RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: PDIL-W02F

Understanding the Security Vendor Landscape Using the Cyber Defense Matrix

Sounil Yu

sounil@gmail.com

@sounilyu

#RSAC

Disclaimers

- The views, opinions, and positions expressed in this presentation are solely my own
- It does not necessarily represent the views and opinions of my employer and does not constitute or imply any endorsement from or usage by my employer

All models are wrong, but some are useful

- George E. P. Box

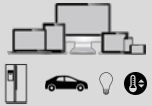
Our industry is full of jargon terms that make it difficult to understand what we are buying

To accelerate the maturity of our practice, we need a **common language**

Our common language can be bounded by five asset classes and the NIST Cybersecurity Framework

Asset Classes

DEVICES



Workstations, servers, VoIP phones, tablets, IoT, storage, network devices, infrastructure, etc.

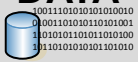
APPS

The software, interactions, and application flows on the devices

NETWORKS

The connections and traffic flowing among devices and applications

DATA



The information residing on, traveling through, or processed by the resources above

USERS

The people using the resources listed above

Operational Functions

IDENTIFY

Inventorying assets and vulns, measuring attack surface, baselining normal, risk profiling

PROTECT

Preventing or limiting impact, patching, containing, isolating, hardening, managing access, vuln remediation

DETECT

Discovering events, triggering on anomalies, hunting for intrusions, security analytics

RESPOND

Acting on events, eradicating intrusion footholds, assessing damage, coordinating, reconstructing events forensically

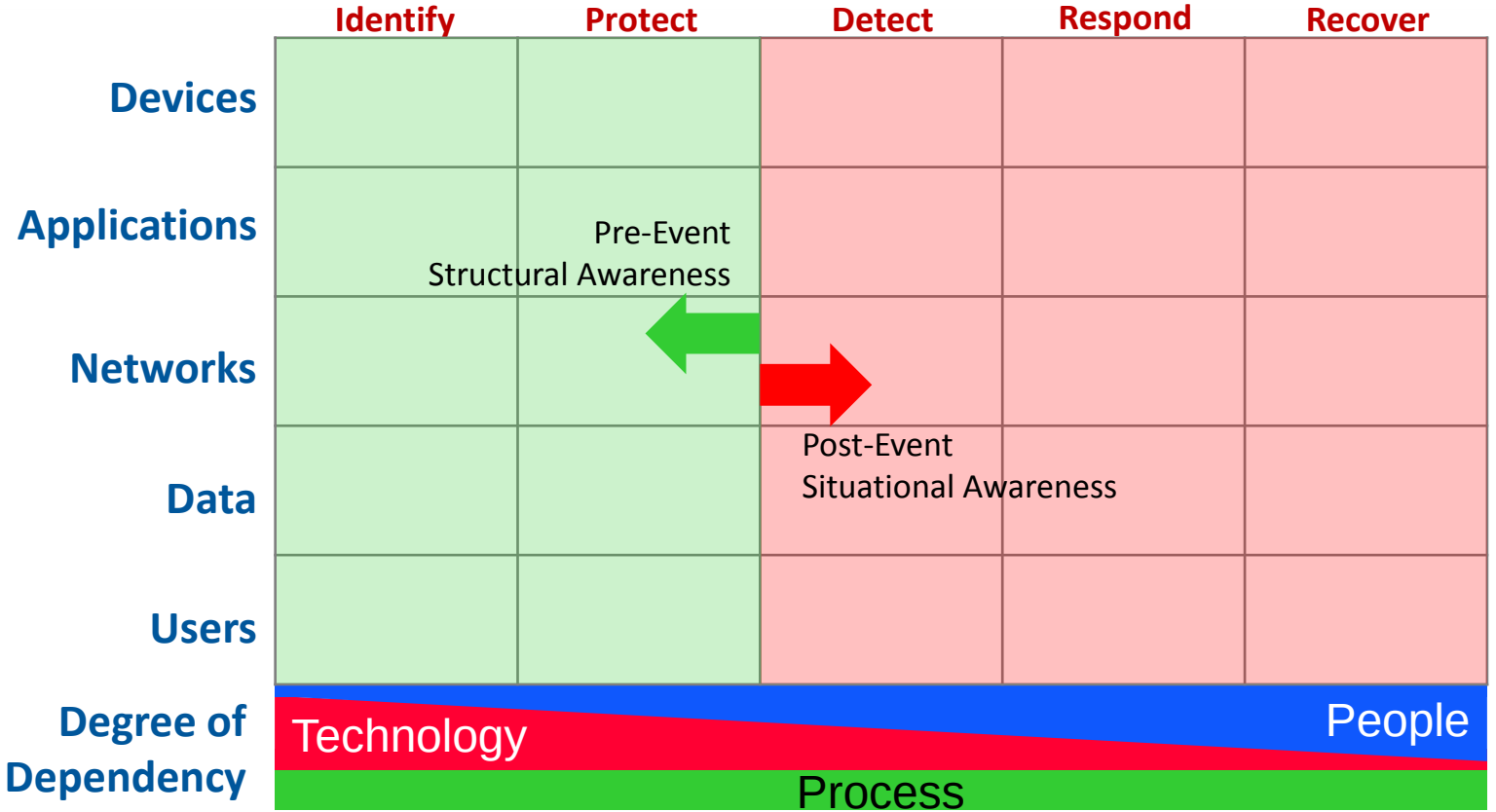
RECOVER

Returning to normal operations, restoring services, documenting lessons learned

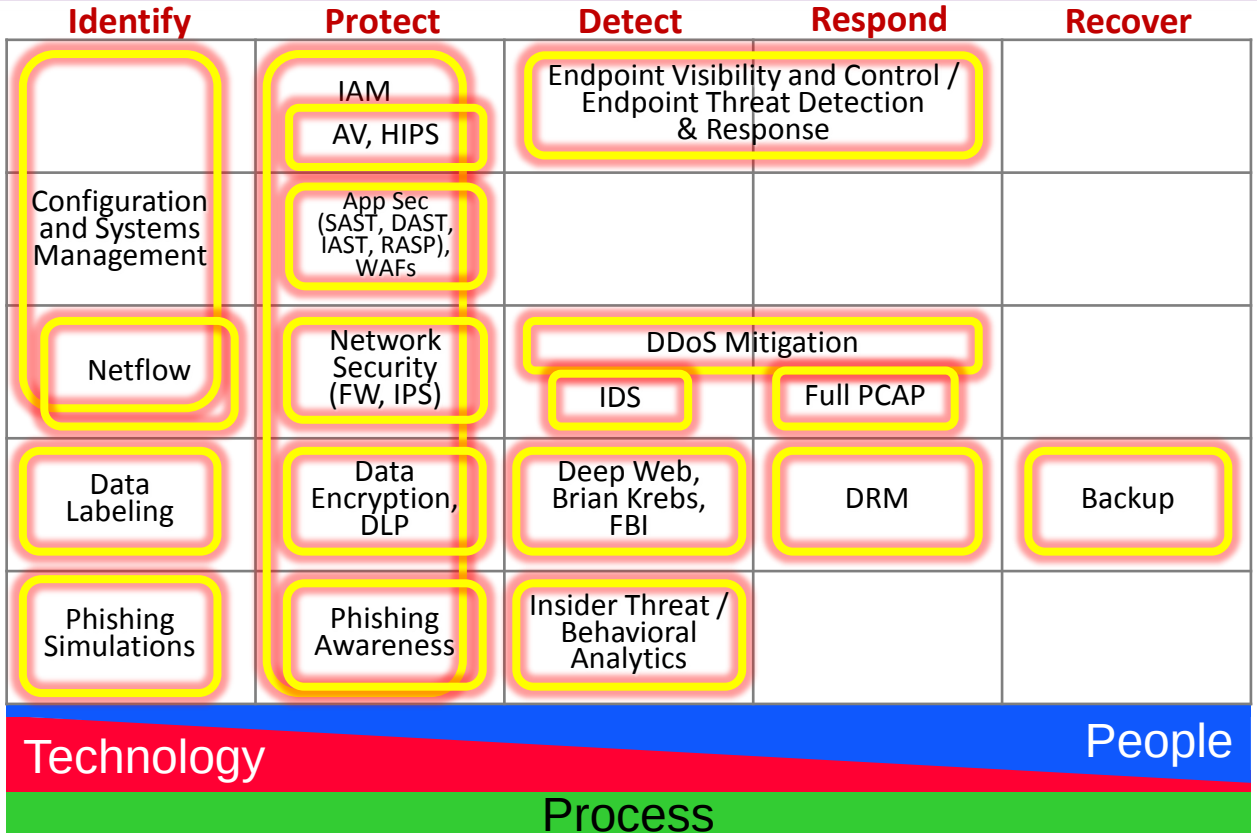
Introducing the “Cyber Defense Matrix”

	Identify	Protect	Detect	Respond	Recover
Devices					
Applications					
Networks					
Data					
Users					
Degree of Dependency	Technology / People				
	Process				

Left and Right of “Boom”



Enterprise Security Market Segments



We care about more than just the assets that are owned and controlled by the enterprise

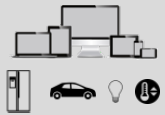
Threat Actors

Vendors

Customers

Employees

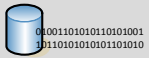
Enterprise Assets



- **Devices** - user workstations, servers, phones, tablets, IoT, peripherals, storage, network devices, web cameras, infrastructure devices, etc.

- **Applications** - The software, interactions, and application flows on the devices

- **Network** - The connections and traffic flowing among devices and applications



- **Data** - The information residing on, traveling through, or processed by the resources listed above

- **Users** – The people using the resources listed above

Operational Functions

- **Identify** – inventorying assets and vulnerabilities, measuring attack surface, baselining normal, risk profiling

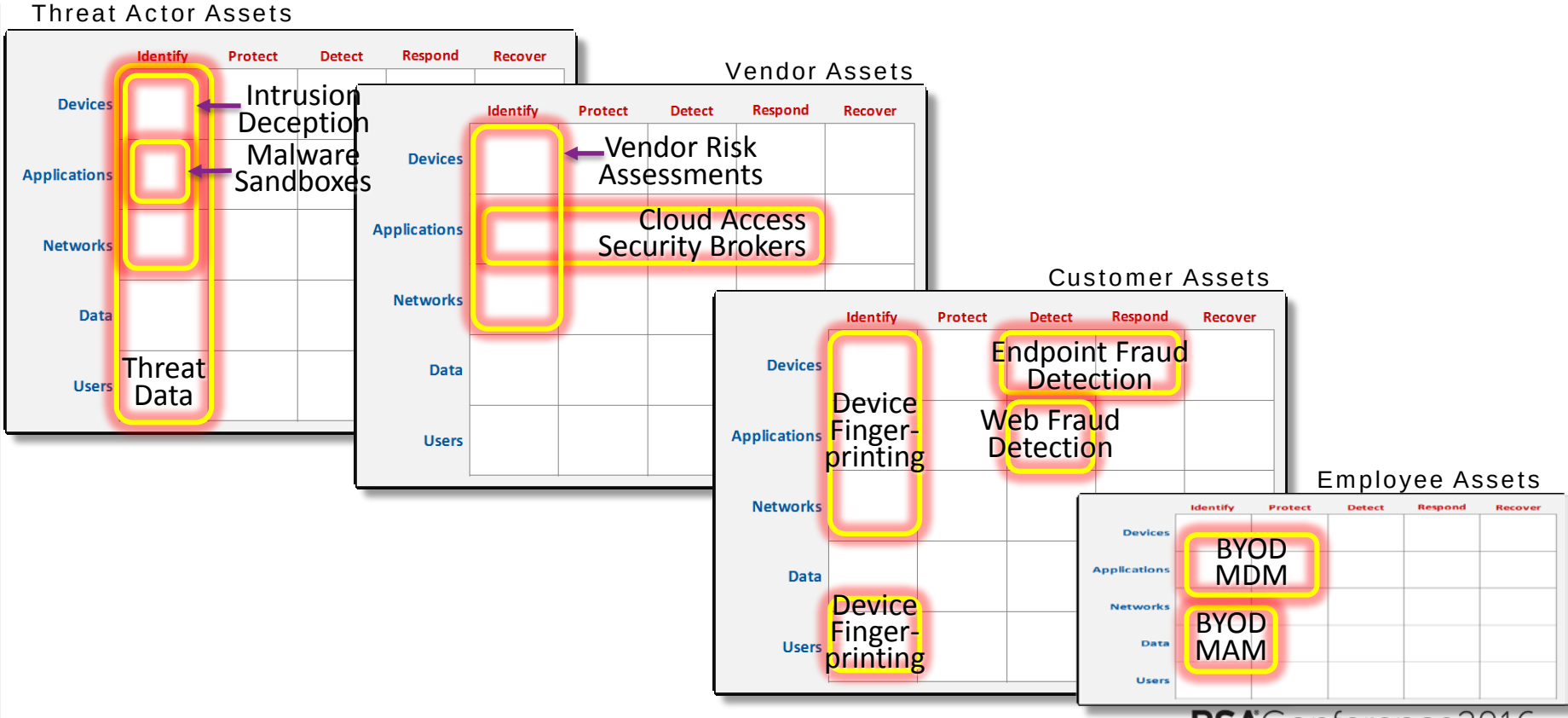
- **Protect** – preventing or limiting impact, patching, containing, isolating, hardening, managing access, vuln remediation

- **Detect** – discovering events, triggering on anomalies, hunting for intrusions, security analytics

- **Respond** – acting on events, eradicating intrusion footholds, assessing damage, coordinating response, forensics

- **Recover** – returning to normal operations, restoring services, documenting lessons learned

Market Segments – Other Environments



Security Technologies Mapped by Asset Class

DEVICES

Workstations, servers, VoIP phones, tablets, IoT, storage, network devices, infrastructure, etc.

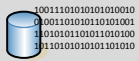
APPS

The software, interactions, and application flows on the devices

NETWORKS

The connections and traffic flowing among devices and applications

DATA



The information residing on, traveling through, or processed by the resources above

USERS

The people using the resources listed above

Disclaimer: Vendors shown are representative only. No usage or endorsement should be construed because they are shown here.

Security Technologies Mapped by Operational Functions

IDENTIFY	Inventorying assets, measuring attack surface, baselining normal, risk profiling
PROTECT	Preventing or limiting impact, containing, hardening, managing access
DETECT	Discovering events, triggering on anomalies, hunting for intrusions
RESPOND	Acting on events, eradicating intrusion footholds, assessing damage, coordinating, reconstructing events forensically
RECOVER	Returning to normal operations, restoring services, documenting lessons learned

TANIUM, Vormetric, BITSIGHT, tripwire, TITUS, THREATSTREAM, DOMAINTOOLS, skyhigh, RISKIQ, Lancope, BIOCATCH, ThreatMetrix, ForeScout, pindrop, ARBOR NETWORKS, CROWDSTRIKE, THREATCONNECT, comilion, LOOKINGGLASS, FARSIGHT SECURITY, DataGravity

AUTHENTIFY, VERACODE, ARXAN, BLUE COAT, waratek, Security Compass, Symantec, CYLANCE, CONTRAST SECURITY, paloalto, skyhigh, zscaler, CipherCloud, SafeNet, PHISHME, NowSecure, invincea, cigital, Malwarebytes, Bit9+CARBON BLACK, hpVoltage, INTRALINKS, CHECKMARX, MAGNUS, CYBERARK

Lancope, tripwire, TANIUM, lastline, SECURONIX, ZEROFOX, NETWORKS, EASYSOLUTIONS, Bit9+CARBON BLACK, FIDELIS CYBERSECURITY, FORCEPOINT, ARBOR NETWORKS, Dtex, SURUCUL, REDOWL, exabeam, CYPHORT, DARKSUM™, TRIUMFANT, DARKTRACE

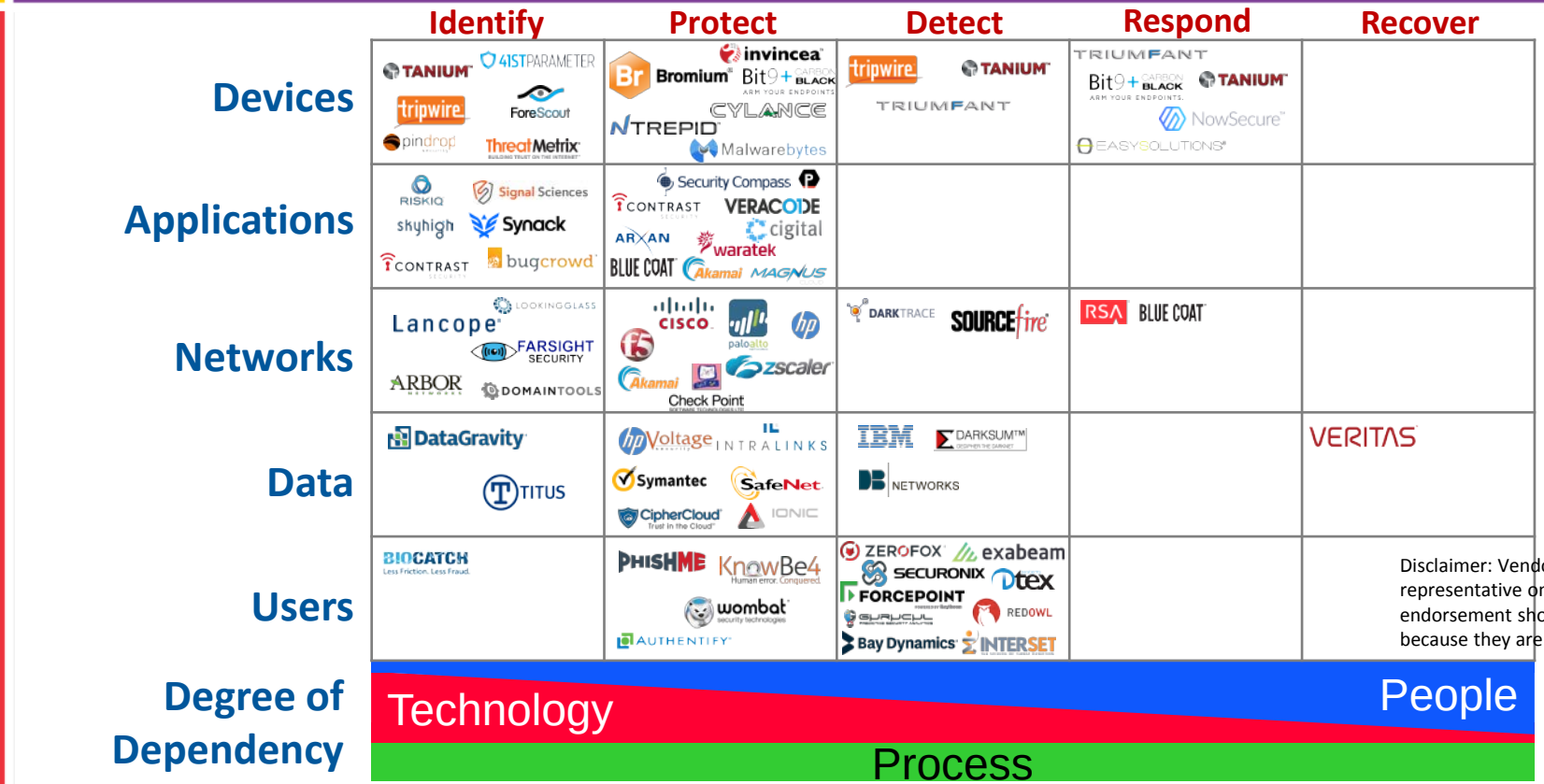
Bit9+CARBON BLACK, TANIUM, BLUE COAT, EASYSOLUTIONS, NowSecure, TRIUMFANT, RSA

MSSPs / IR: Deloitte., pwc, EY, accenture, Booz Allen

VERITAS

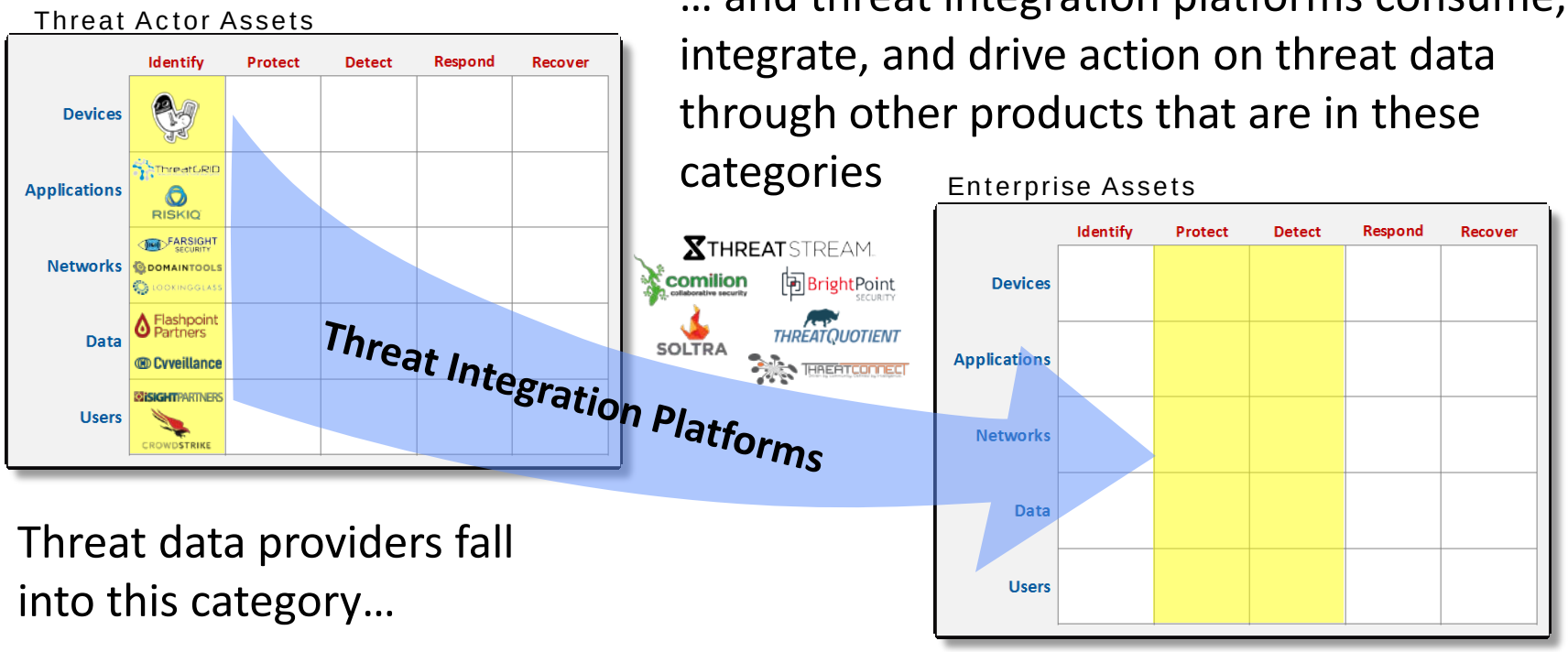
Disclaimer: Vendors shown are representative only. No usage or endorsement should be construed because they are shown here.

Security Technologies by Asset Classes & Operational Functions



Disclaimer: Vendors shown are representative only. No usage or endorsement should be construed because they are shown here.

Use Case 1: Understand how products in one area support the capabilities of another area



… and threat integration platforms consume, integrate, and drive action on threat data through other products that are in these categories

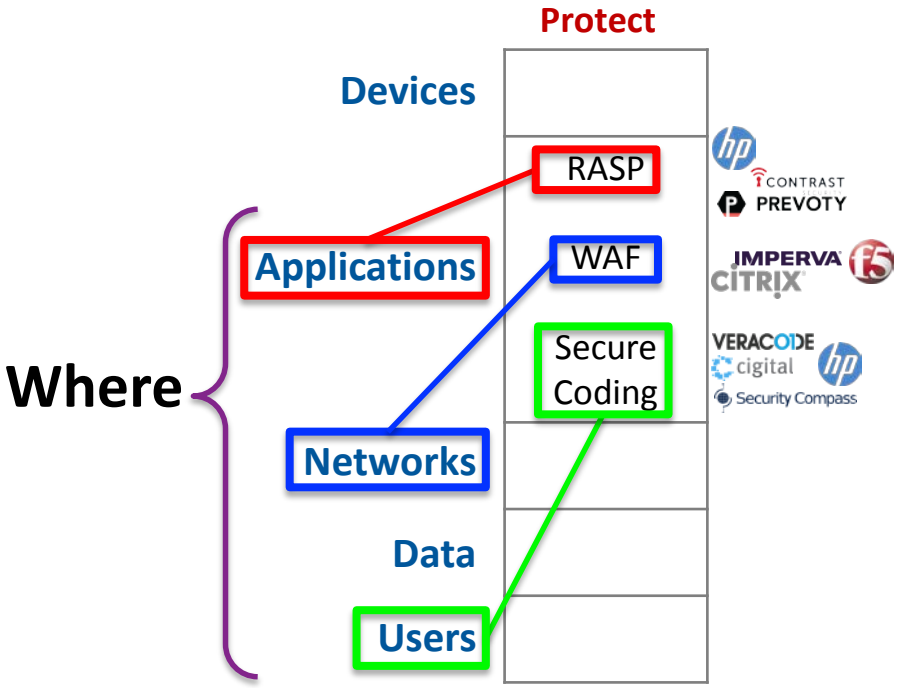
Threat data providers fall into this category…

Use Case 2: Define Security Design Patterns (a.k.a. Security Bingo Card)

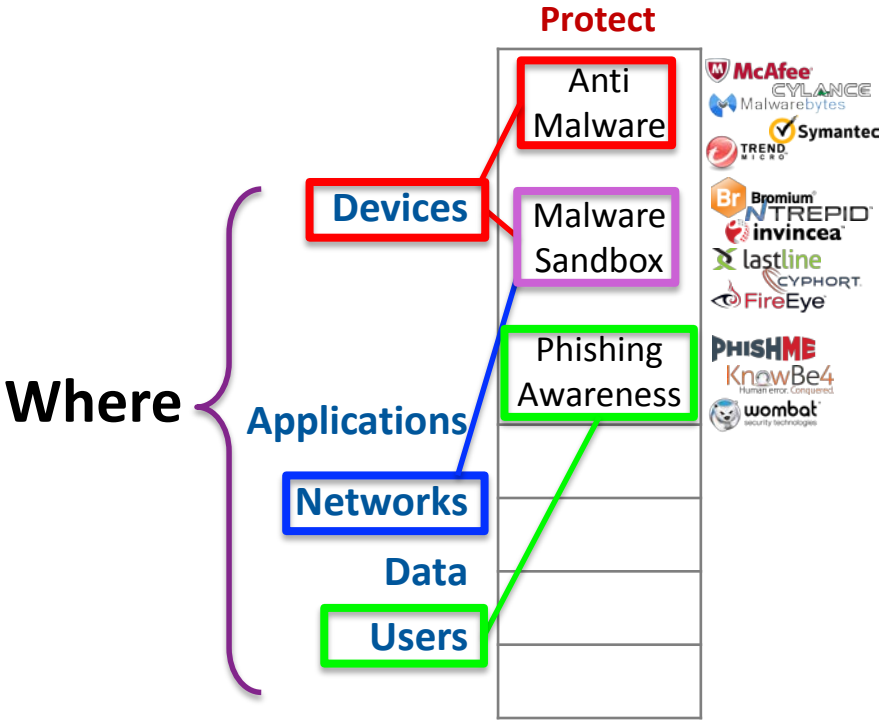
	Identify	Protect	Detect	Respond	Recover
Devices		X	X		X
Applications	X	X		X	X
Networks	X		X	X	
Data		X	X		X
Users	X			X	

Use Case 3: Maximizing Your Available Deployment Footprint (What vs Where)

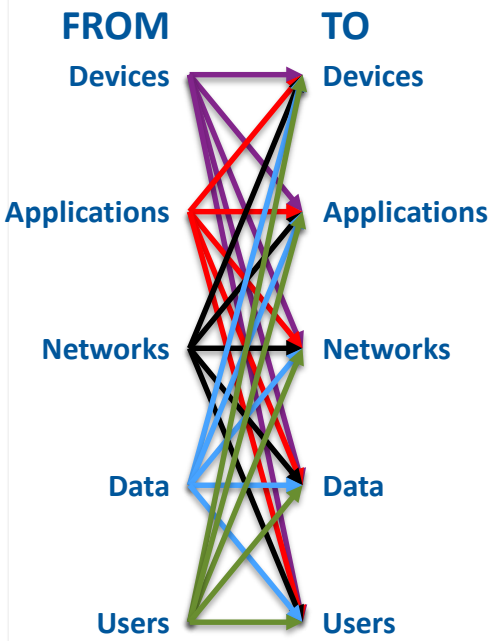
What: Application Security



What: Endpoint Protection



Use Case 4: The (network) perimeter is dead. Long live (other) perimeters



PROTECT

FROM \ TO	Devices	Apps	Networks	Data	Users
Devices	• SSH Certificates	• Client-side SSL Cert • Geofencing • Fingerprinting	• NAC	• Encryption keys	• ?
Apps	• Server-Side SSL Cert	• API Key	• ?	• Encryption keys	• Enhanced SSL Certificates
Networks	• 802.1X Certificate	• ?	• Firewall Rules	• ?	• ?
Data	• Hashes / Checksums	• Hashes / Checksums	• ?	• ?	• Hashes / Checksums
Users	• User Creds • Biometrics • 2FA	• User Creds • Biometrics • 2FA	• User Creds • 2FA	• User Creds • 2FA	• Photo ID • Handshake

Reduce/Eliminate these perimeters to make security more usable

Use Case 5: Calculate Defense-in-Depth

	Identify	Protect	Detect	Respond	Recover	D-in-D Score
Devices		0.25	0.40		0.20	0.64
Applications	0.20	0.10		0.10	0.15	0.45
Networks	0.15		0.10	0.20		0.39
Data		0.05	0.10		0.20	0.32
Users	0.30			0.10		0.37
Defense in Depth Score	0.52	0.36	0.51	0.35	0.46	44 (sum of columns and row *100)

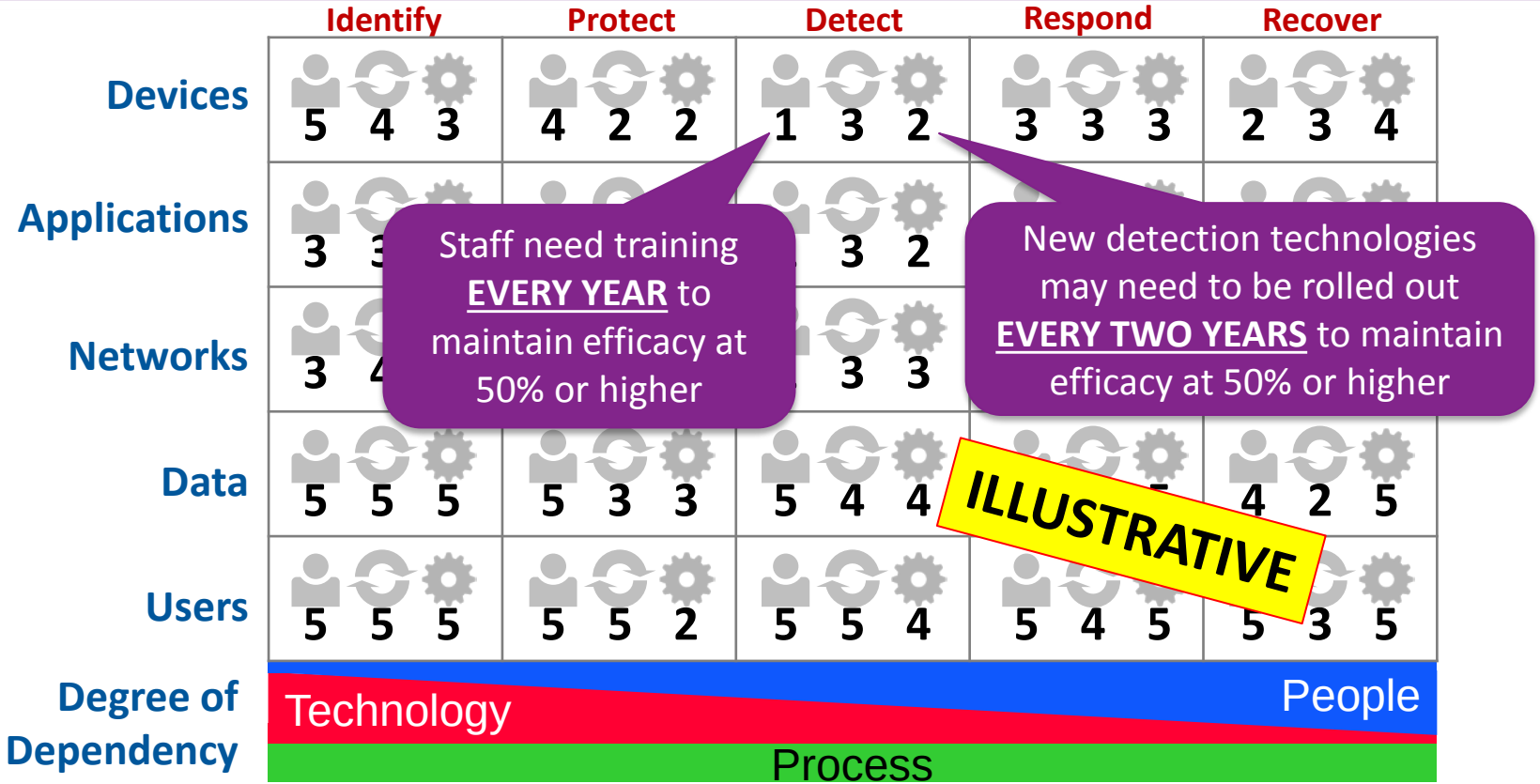
ILLUSTRATIVE

Use Case 6: Understand how to balance your portfolio without breaking the bank

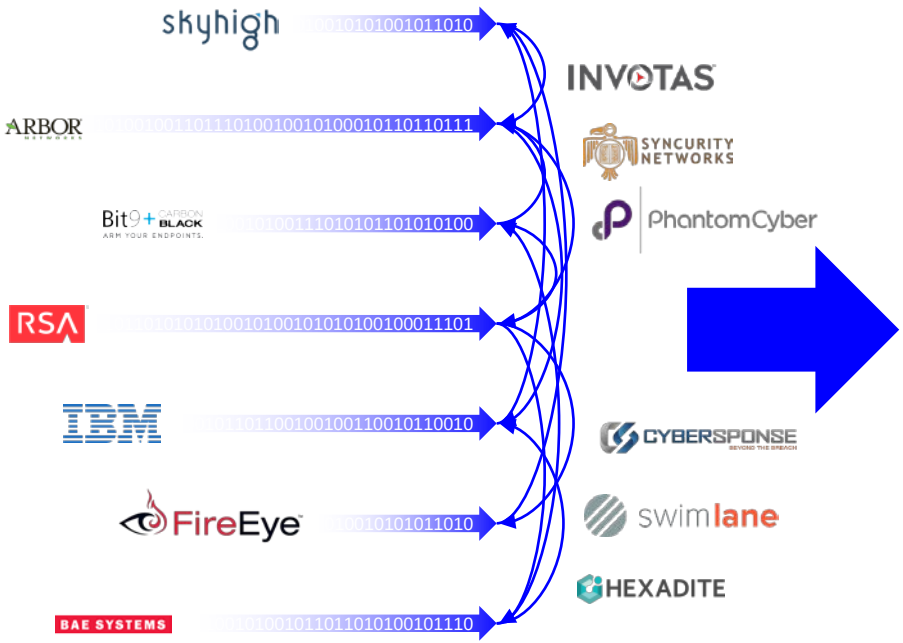
	Identify	Protect	Detect	Respond	Recover	Total
Devices		$50	$100		$50	$200
Applications	$50	$100		$50	$100	$300
Networks	$100		$100	$50		$250
Data		$50	$50		$50	$150
Users	$50			$50		$100
Total	$200	$200	$250	$150	$200	$1000

ILLUSTRATIVE

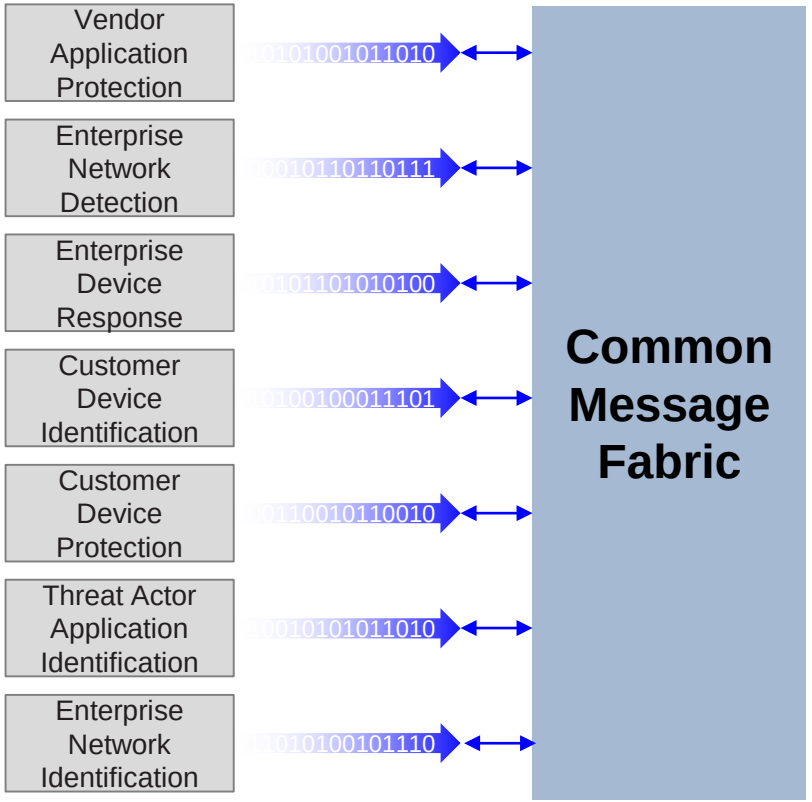
Use Case 7: Anticipate the "Effective Half Life" of People Skills, Processes, and Technologies



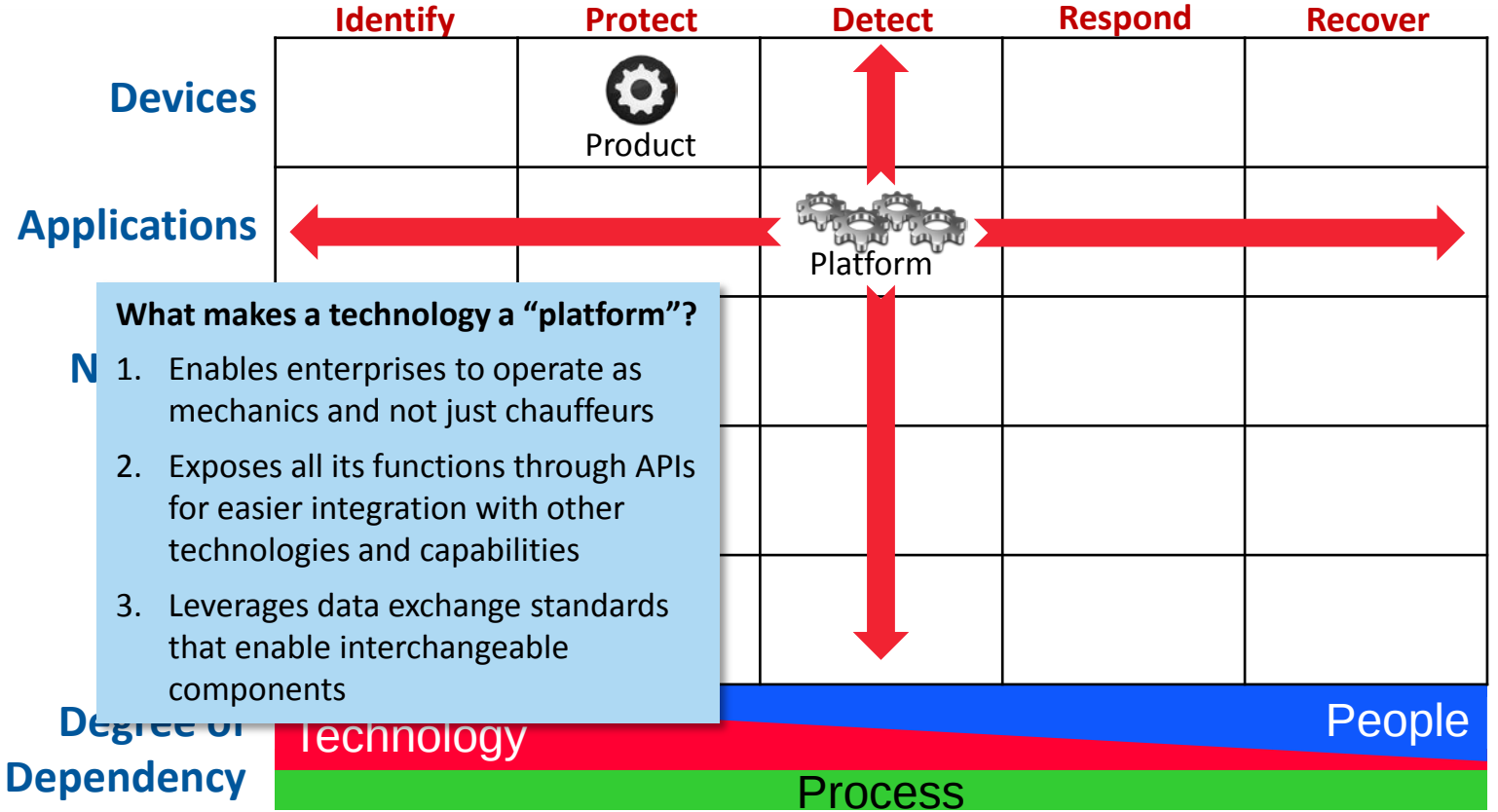
Use Case 8: Disintermediate Components for Easier Orchestration



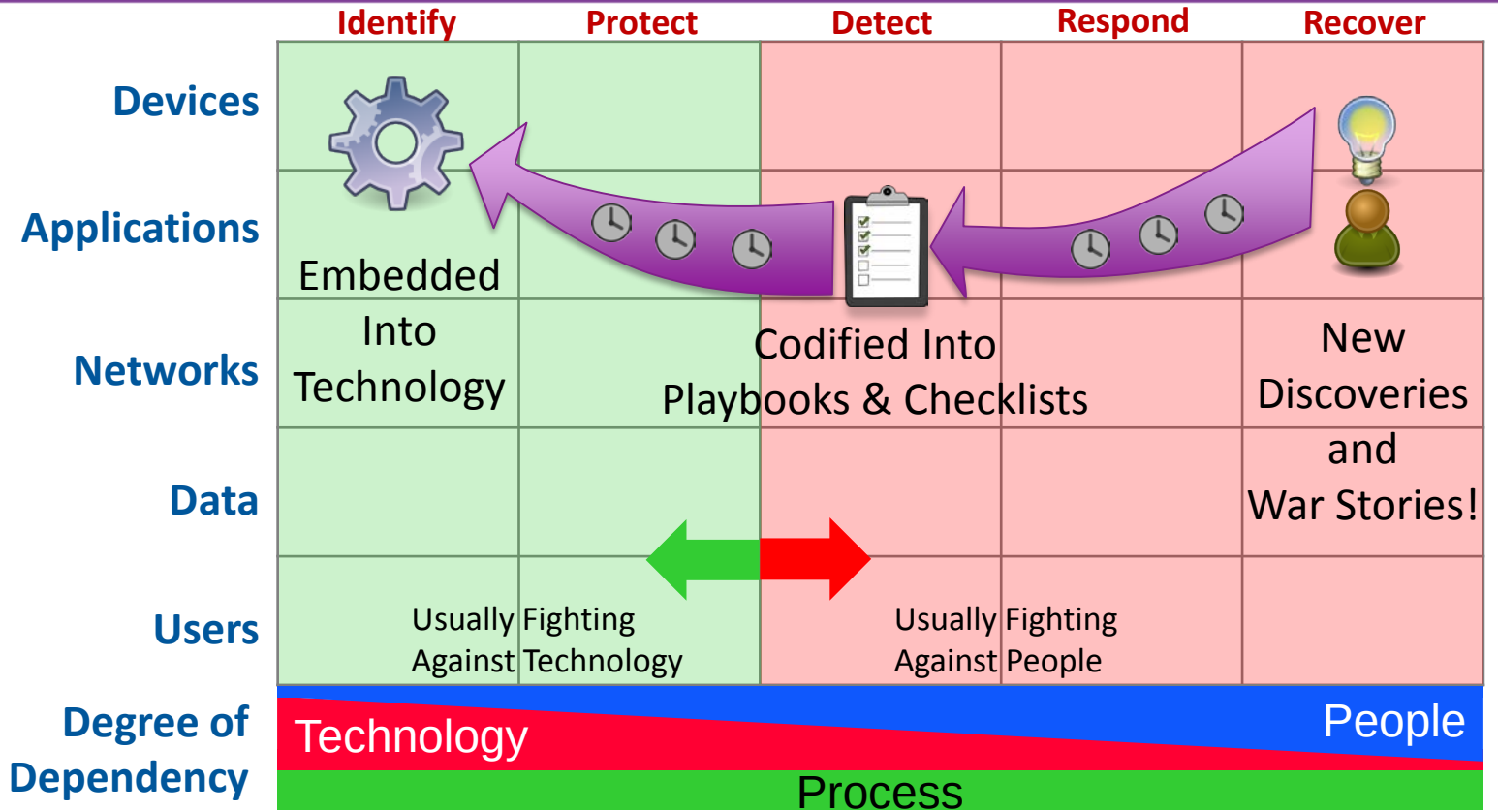
Disclaimer: Vendors shown are representative only. No usage or endorsement should be construed because they are shown here.



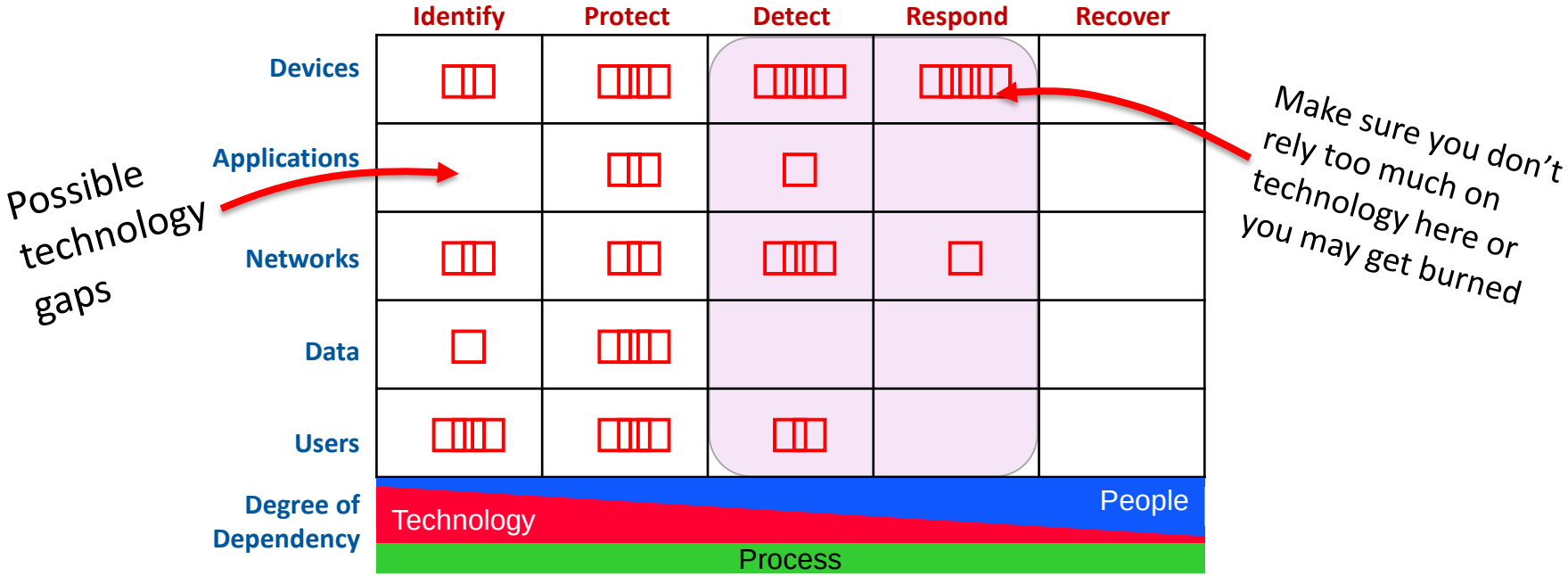
Use Case 9: Differentiate between a platform and a product



Use Case 10: Identifying Opportunities to Accelerate the People>Process>Technology Lifecycle

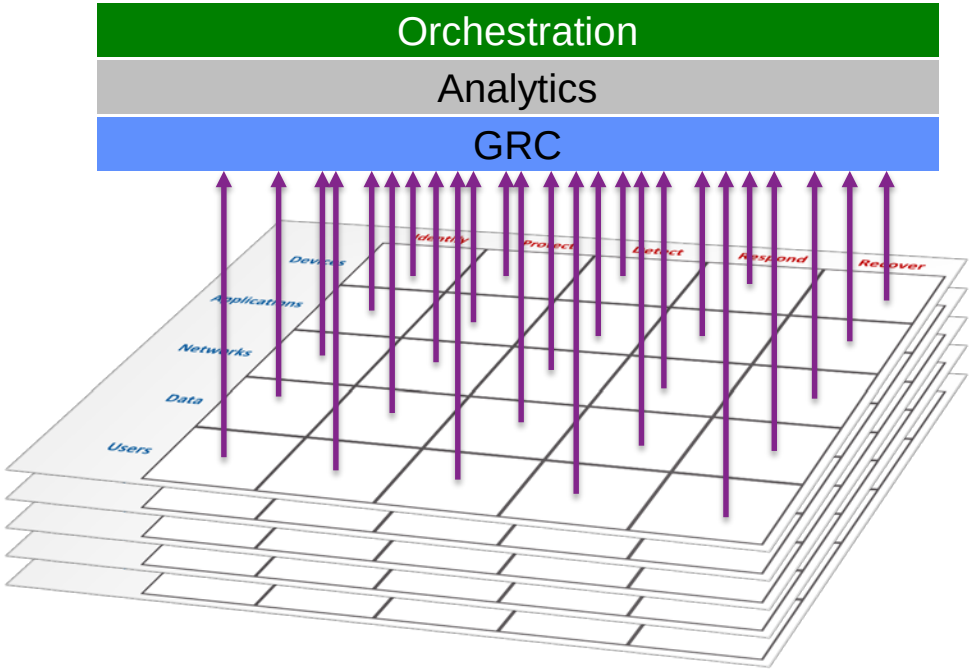


Use Case 11: Identify technology gaps or overreliance in your technology portfolio

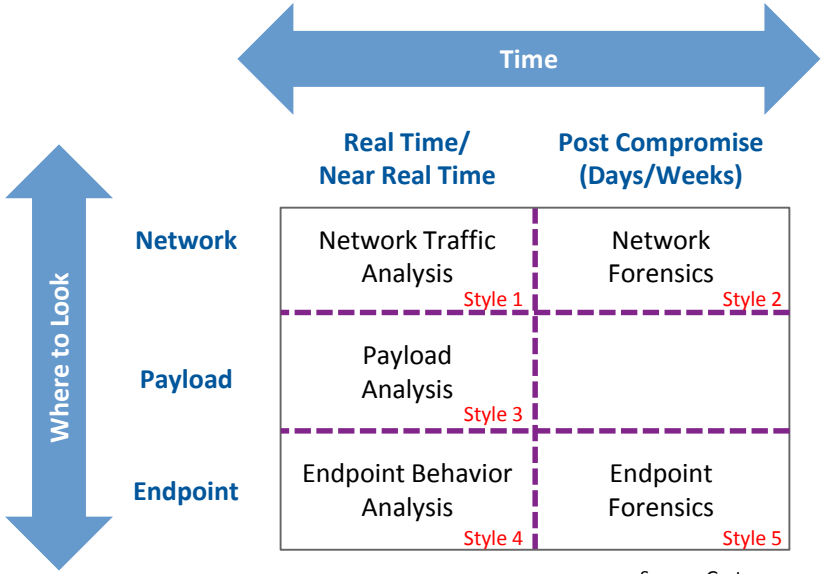


Model Shortfalls: Where is analytics? GRC? Orchestration?

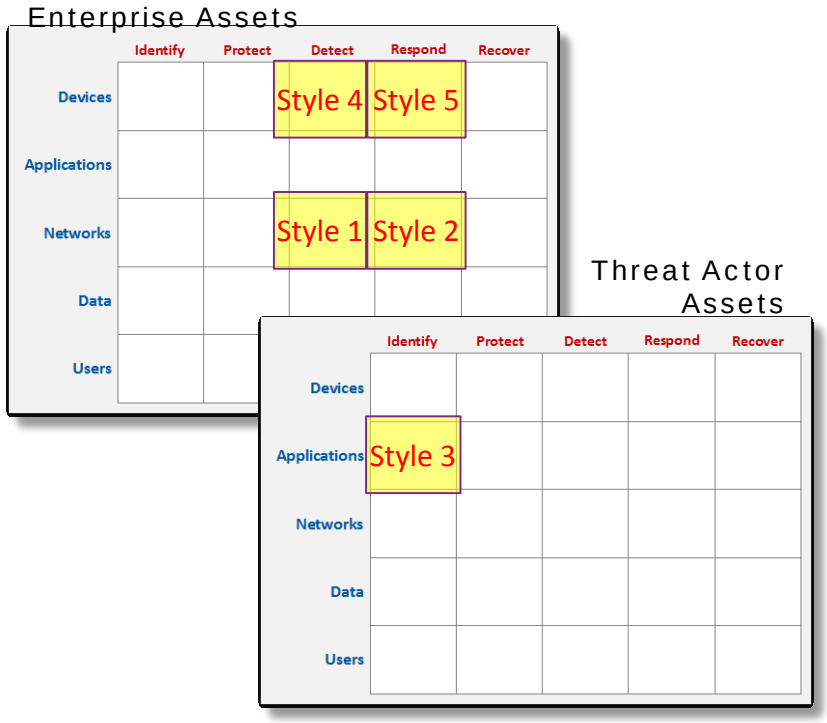
This framework supports the higher level functions of orchestration, analytics, and governance/risk/compliance, but they are represented on a different dimension



Comparison of Models: Gartner's Five Styles of Advanced Threat Defense

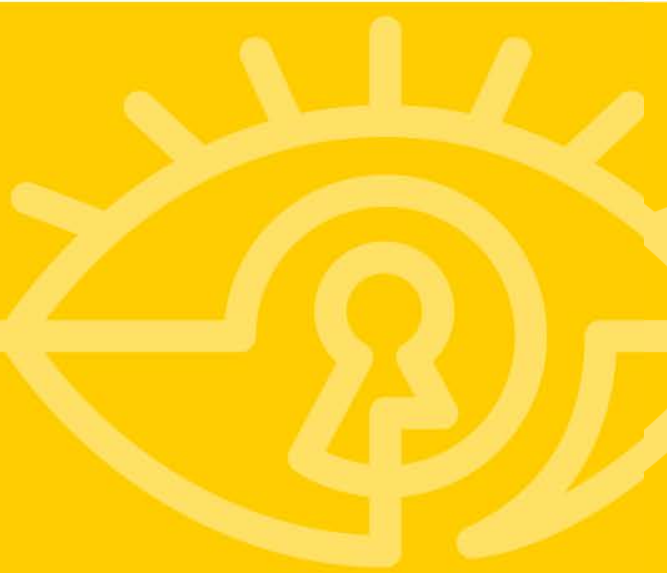


Source: Gartner



Applying the Cyber Defense Matrix

- This week
  - Use the matrix to categorize vendors that you encounter in the Expo Hall
  - Ask them where they fit and don't allow them to be in multiple shopping aisles
- In the first three months following this presentation you should:
  - Send me feedback on how you have mapped vendors to it
  - Organize your portfolio of technologies to see where you might have gaps
  - Identify vendors that may round out your portfolio based on your security design pattern (a.k.a. security bingo card)
- Within six months you should:
  - Send me feedback on how you used the Cyber Defense Matrix and improved it



Sounil Yu
sounil@gmail.com