Today's Predictions for Tomorrow's Connected World

Renault Ross CISSP, CISM, CHSS
Chief Cybersecurity Business Strategist

POINTS OF DISCUSSION

48%
of incidents involved a malicious or criminal attack

25%
caused by negligent employees or contractors

27%
involve system glitches

Top 7 Security Trends

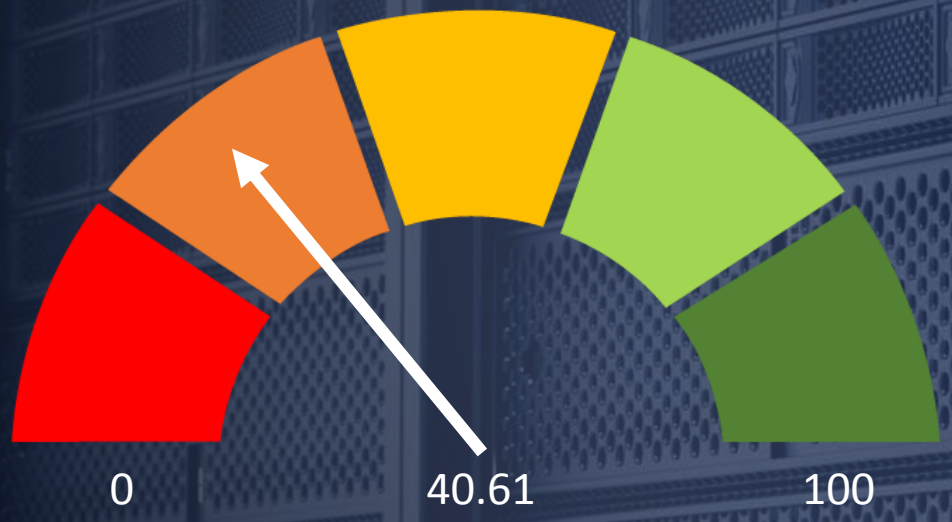
1. NIST – CYBERSECURITY FRAMEWORK
2. INFORMATION CENTRIC SECURITY
3. SECURITY ANALYTICS
4. NEXT GEN WEB SECURITY
5. UNIFIED ENPOINT – DECEPTION
6. CLOUD SECURITY
7. SIMULATED TRAINING PLATFORMS

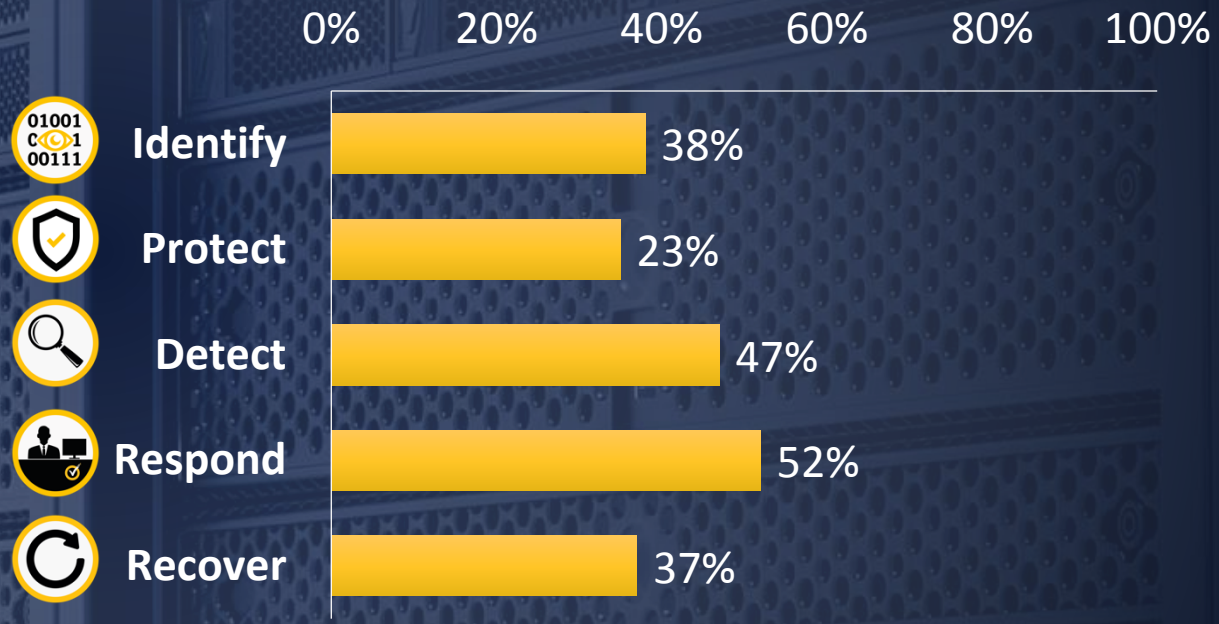
THE NIST CYBERSECURITY FRAMEWORK (NIST CSF)

Governance Drives Security Operations

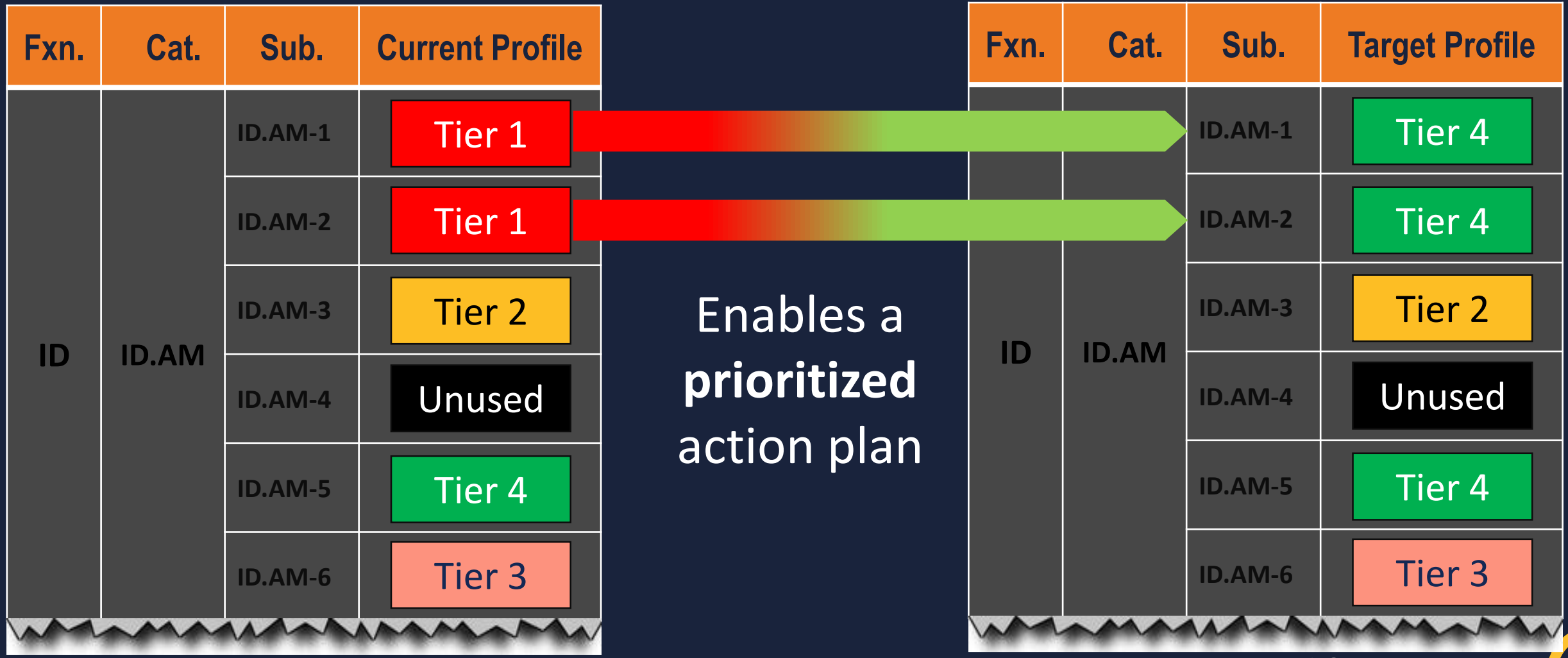
NIST CYBER SECURITY FRAMEWORK ADOPTION

GETTING EVERYONE ON THE SAME PAGE

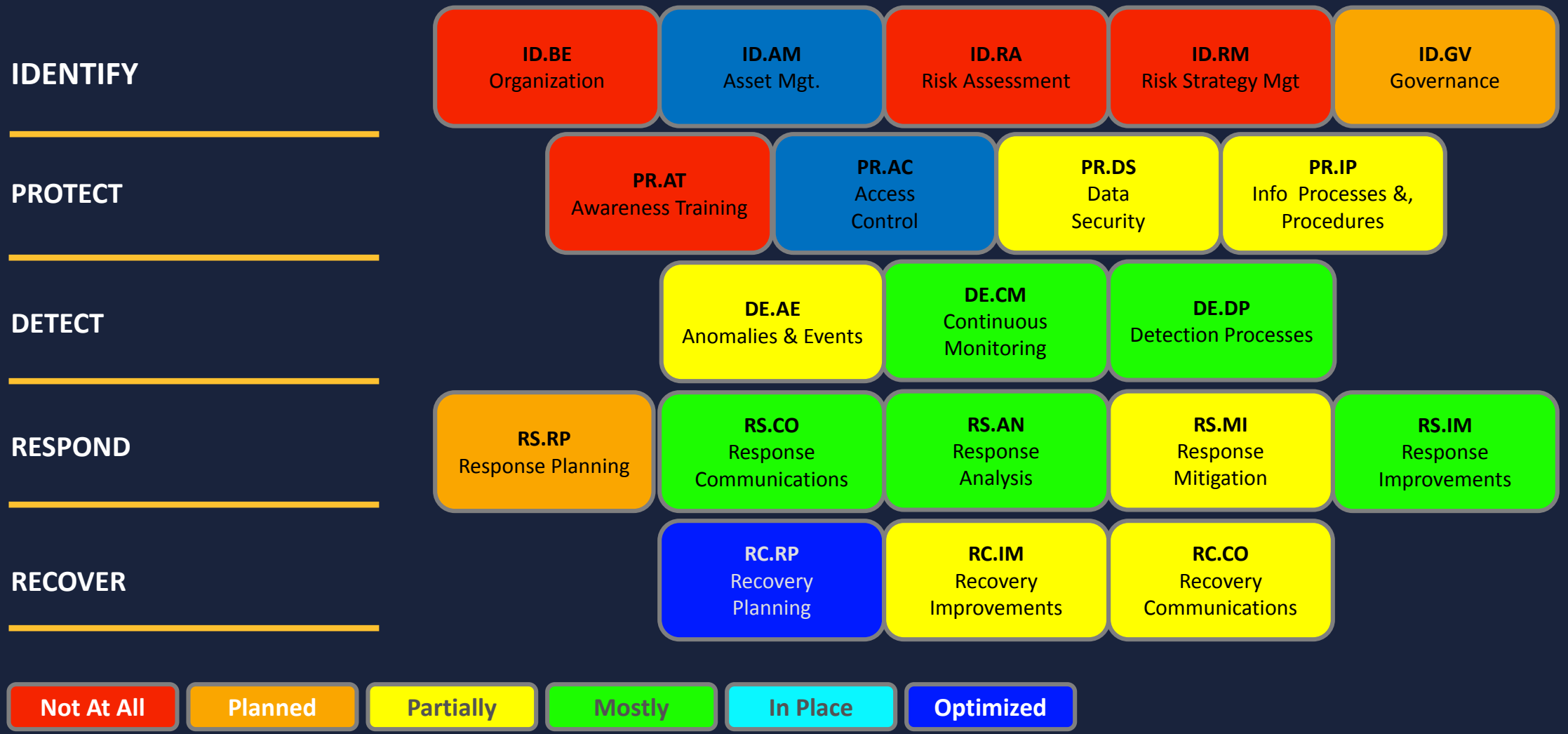




WHERE TO START



NIST – FLUSH ORGANIZATION'S GAPS



CROSS-REFERENCES TO OTHER BEST PRACTICES

Function	Category	Subcategory	Informative Resources
Identify (ID)	Asset Management (ID.AM)	Physical device inventories (ID.AM-1)	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8

SUPPORT MORE PRESCRIPTIVE STEPS FOR IMPLEMENTATION

The Center for Internet Security Critical Security Controls Version 6.0		
Family	**Control**	**Control Description**
Critical Security Control #1: Inventory of Authorized and Unauthorized Devices		
System	**1.1**	Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.
System	**1.2**	If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.
System	**1.3**	Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.
System	**1.4**	Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.
System	**1.5**	Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems.
System	**1.6**	Use client certificates to validate and authenticate systems prior to connecting to the private network.

FINALLY ALIGN SECURITY INITIATIVES WITH BUSINESS GOALS

Nebraska xxxxxx

Plan IT

5 Year Project Gantt Chart

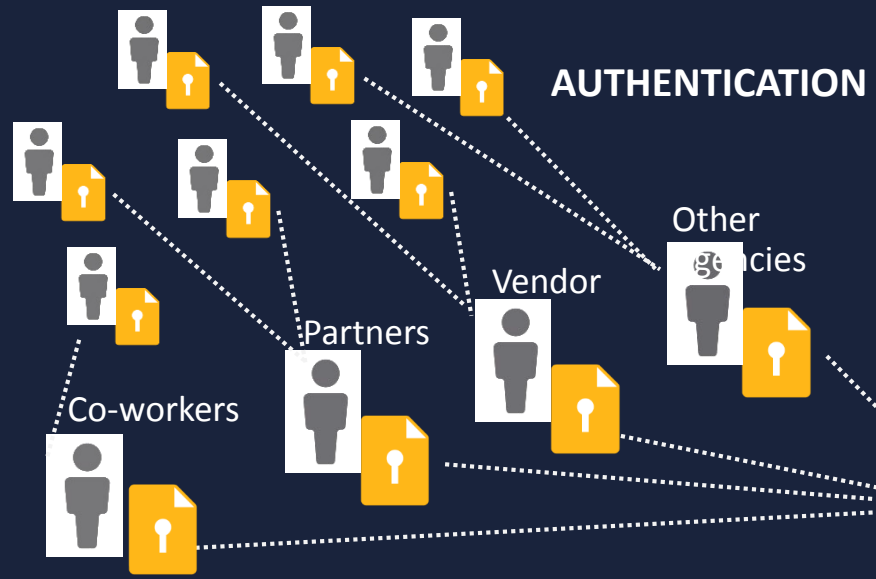
							Cyber		IR		GRC		AppSec		Messaging		CISO		IAM			
				Fiscal Year			2015 - 2016				2016 - 2017				2017 - 2018				2018 - 2019			
#	Project Request Name	Brief Description	Frequency	Impacted Teams	Project Category	Est. Duration	Q1 7/1-9/30	Q2 10/1-12/31	Q3 1/1-3/31	Q4 4/1-6/30	Q1 7/1-9/30	Q2 10/1-12/31	Q3 1/1-3/31	Q4 4/1-6/30	Q1 7/1-9/30	Q2 10/1-12/31	Q3 1/1-3/31	Q4 4/1-6/30	Q1 7/1-9/30	Q2 10/1-12/31	Q3 1/1-3/31	Q4 4/1-6/30
	Security Initiative Phase I																					
	Security Initiative Phase II																					
	Security Initiative Phase IIII																					

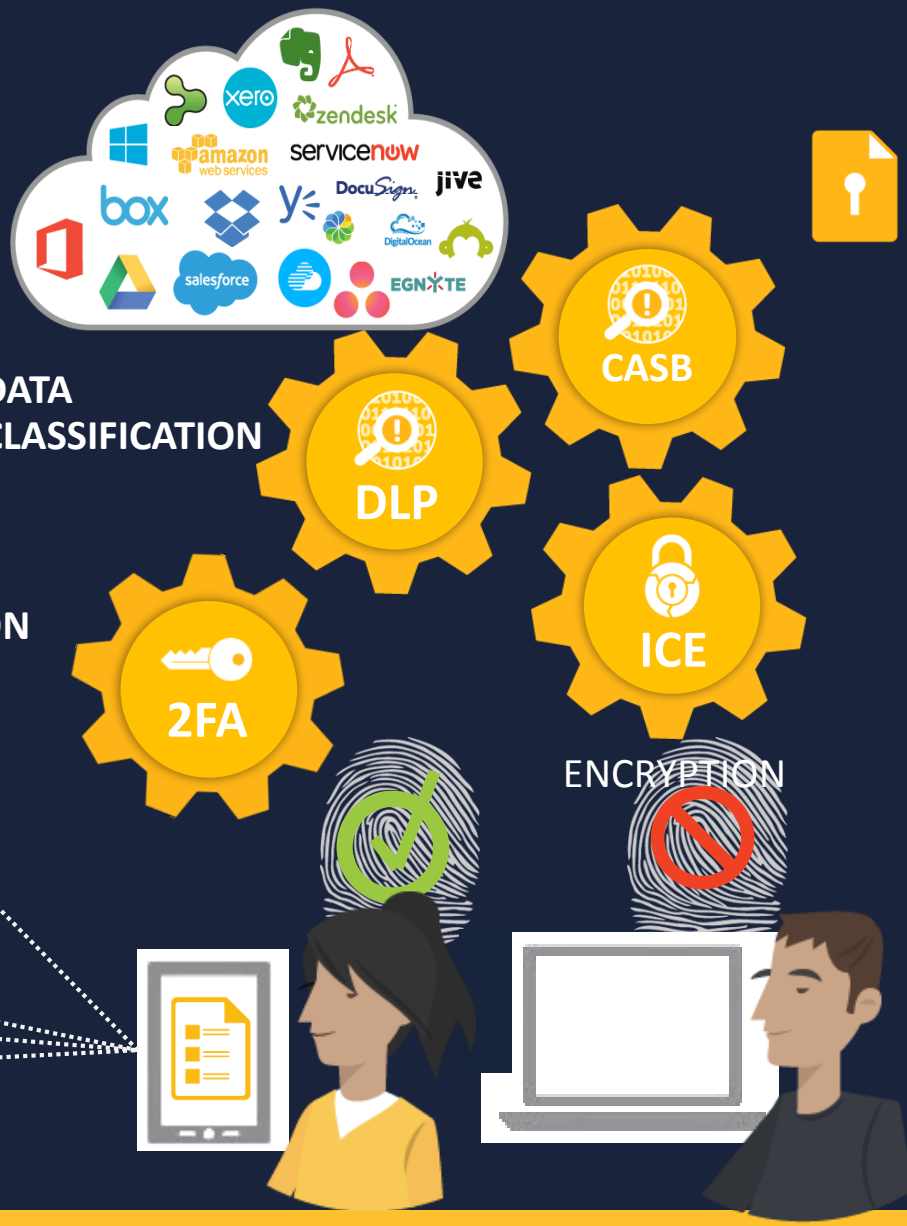
INFORMATION CENTRIC SECURITY
SECURING THE LIFE CYCLE OF INFORMATION

INFORMATION CENTRIC SECURITY

SCENARIO

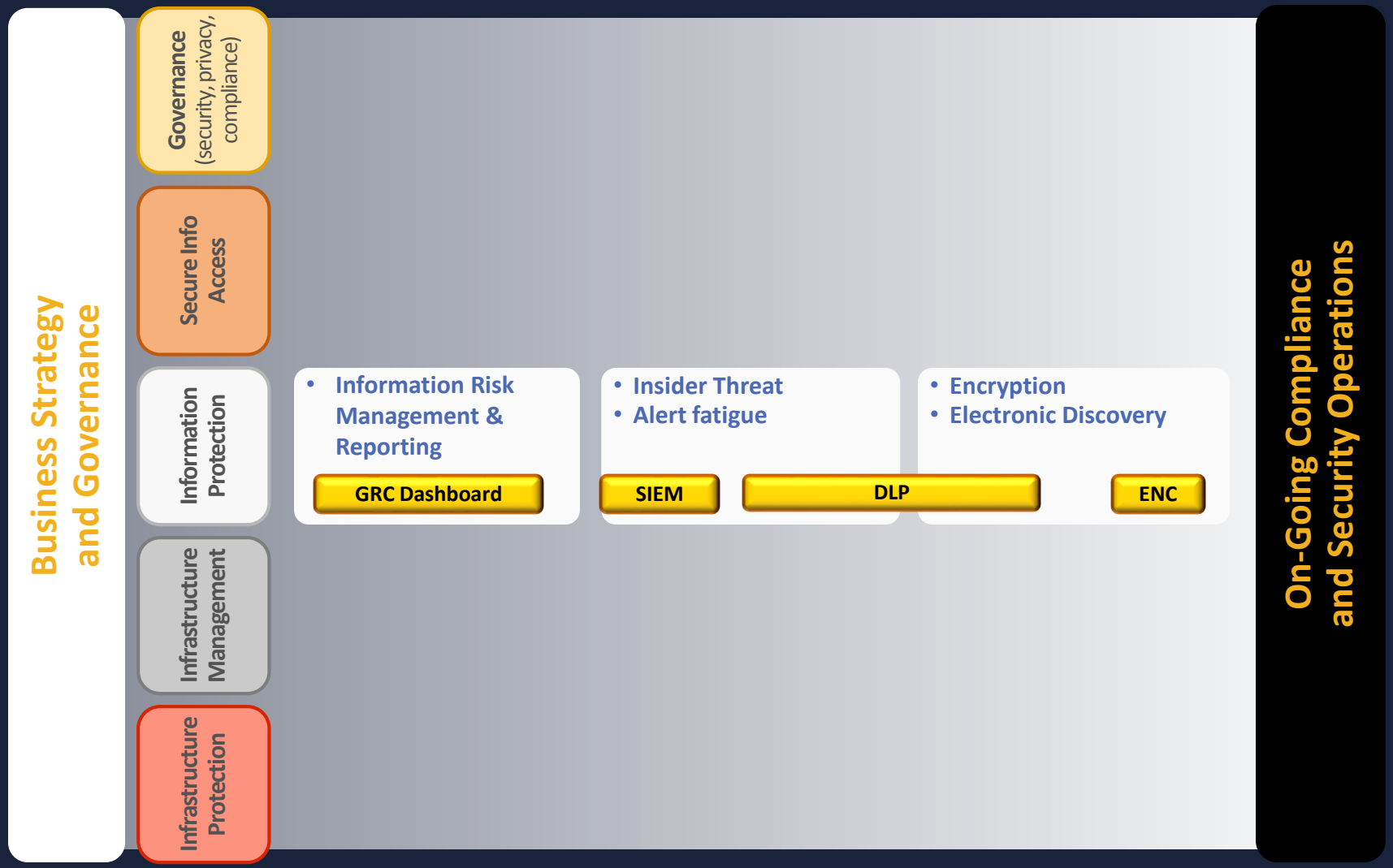
- DLP decides data to protect and drives encryption
- CASB Protect cloud apps
- Multi-Factor Authentication (MFA) for decryption
- ICE Console for centrally revocable files



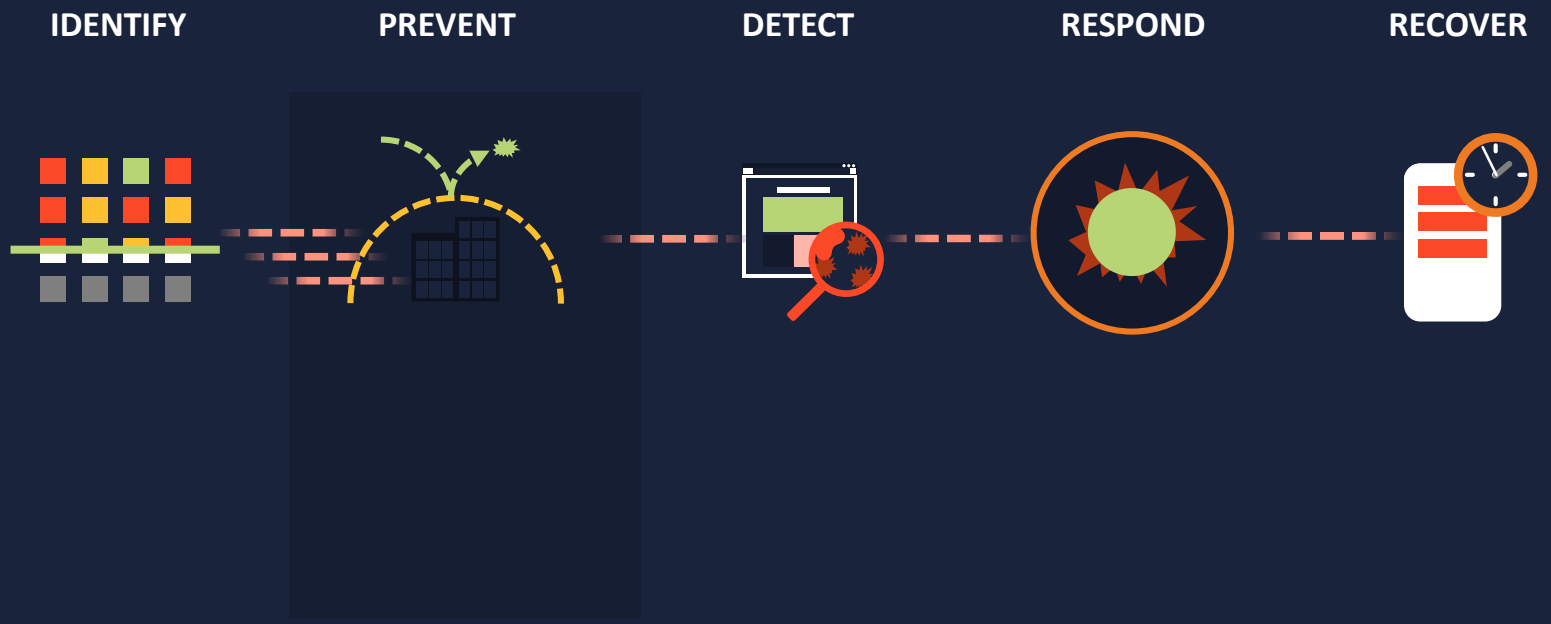


Centralized Management Console

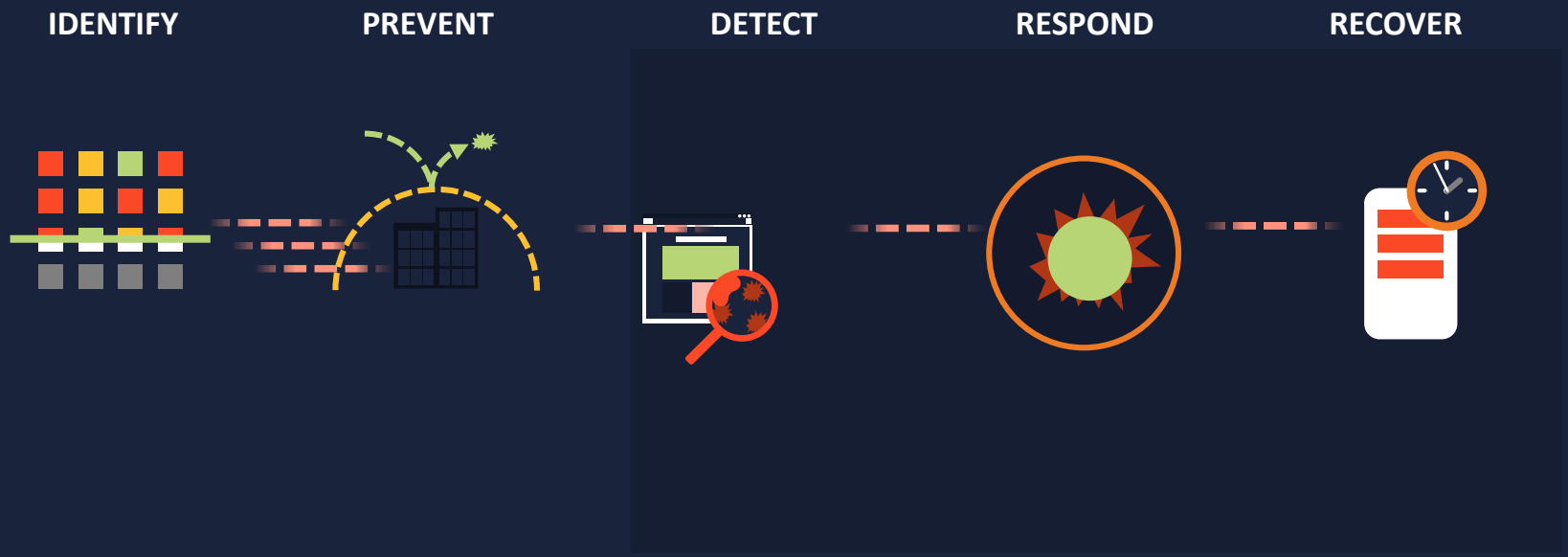
SECURITY ANALYTICS
UNDERSTANDING THE NORMS



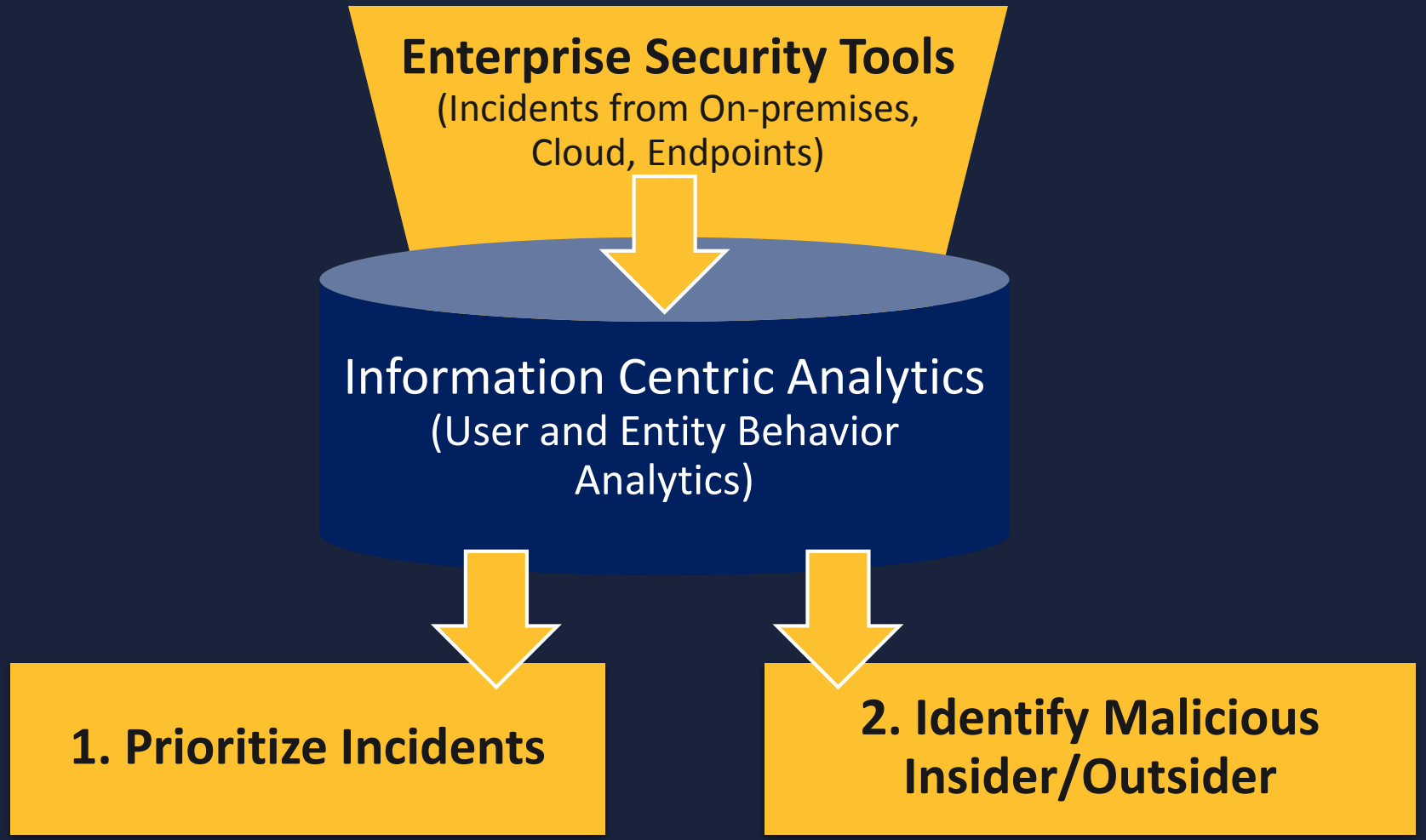
CAN YOU STOP ALL THREATS?

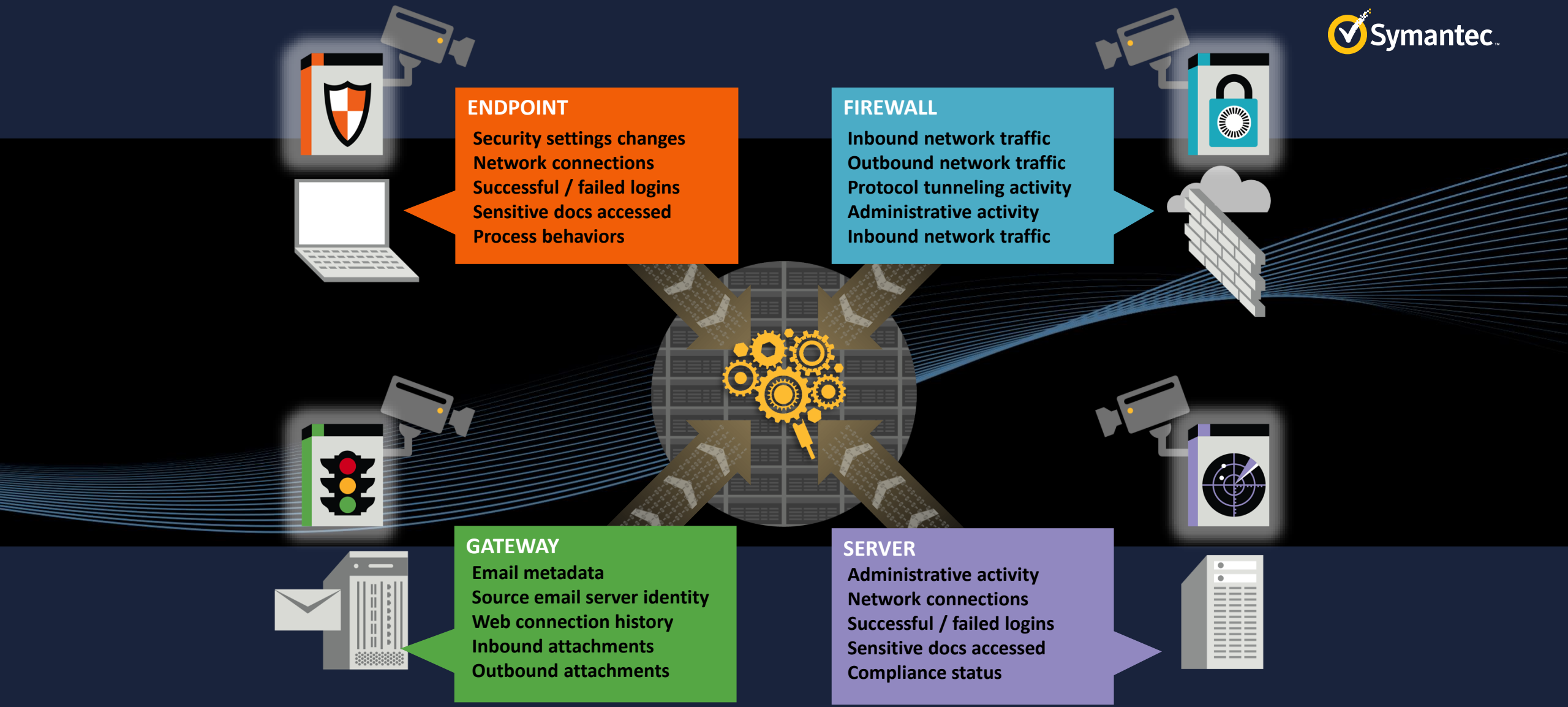


DETECTING, RESPONDING & RECOVERING IS THE KEY!



USER AND ENTITY BEHAVIOR ANALYTICS





WEB ISOLATION
AGENTLESS TECHNOLOGY

90% OF CYBER ATTACKS COME THROUGH WEB AND EMAIL

Symantec

Web Threats

1,400+
New **browser & plug-in vulnerabilities** per year

78%
of sites can be **used to deliver malware**

Every 4 seconds
an unknown **malware** is downloaded

Email & Phishing Threats

83%
Growth in **active phishing URLs**

55%
of Large Enterprise were **targeted by spear phishing**

12%
of **users click untrusted links** or attachments

Source: Verizon DBIR, Symantec ISTR, Gartner

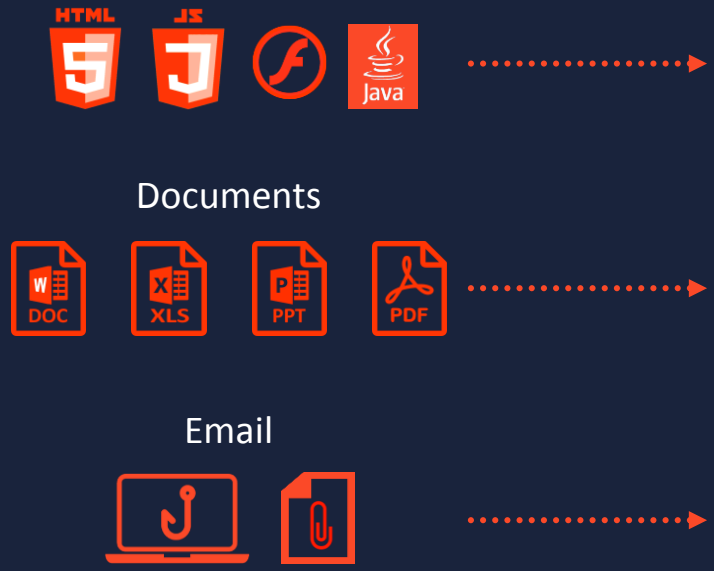
WEB ISOLATION

Risks

Web

Documents

Email



User

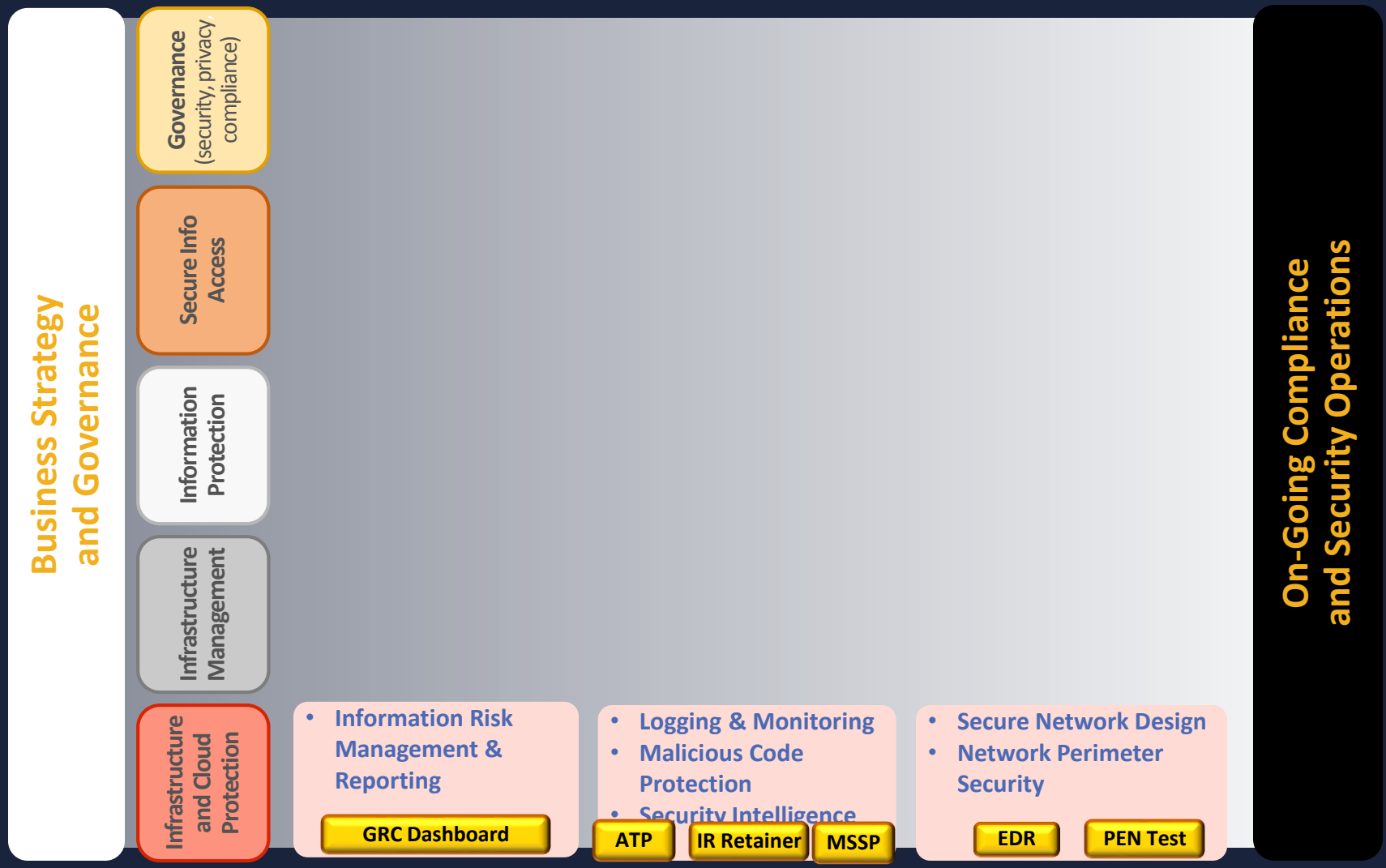
100% safe rendering information

User gestures

- Seamless browsing experience
- Isolate both web and email, including documents
- On premise, cloud and hybrid

UNIFIED SECURITY ENDPOINT WITH DECEPTION & CLOUD SECURITY

DEFENDING AGAINST UNKNOWN THREATS



UNIFIED ENDPOINT WITH DECEPTION

Symantec

Cloud Enabled

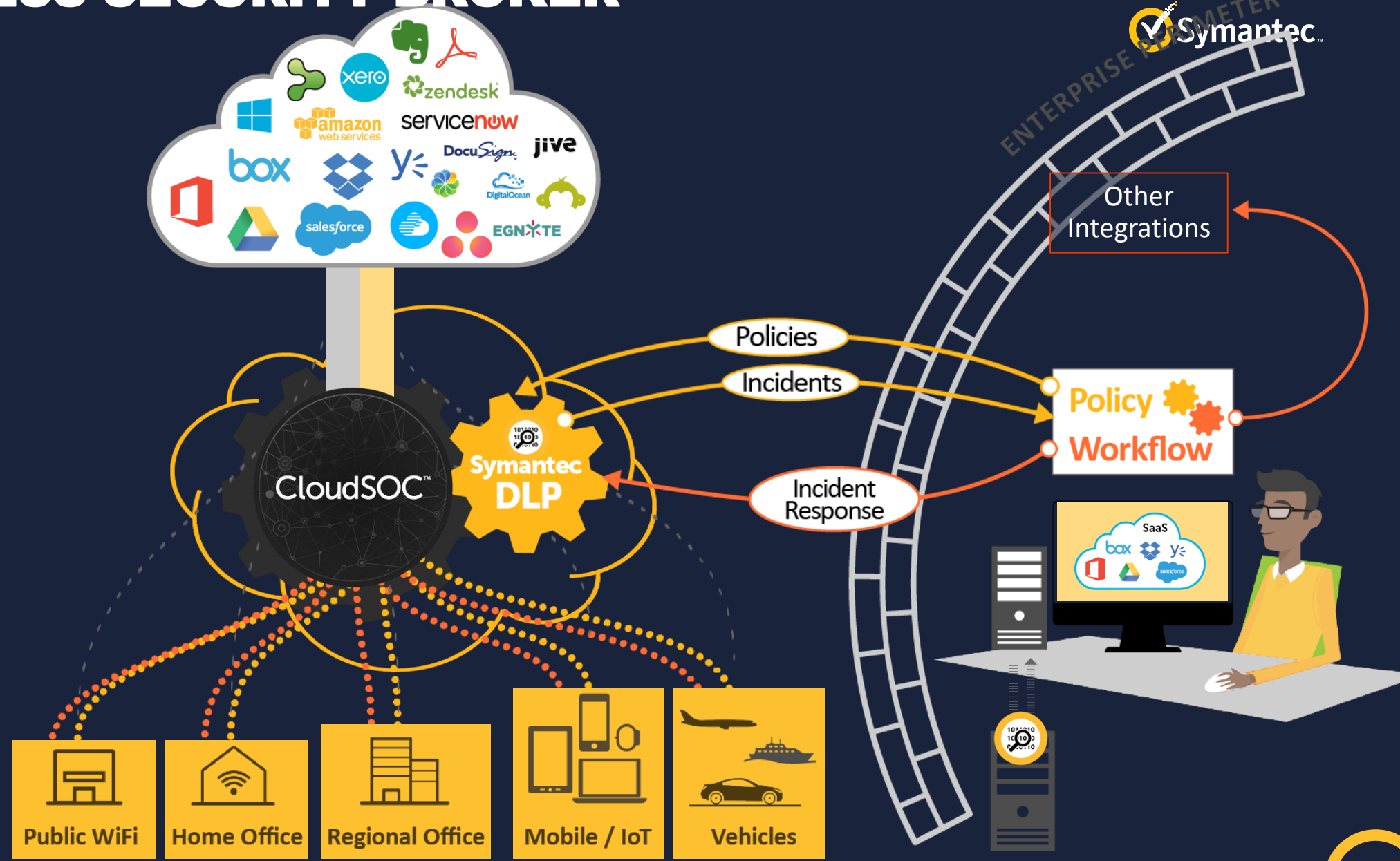
Endpoint Detection and Response

ATP: Endpoint, Email & Web

Silent Alarm

Endpoint Hardening

CLOUD ACCESS SECURITY BROKER



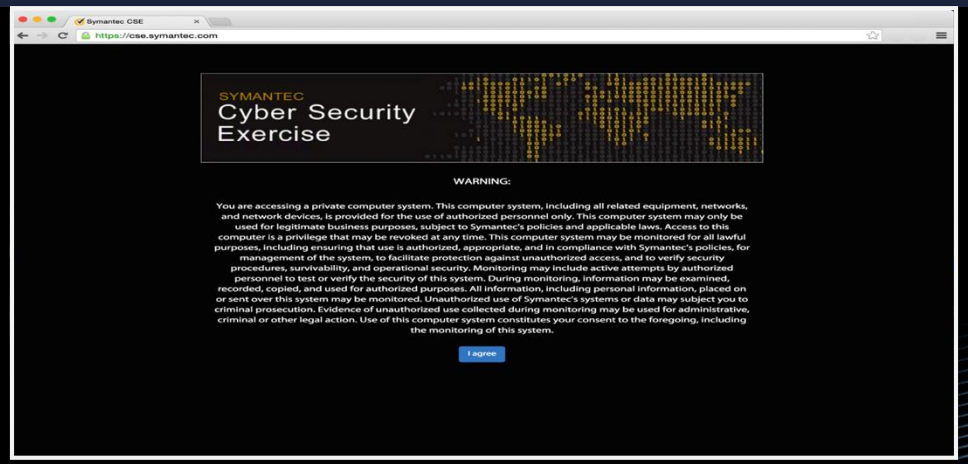
THE SKILLS GAPS

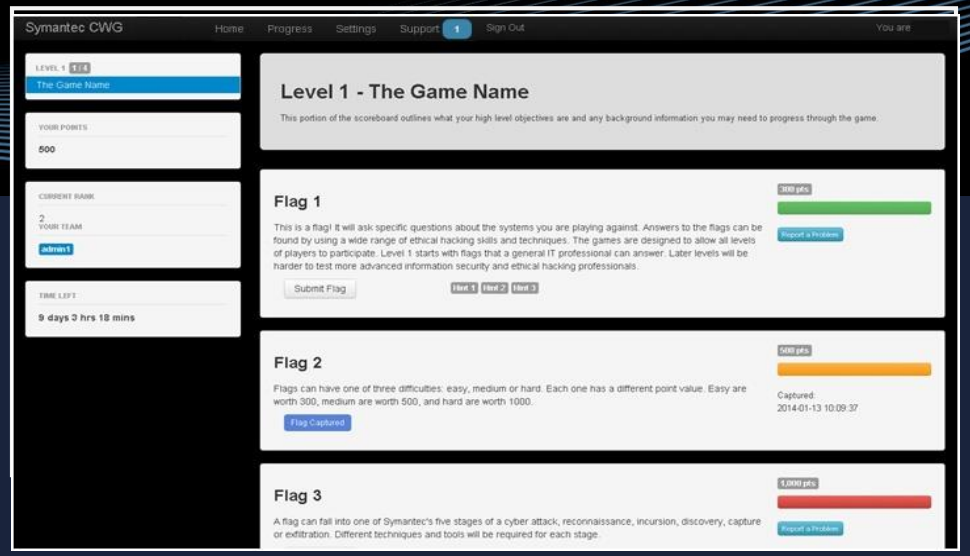
"By 2020, security industry will be shortage of millions of information security professionals, with this shortage interestingly cited by half of cyber-security staff as a key reason for data breaches (48%)."

-(ISC)²

Cyber Security Exercise

Continuous skills development for Security Teams





- Fully managed SaaS and Platform-as-a-Service offering with global coverage
- Comprehensive scoring and reporting functionality
- Over 600 hours of live system challenge scenarios, covering different industry verticals
- Over 7,000+ participants in 30+ countries
- Scenarios designed for different levels of difficulty
- Exercises can be run 1 day monthly, quarterly or yearly

SUMMARY