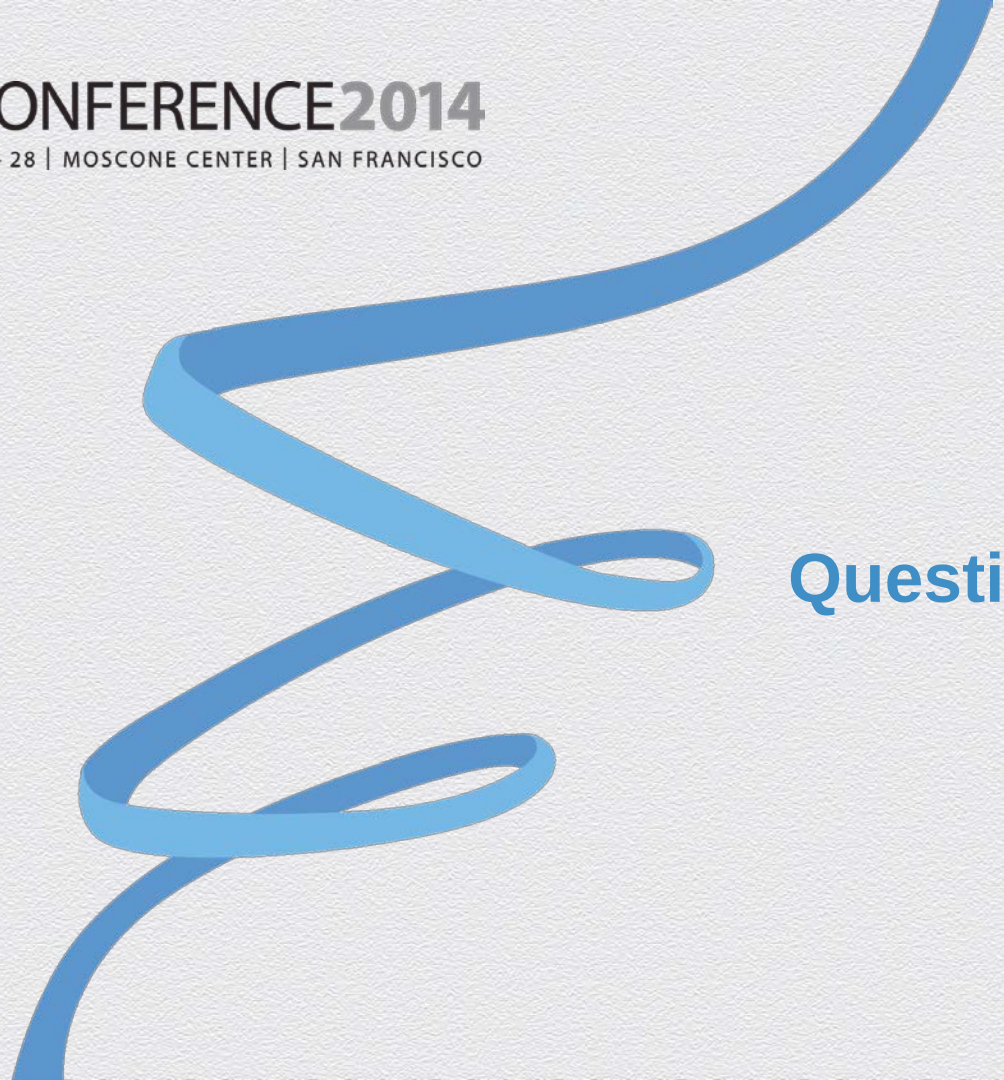
*Security Operations To Security Intelligence to Business Intelligence*




**The Relative Value of Information**

# Take Aways

- The data-centric model is crucial, because the risk associated with cloud, mobile, social, data is much less when the data (information) is managed well, or kept out of those zones.
- In order to enable the business, you sometimes need to accept equivalent services (w/SLA) from vendors.
- It is important to seek integration and synergy between products and across boundary layers
- Consumerization is a wave that we cannot stop, and we can surf it or drown. We need to partner with the business to develop reasonable solutions, focusing on the greatest risk/value, and that means architecting flexible solutions that draw upon security controls across all layers.



# Questions?