CYBERSECURITY ROADMAP: GLOBAL HEALTHCARE SECURITY ARCHITECTURE

Nick H. Yoo

DISCLOSURE

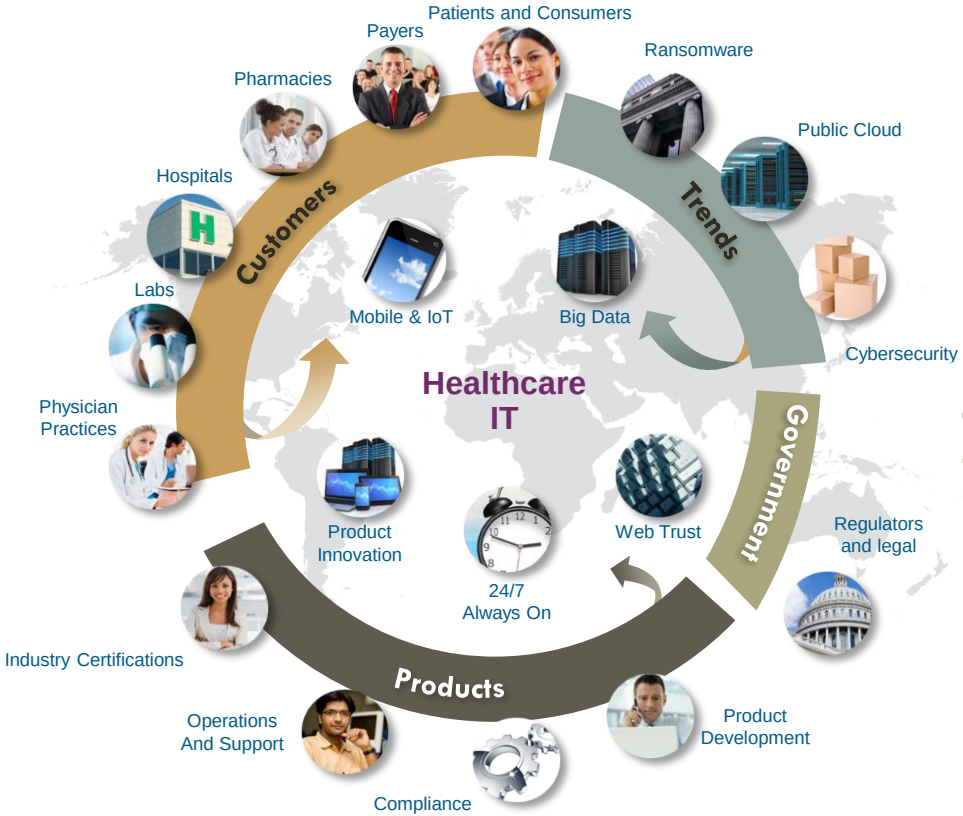
No affiliation to any vendor products

No vendor endorsements

Products represented here are just examples

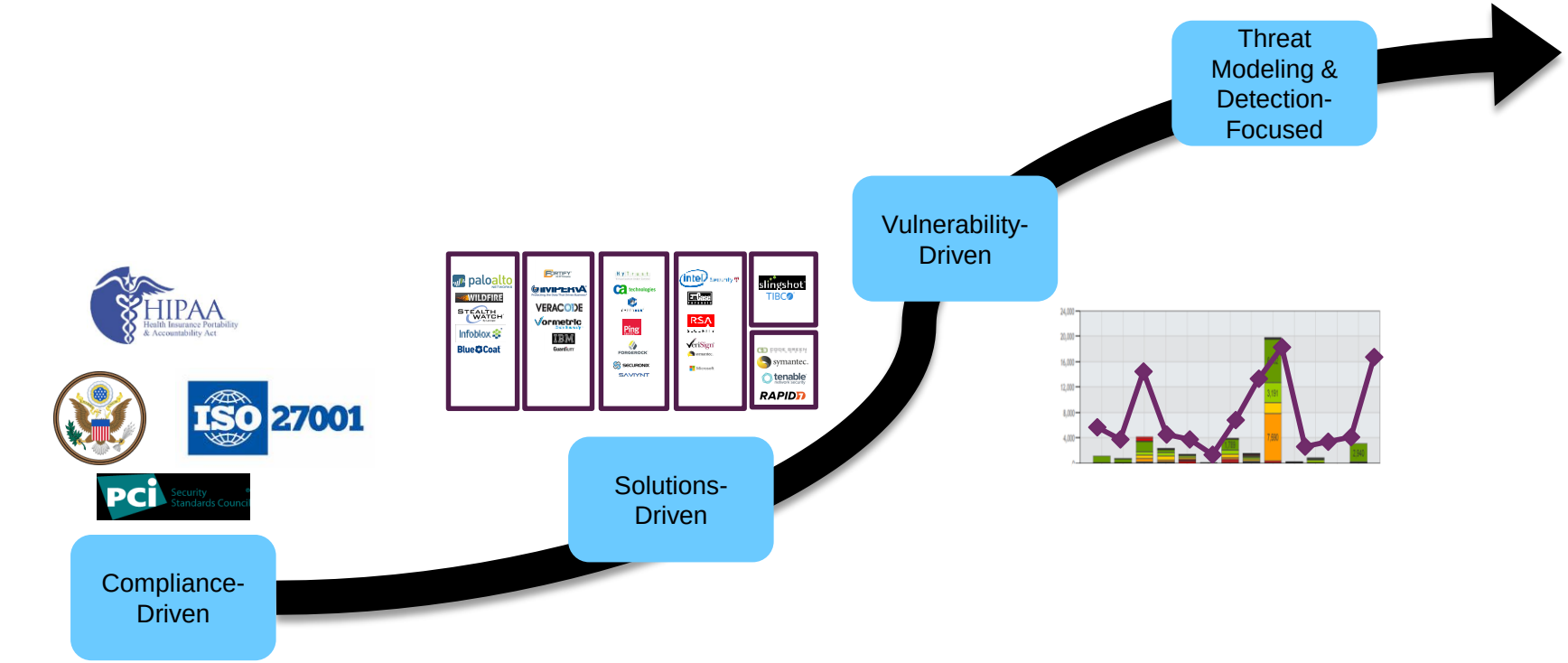
References to any gaps, product information, and roadmaps are mainly for illustrative purposes and do not represent any specific companies

HEALTHCARE IT CHALLENGES



Healthcare Industry is Increasingly Difficult to Protect & Is becoming a Rich Target

CYBERSECURITY JOURNEY



"Perimeter Security"

"Layered Security"

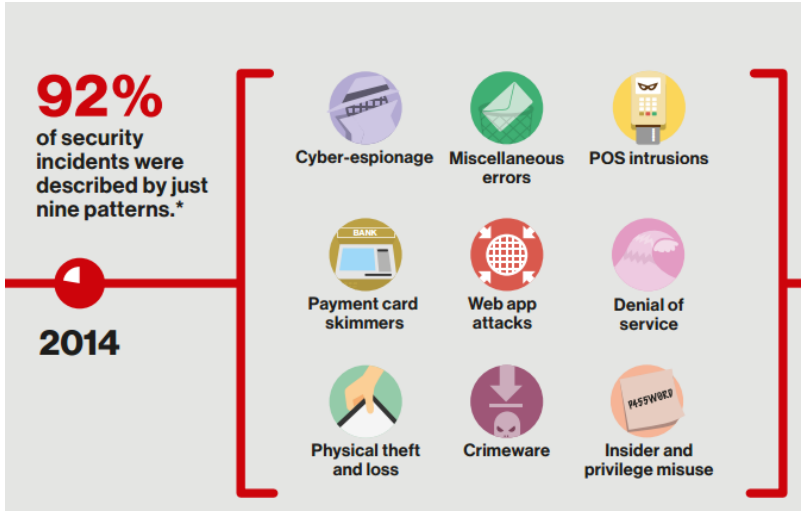
""Identity as New Perimeter"

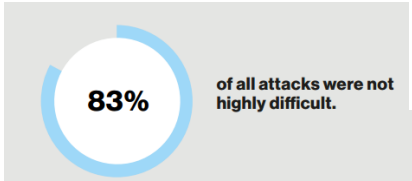
SECURITY TECHNOLOGY LANDSCAPE

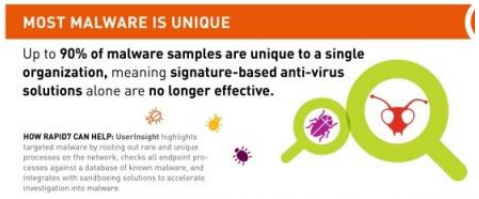
TECHNOLOGY OVERVIEW

130	Total # of Products
70	Total # of Vendors
20	Most # of Products by Domain: IAM
10	Most # of Capabilities covered by one Vendor
160	Total # of Capabilities covered by Product
8	Least # of Products by Domain: Monitoring, Analytics & Audit
30	Approximate # of Products: EOL, Obsolete in 12 – 24 Month

THREAT LANDSCAPE





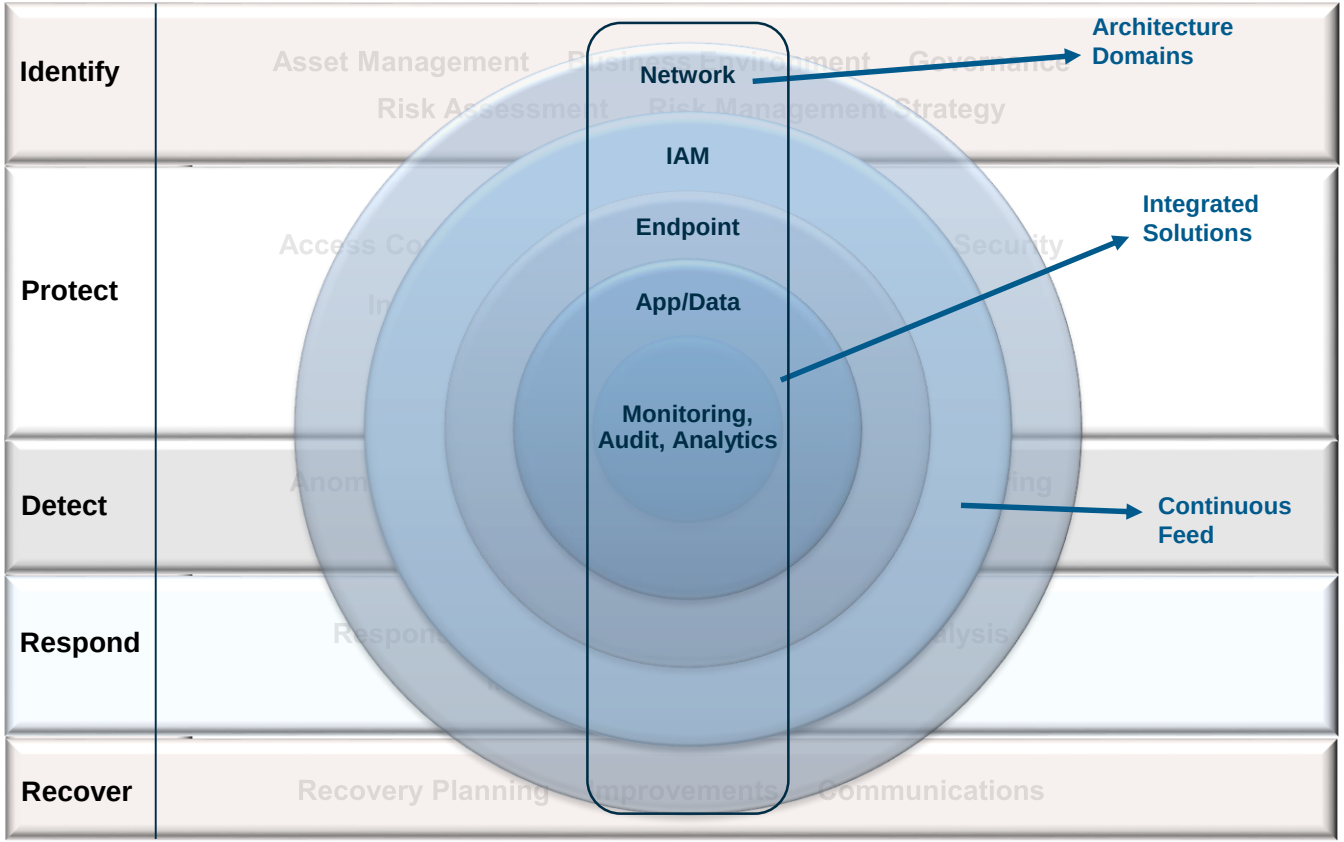


Source: Verizon Data Breach Report

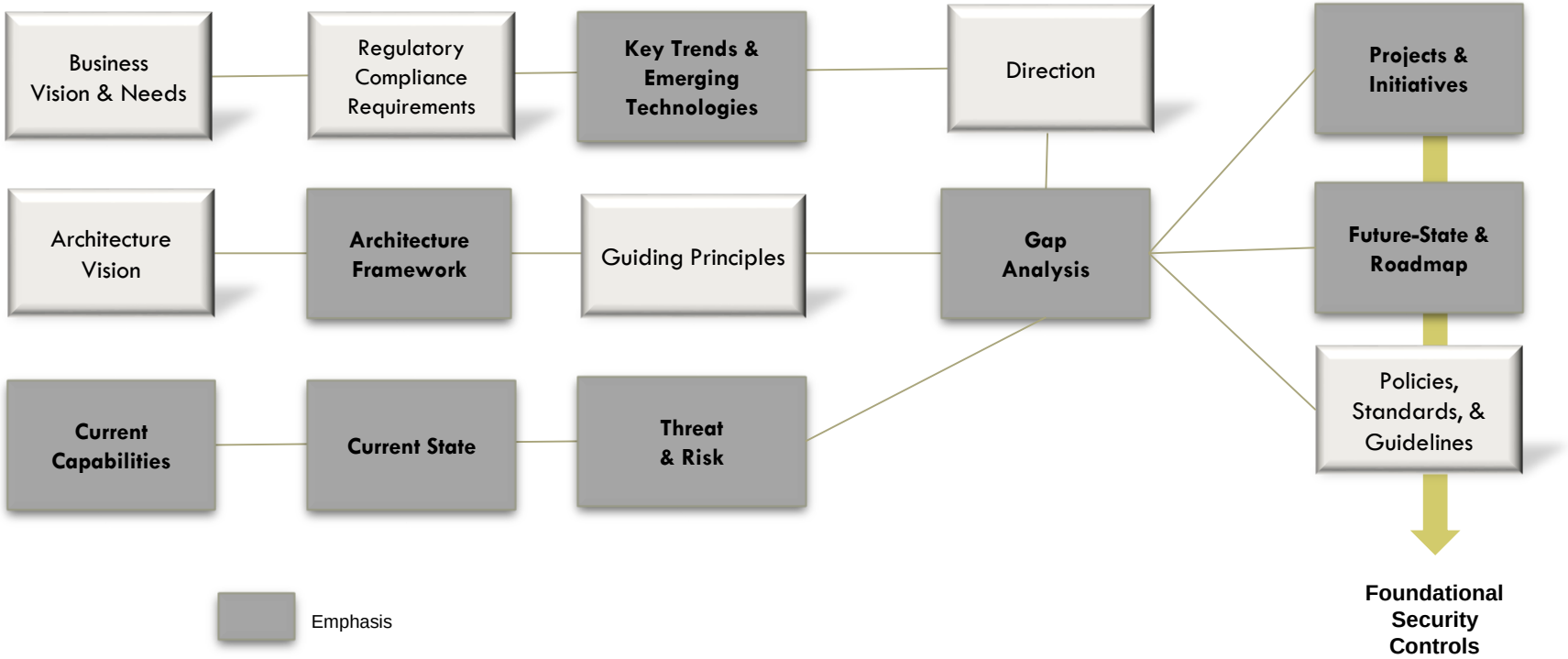
NIST CYBERSECURITY FRAMEWORK

Identify	**Asset Management Business Environment Governance Risk Assessment Risk Management Strategy**
Protect	**Access Control Awareness and Training Data Security Information Protection Process & Procedures Maintenance Protective Technology**
Detect	**Anomalies and Events Security Continuous Monitoring Detection Processes**
Respond	**Response Planning Communications Analysis Mitigation Improvements**
Recover	**Recovery Planning Improvements Communications**

CYBERSECURITY ARCHITECTURE FRAMEWORK



ARCHITECTURE DEVELOPMENT APPROACH

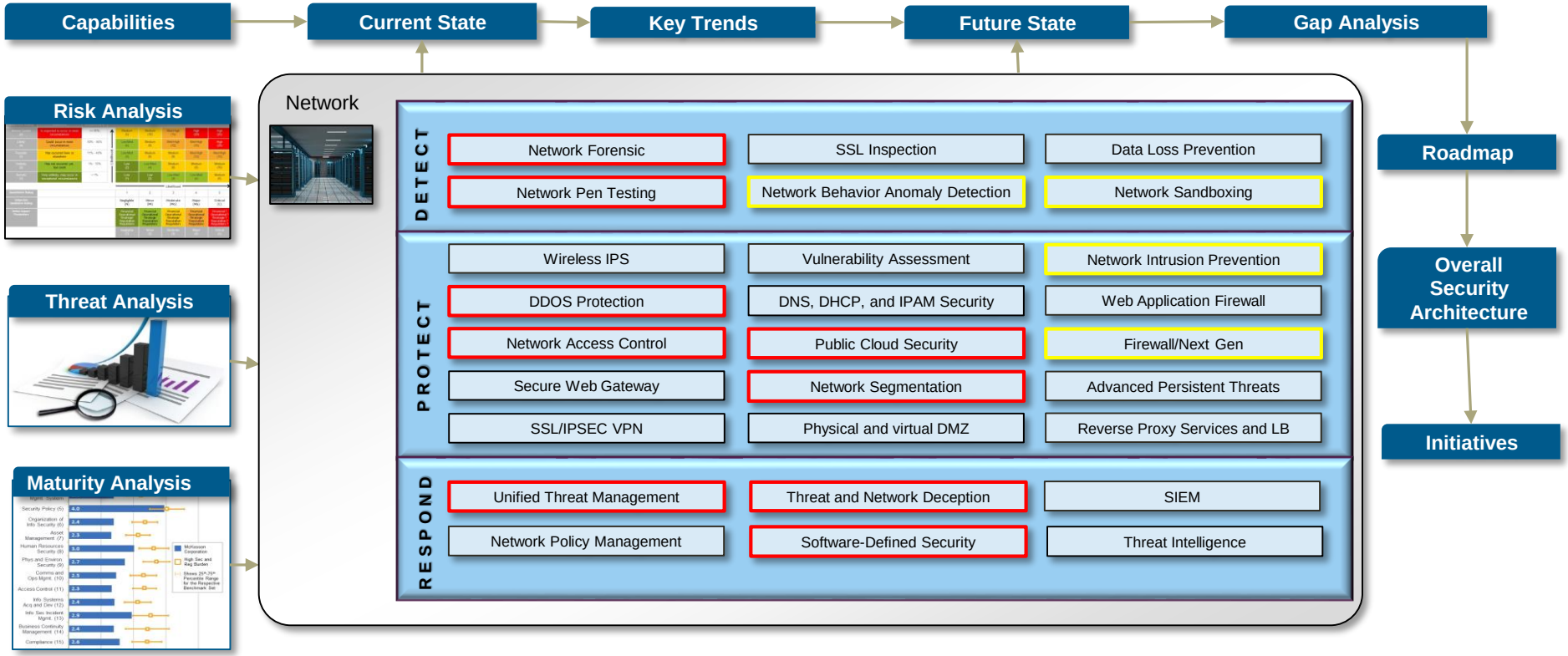


KEY TRENDS

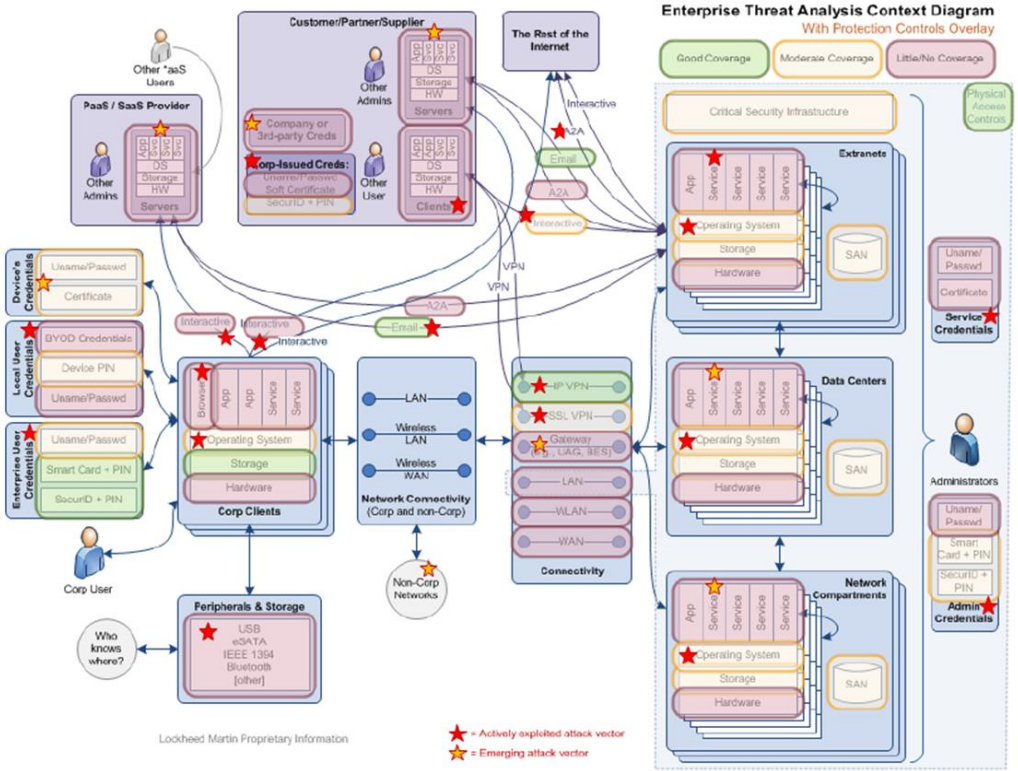
- From blocking and detecting attacks to detecting and responding to attacks
- Rapid breach detection using endpoint threat detection and remediation tools
- Aggressive segmentation of the network
- Spot abnormal user and session behavior by conducting continuous monitoring, behavioral analytics and identity verification
- Use big data analytics of transactions, security events and contextual information to gain faster and smarter correlation of security incidents so they can be rapidly prioritized.
- Use and contribute to shared threat intelligence and fraud exchange services.

Source: Gartner

CYBERSECURITY ROADMAP DEVELOPMENT PROCESS NETWORK EXAMPLE

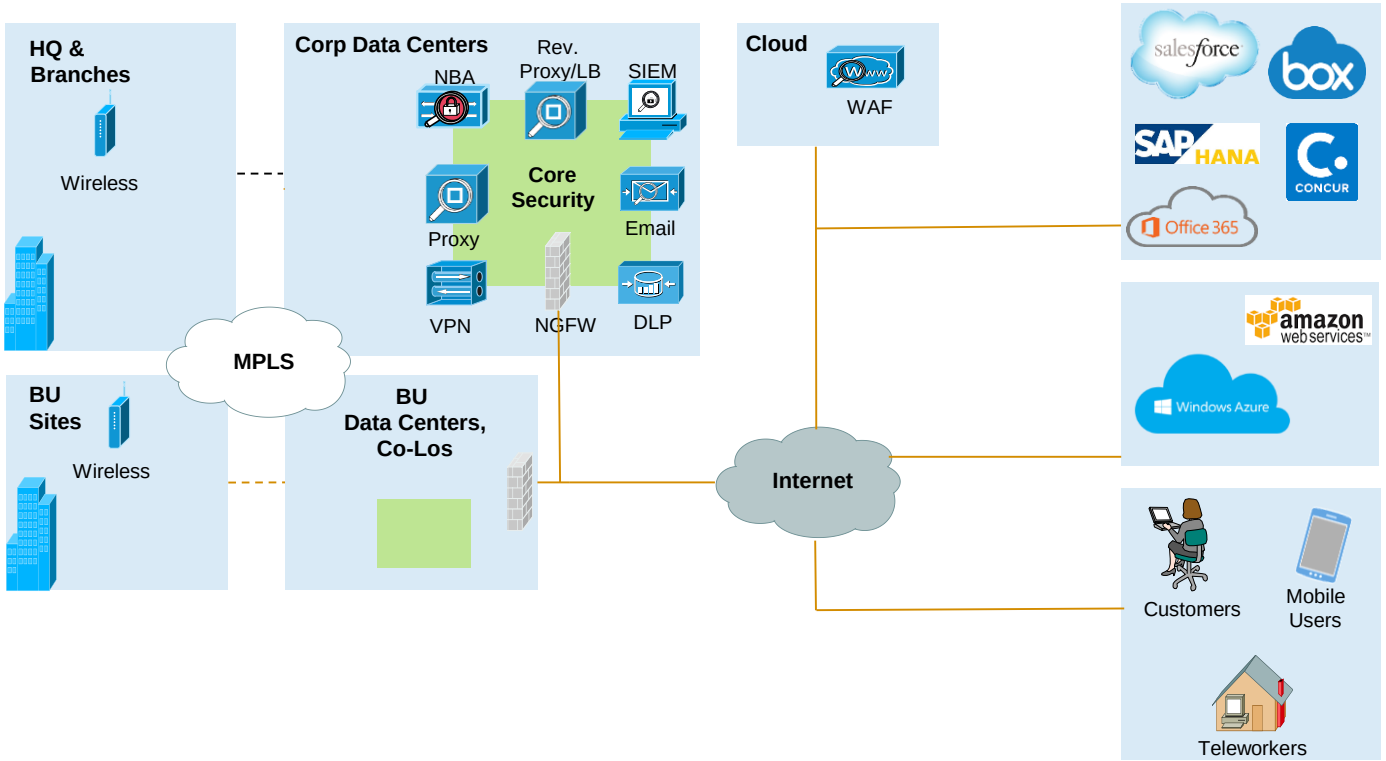


THREAT MODELING

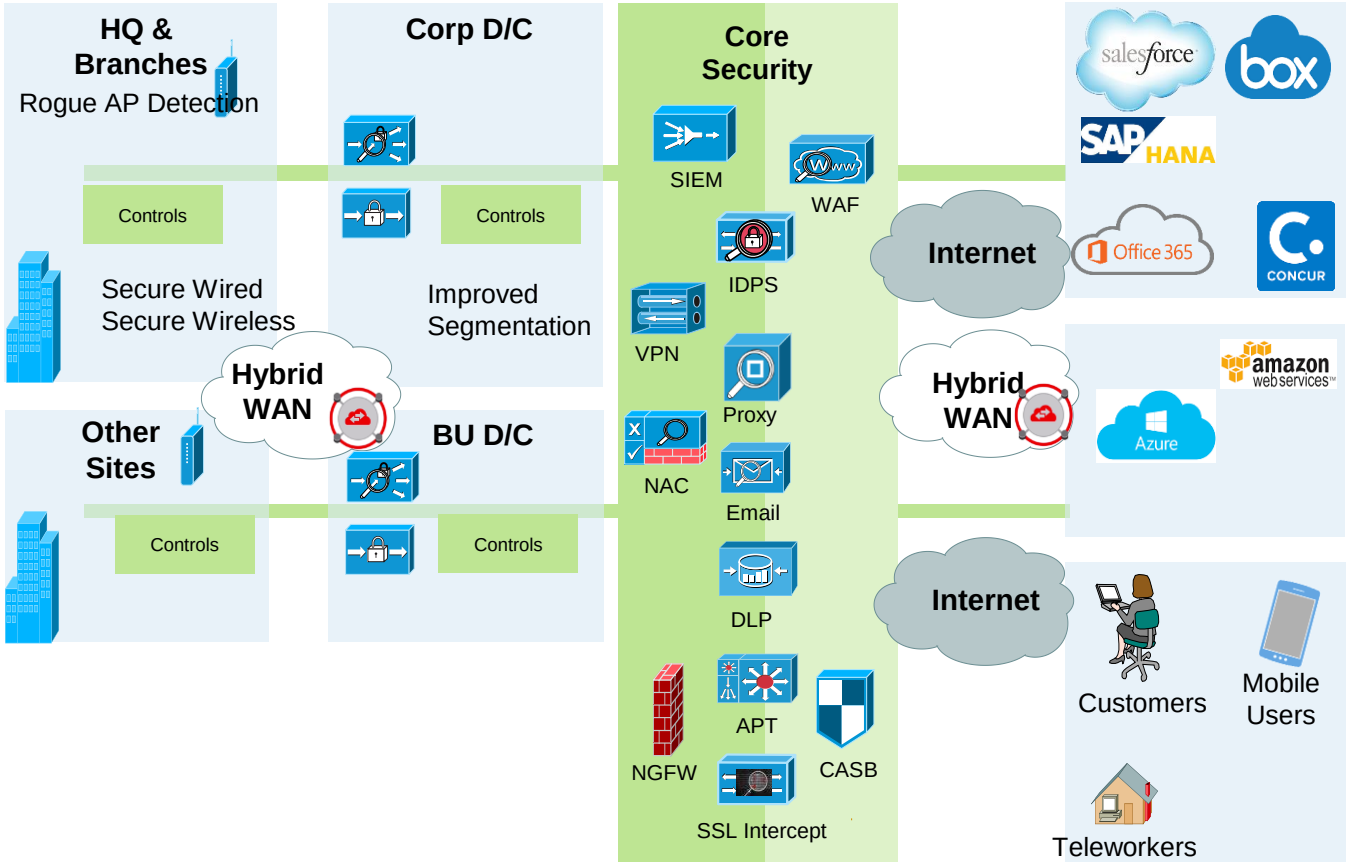


Source: Lockheed Martin

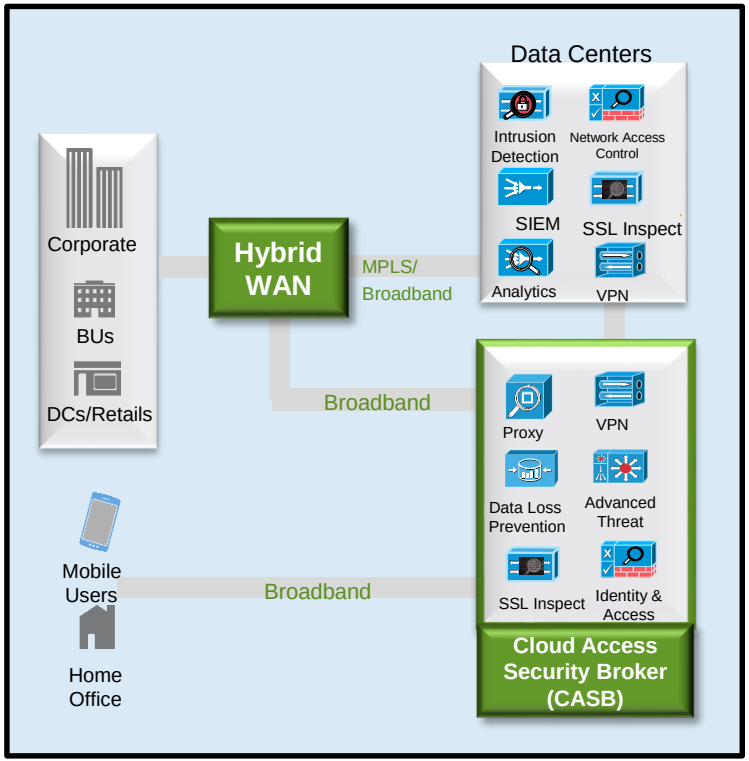
CURRENT NETWORK ARCHITECTURE

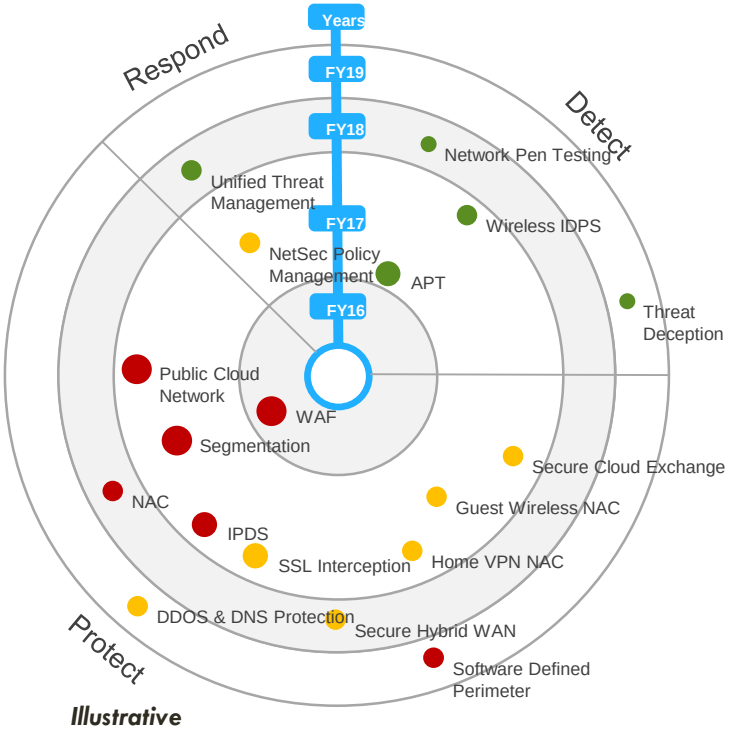


FUTURE STATE NETWORK ARCHITECTURE

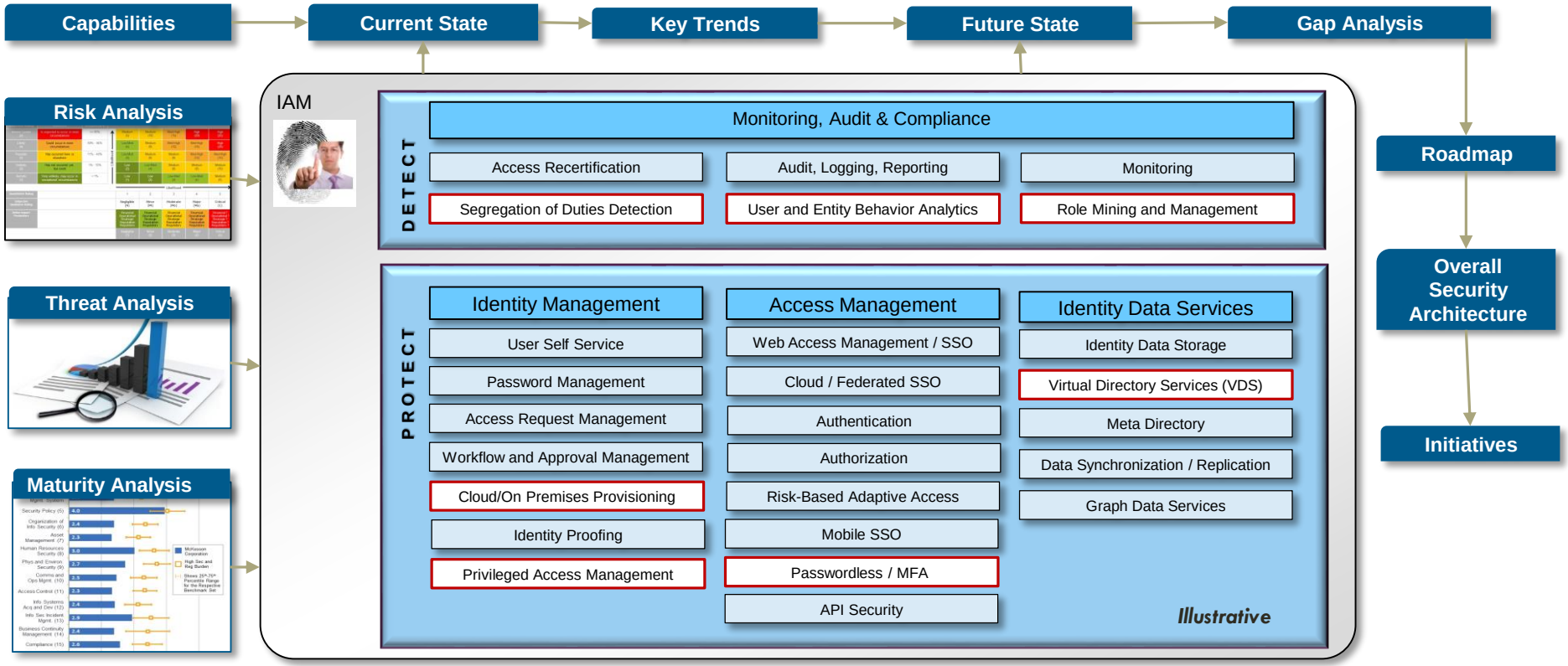


ARCHITECTURE & ROADMAP

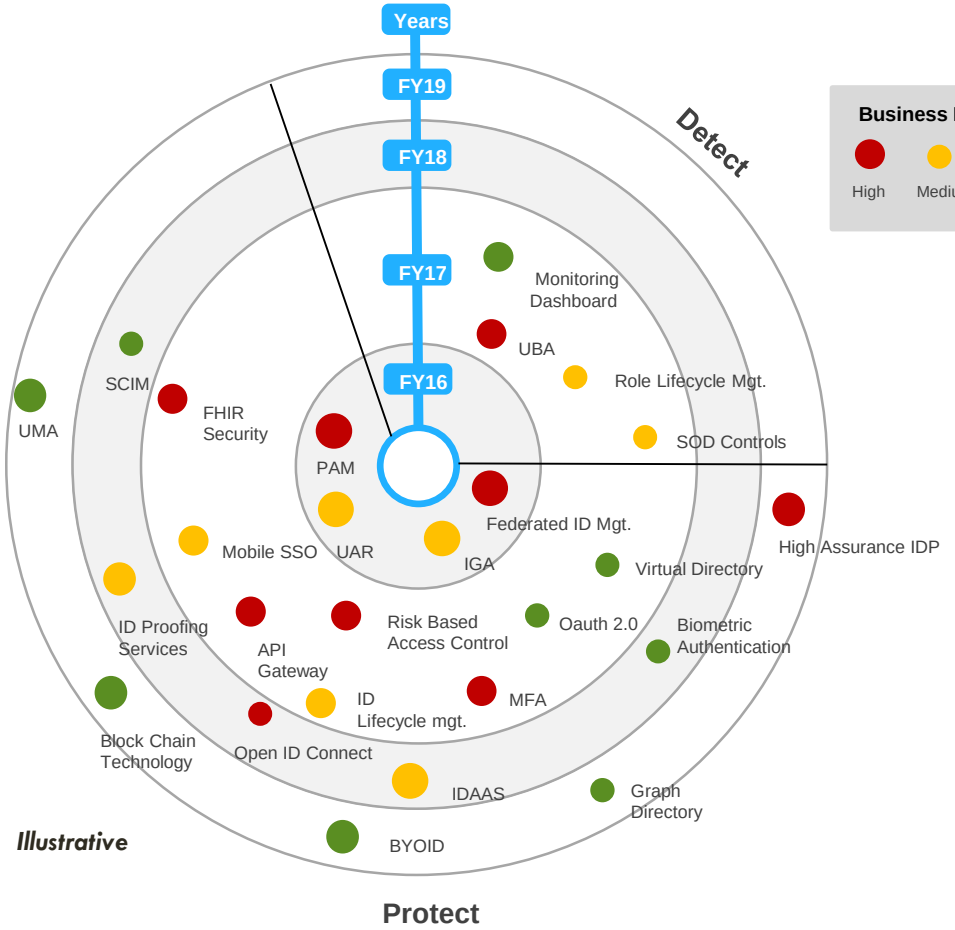


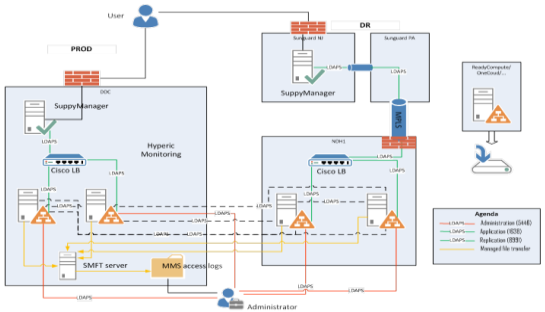


CYBERSECURITY ROADMAP DEVELOPMENT PROCESS
IAM EXAMPLE



IAM TECHNOLOGY ROADMAP





CYBERSECURITY FRAMEWORK DOMAIN MAPPING

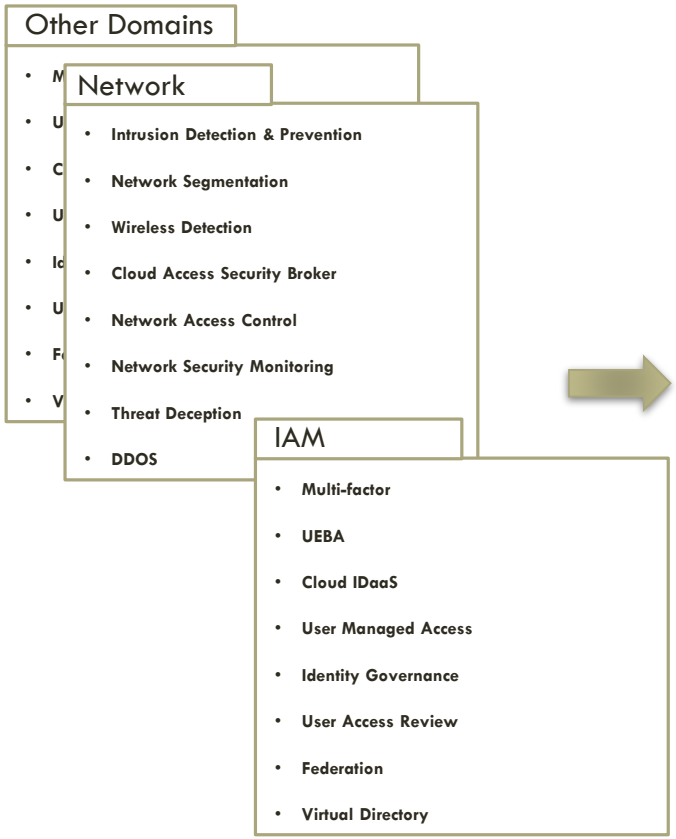
Cybersecurity Framework	Network	IAM	Endpoint	App/ Data	Monitor
Identify					
Protect					
Detect					
Respond					
Recover					

Rating Scale	Description
	Fully Meet
	Usually Meet
	Partially Meet
	Rarely Meet
	Does Not Meet

Observations
• Sufficient coverage for endpoint • Network domain lacks detection controls • Overall lack of detection controls • Monitoring capability exist mainly in the Protect

Illustrative

KEY INITIATIVES



Advanced Detection

Security Analytics

Advanced Endpoint Protection & Detection

Threat Intelligence

Application Security

Adaptive Authentication (IAM)

Malware protection system

Cloud Security

CORE SOLUTIONS ARCHITECTURE

Illustrative

SUMMARY

- NIST – comprehensive, risk-based, proactive
- Guideline, flexibility
- Knowing your assets
- Threat actors, method, and appropriate controls (segmentation, encryption)
- Architectural analysis

Source: Gartner