Protect with Visibility

Steve Poulson, Bay Dynamics

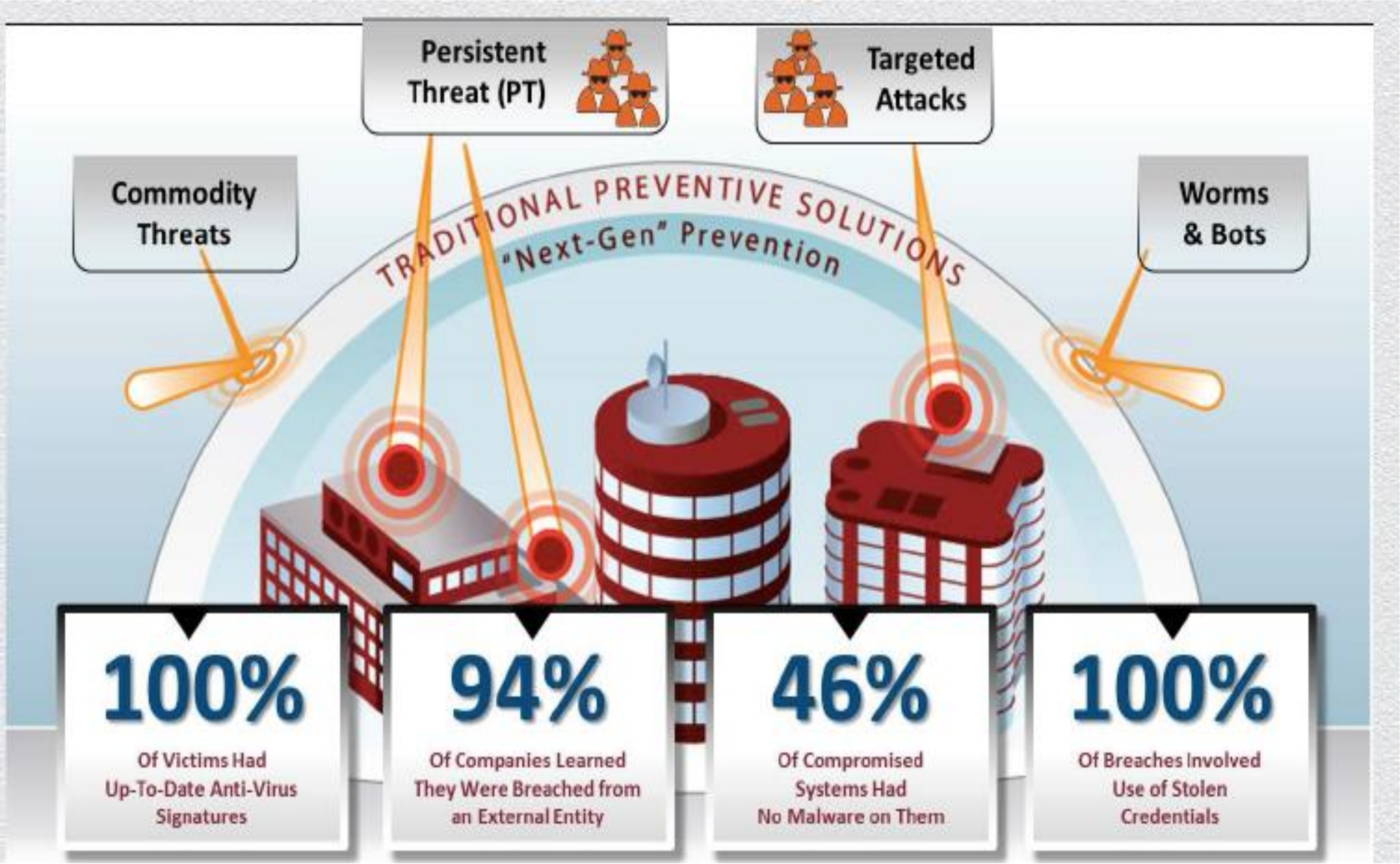
Reality Today

“ Most organizations have reached a level of maturity where people, not process or technology, are the primary security concern… ”

Excerpt from Gartner Research Note

“Eight Practical Tips to Link Risk and Security to Corporate Performance “

Attacks will eventually bypass defenses given time and persistence


Persistent Threat (PT)
Targeted Attacks
Commodity Threats
Worms & Bots
TRADITIONAL PREVENTIVE SOLUTIONS
"Next-Gen" Prevention
100%
Of Victims Had Up-To-Date Anti-Virus Signatures
94%
Of Companies Learned They Were Breached from an External Entity
46%
Of Compromised Systems Had No Malware on Them
100%
Of Breaches Involved Use of Stolen Credentials

Source Mandiant M-Trends

BAY DYNAMICS™

Key Findings Common To Data Breaches

1. IT security solution data overload
2. Individual security silos do not communicate
3. No active federated security view
4. Attackers hide in noise and low severity events
5. Post event federated security search finds cookie crumbs of significant importance, after the fact

Typically notified by Government Agency, Partners, Clients

Are your IT security conditions a perfect storm for a data breach?

Traditional Approach to Security Deployments

Is your actionable security data stuck in silos?

BAY DYNAMICS™

The value of security information deteriorates over time

We’ve heard this before….

Something needs to Change. Need to improve visibility.

Consumerization of IT or Nexus of Forces

CLOUD, SOCIAL, MOBILE AND INFORMATION –

- Convergence of these forces, has created a technology-immersed environment and is transforming the way people and businesses relate to technology. In order to stay competitive organizations cannot ignore this because:
- This extends organizations' reach and relationship to their customers, employees, partners and really their entire ecosystem.
- Pervasive mobility, near-ubiquitous connectivity, Cloud efficiencies, and access to information decrease the gap between idea and action.

THE DARK SIDE

- Current Approach to security and risk Management needs to be reset
- Today, security solutions operate in complete isolation and report their findings independently of each other – there is a weakness in this approach and attackers are exploiting it today.

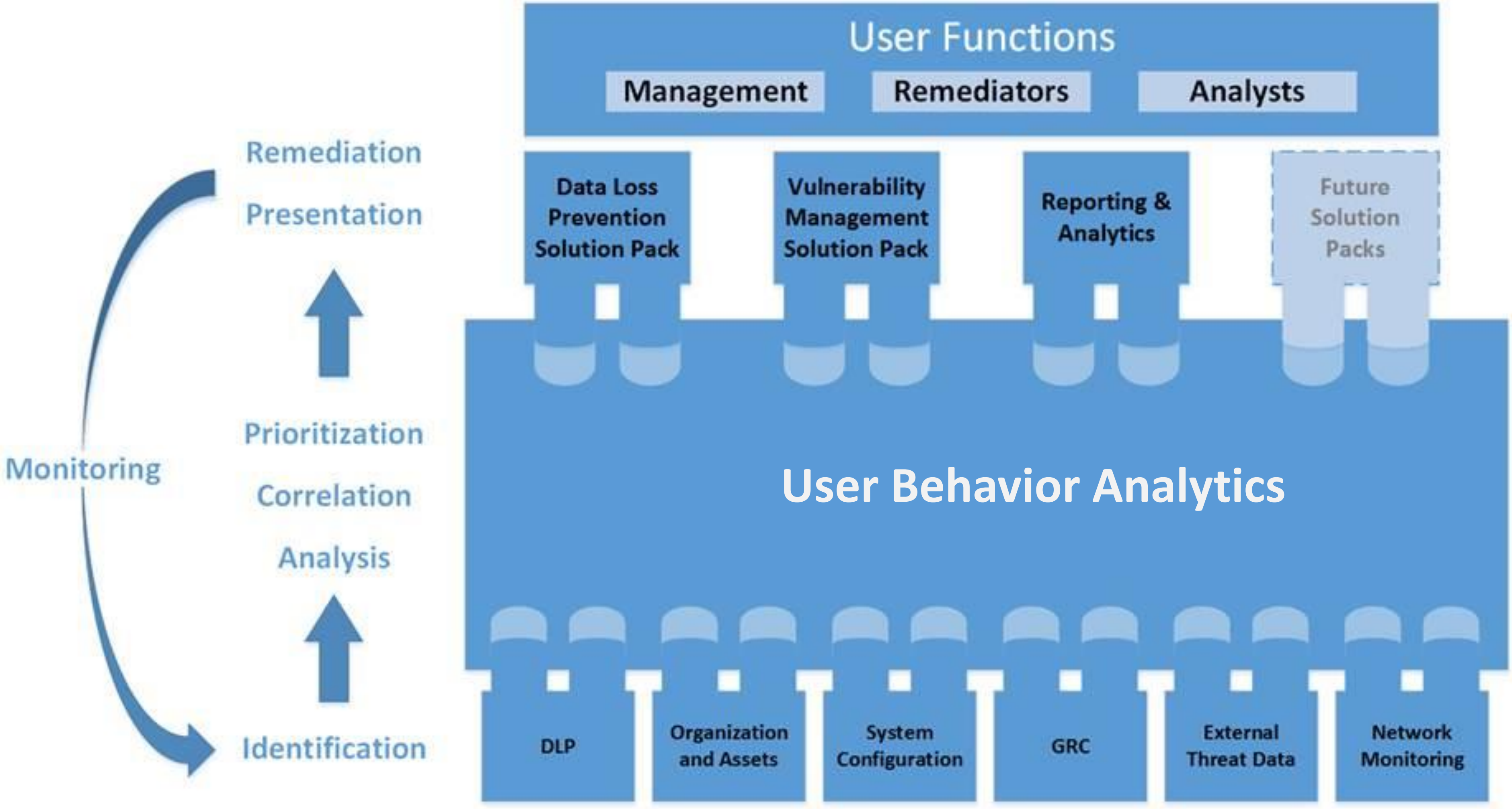
Applying User Behavior Analytics

- Using User Behavior Analytics **Companies** will **establish high-quality federated** user behavioral context or a story line **across their existing security solutions**.

- **Individual actions reporte**d in one security solution must be viewed in context to those of the same user reported in other solutions.

- What might appear to **be benign in isolation** may be indicative of a trend when reviewed in combination.

Unified Context – Gives you a Prioritized list of your Organization’s riskiest behaviors



Leverage existing security solutions

Gartner Market Guide for User Behavior Analytics

August 25, 2014

“While security information and event management (SIEM) supports activity monitoring with user context**, UBA technologies augment SIEM by enabling more effective exception monitoring due** to more advanced profiling and anomaly detection that is not dependent on IAM policy definitions for roles and authorization rights.”

“User Behavior Analytics (UBA) is transforming security and fraud management practices because it makes it much easier for enterprises to gain visibility into user behavior patterns to find offending actors and intruders.”

Strategic Planning Assumption(s)

By 2017, at least 80% of companies that adopt UBA will achieve at least **a 5-to-1 ROI** within one year of implementation by achieving productivity gains and lower security or fraud incidence costs.

- **3-1? 5-1? 10-1? No one disagrees there will be cost savings.**
- **More importantly, a safe secure infrastructure.**

Questions?