websense®

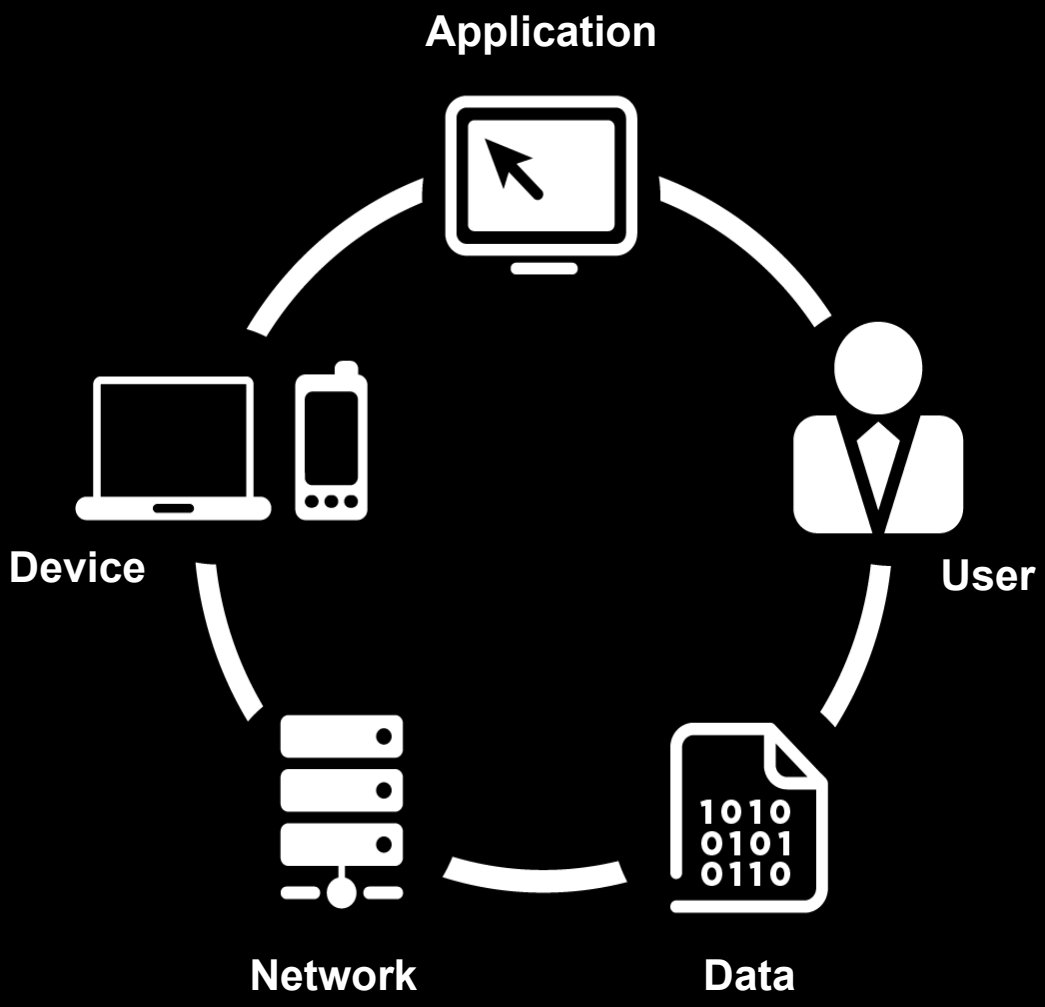
UTILIZING KILL CHAINS TO REALIZE SECURITY STRATEGY

Eric Stevens, Information Security & Strategy Officer

TRITON STOPS MORE THREATS. WE CAN PROVE IT.

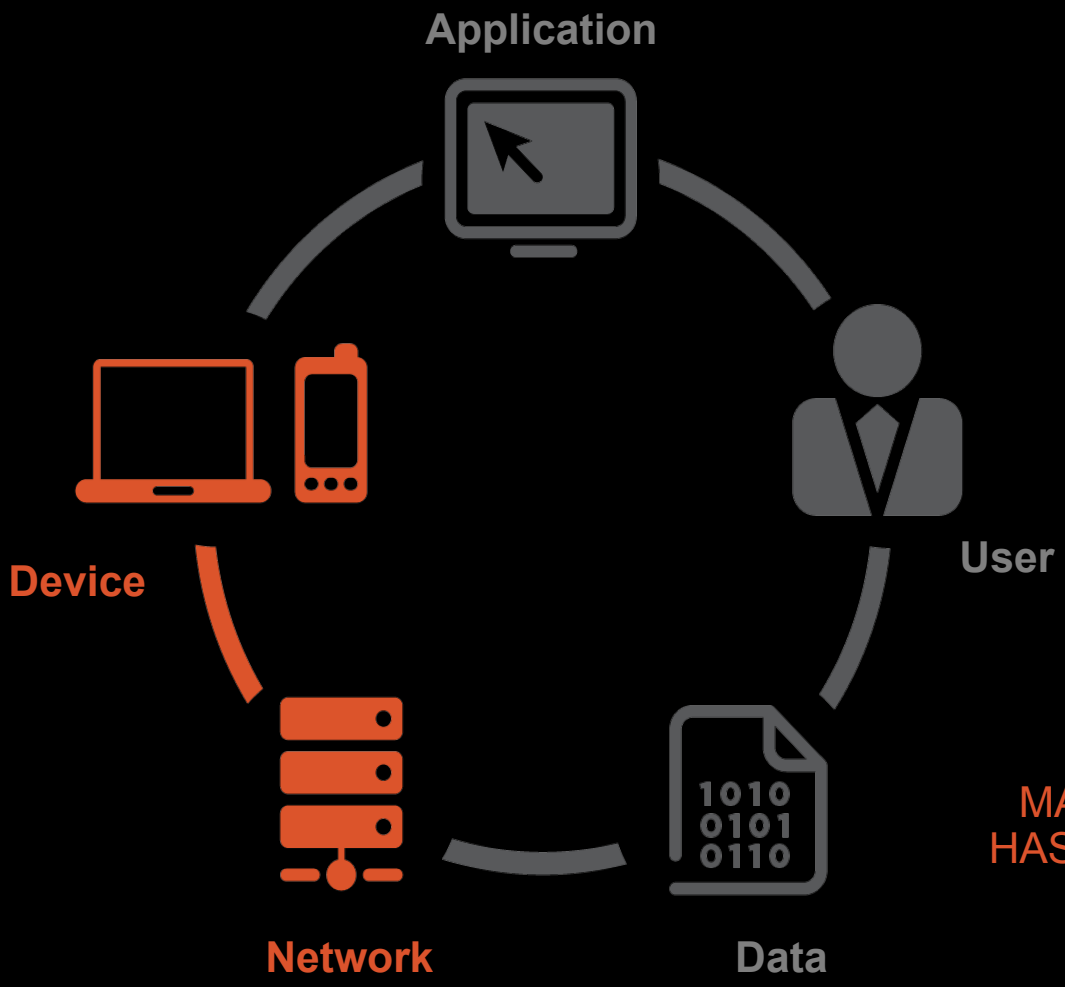
websense TRITON®

HOW WE SECURE THE PERIMETER TODAY



websense®

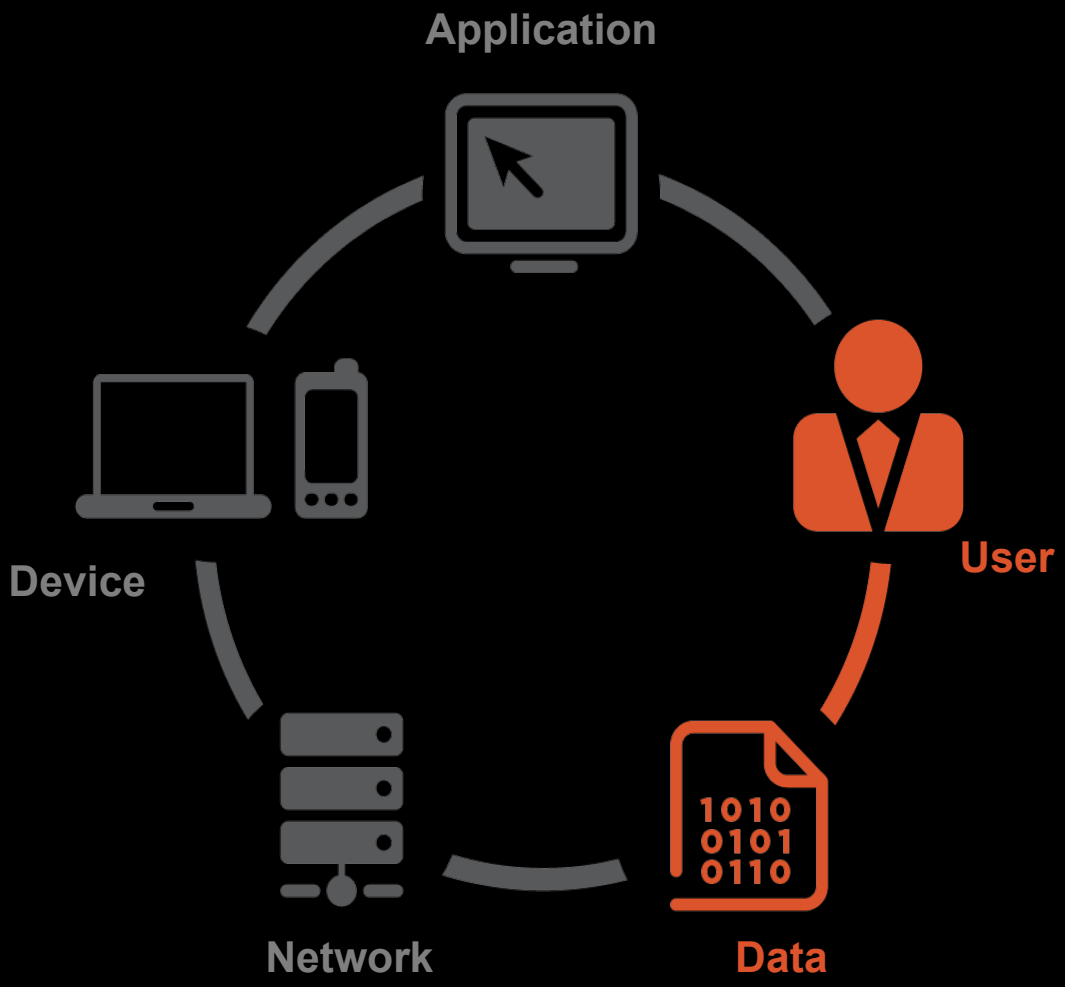
HOW WE SECURE THE PERIMETER TODAY



MAJORITY OF THE SECURITY SPEND HAS BEEN FOCUSED IN STOPPING OR DETECTION THE THREATS ON THE NETWORK OR DEVICE.

websense®

HOW WE SECURE THE PERIMETER TODAY

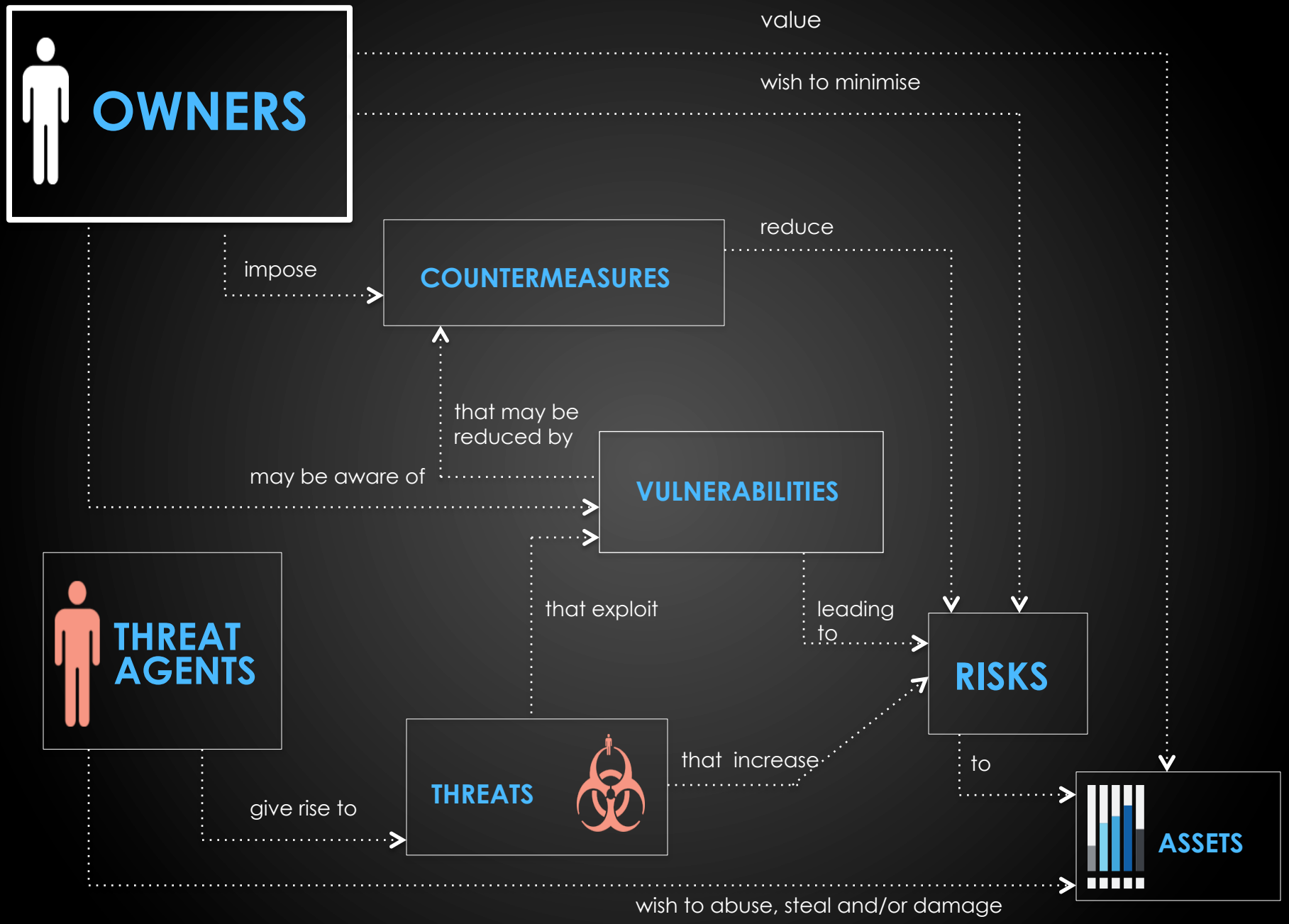


IN COMPARISON LITTLE SPEND HAS BEEN PUT TOWARDS USER ACTIVITY AND DATA PROTECTION. MOST ORGANIZATIONS ARE IMMATURE IN UNDERSTANDING USER AND DATA BEHAVIOUR.

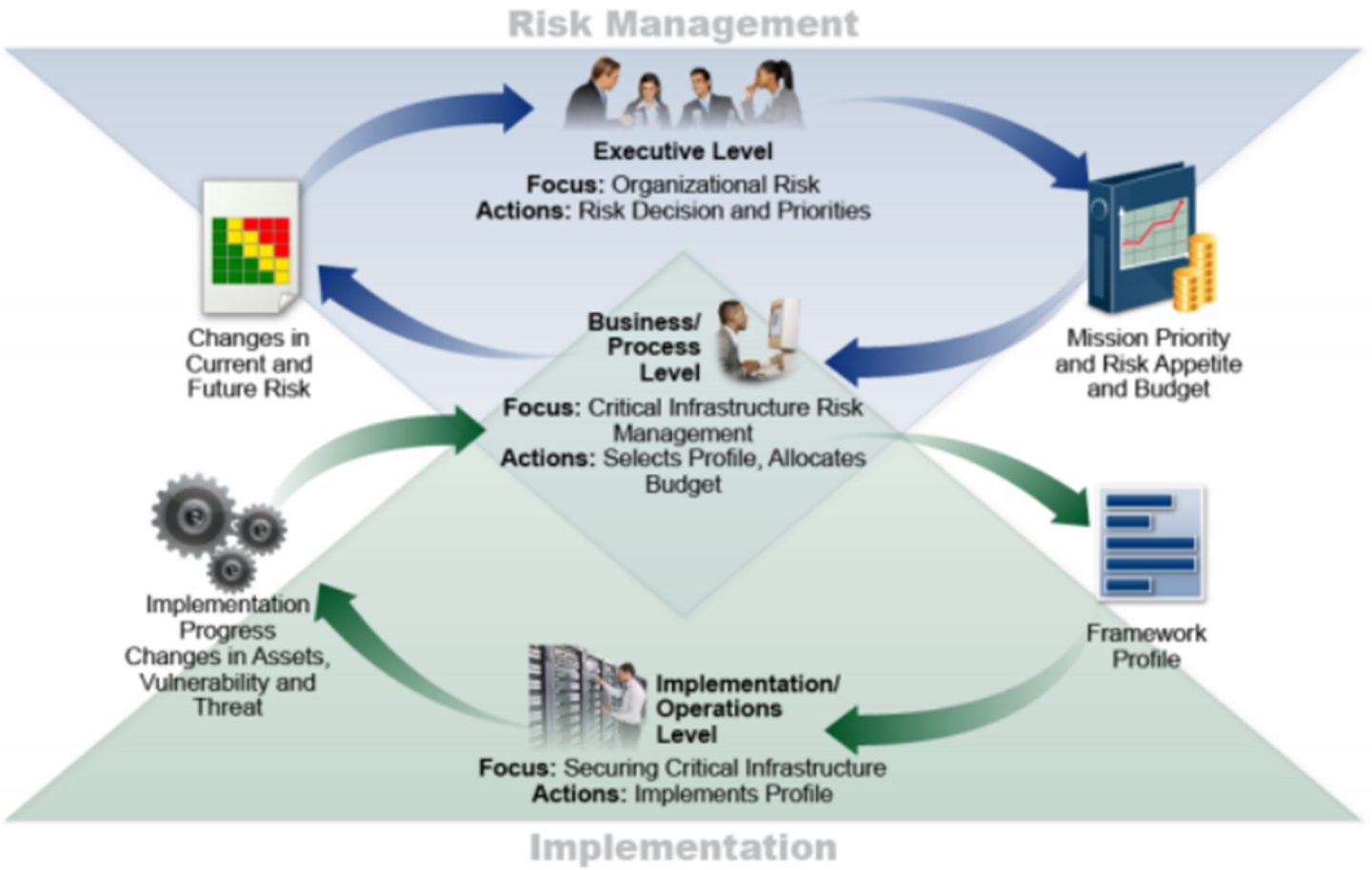
websense®

IP your IP…then DRR

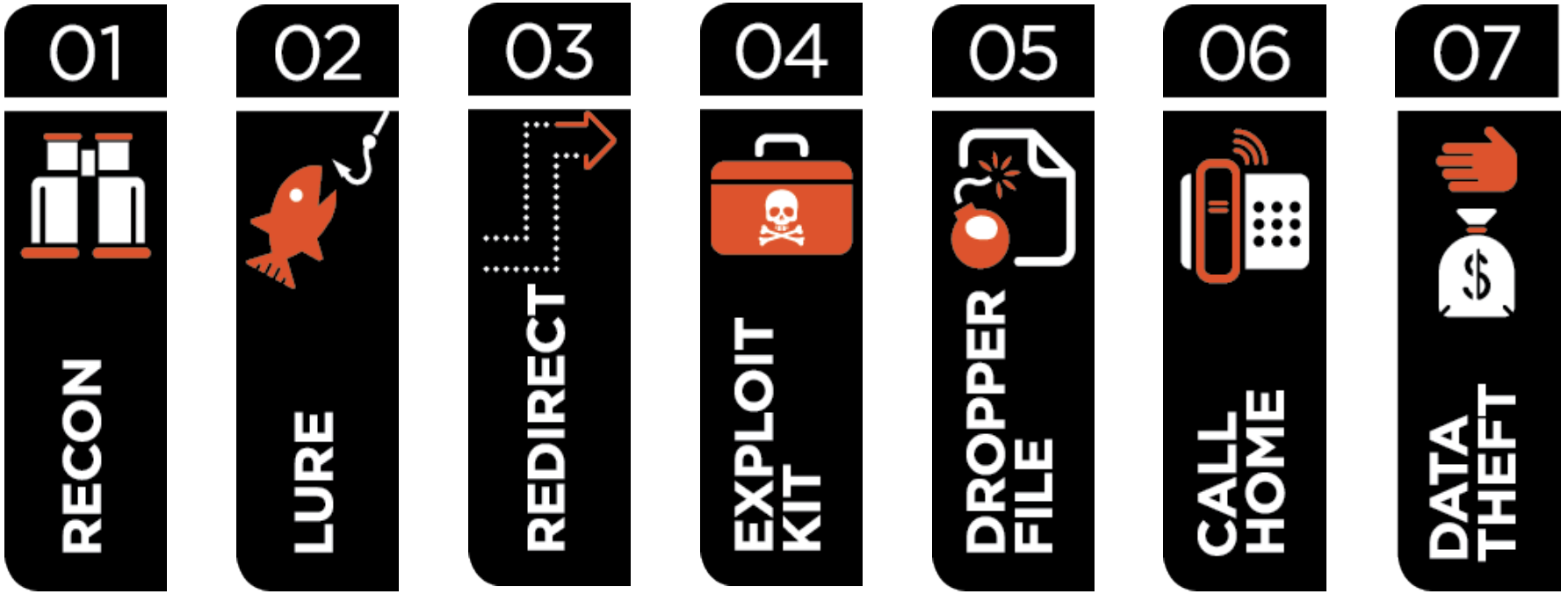
websense


OWNERS
value
wish to minimise
impose
COUNTERMEASURES
reduce
that may be reduced by
may be aware of
VULNERABILITIES
THREAT AGENTS
that exploit
leading to
RISKS
THREATS
that increase
to
give rise to
ASSETS
wish to abuse, steal and/or damage

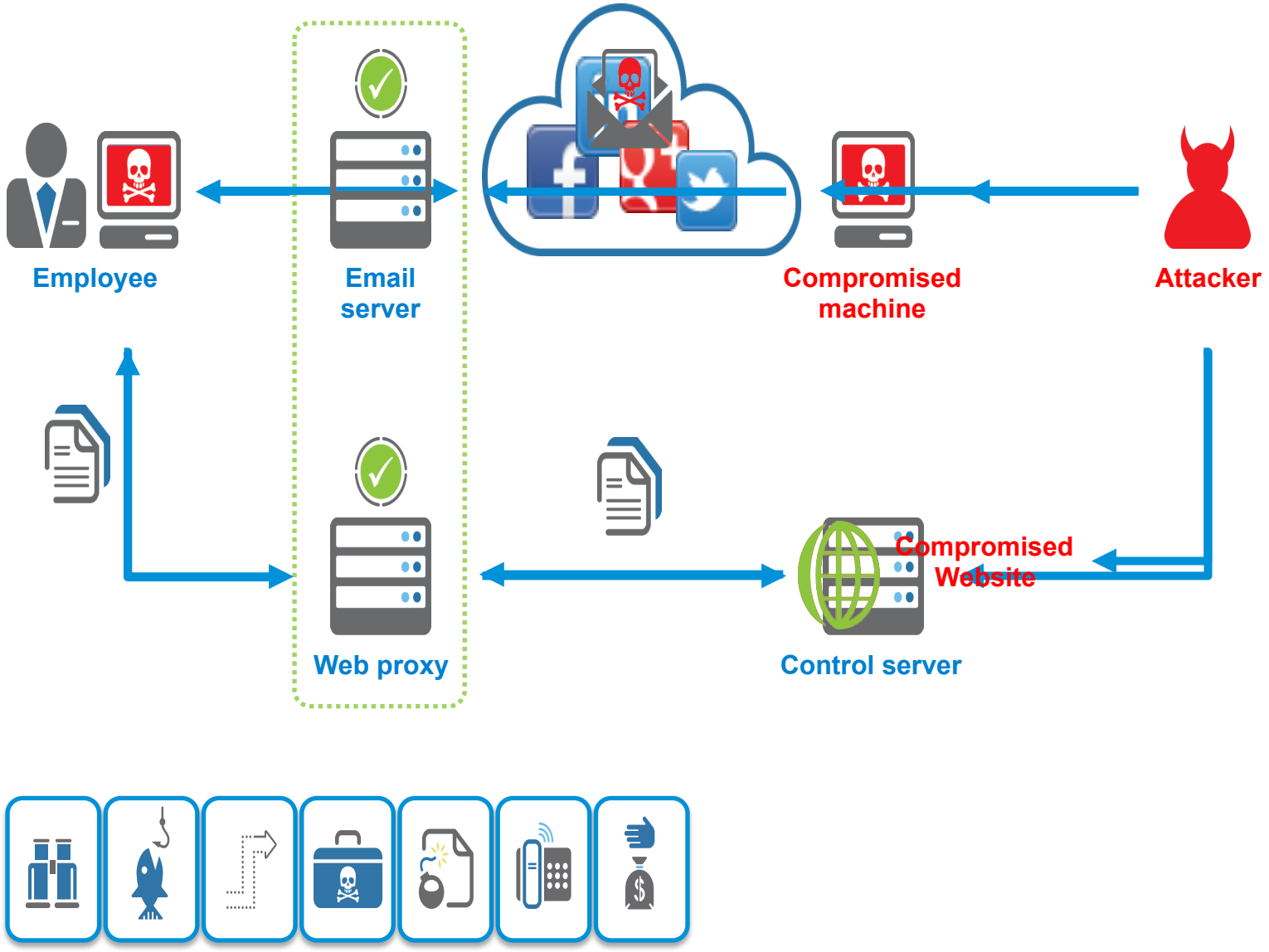
Integrated IT Risk & Security Governance ~ NIST 2014



The 7 Stages of Advanced Threats

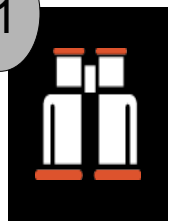
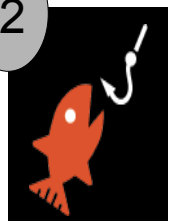
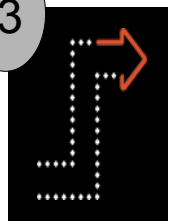
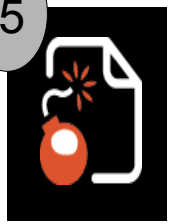
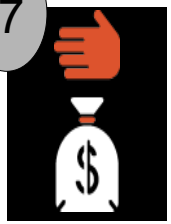


7-Stage Kill Chain



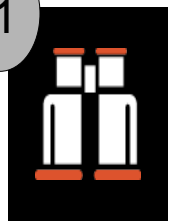
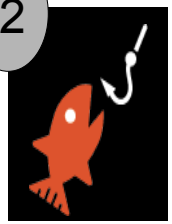
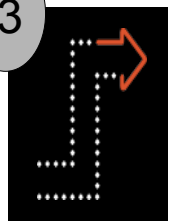
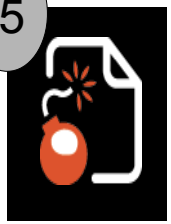
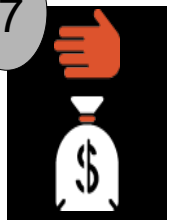
Not All Attacks Use All 7 Stages (Slide 1 of 2)

websense

	1 	2 	3 	4 	5 	6 	7 
Watering Hole Attack		Legitimate looking website draws interest		Scan for Vulnerabilities	Download Malware File	Establish connection for complete download	Steal Data
Spear Phish Attack	Attacker must do research to customize a Lure	Customized email with URL (aimed at trusted entry)	May use Re-Direct	May use Exploit Kit	Definitely uses Dropper File	May use call home	Definitely after data theft
Credit/ Debit Card Scam	Recon to design email or web lure	Send fake survey, with request for bank info to get paid.					Theft of banking data through survey

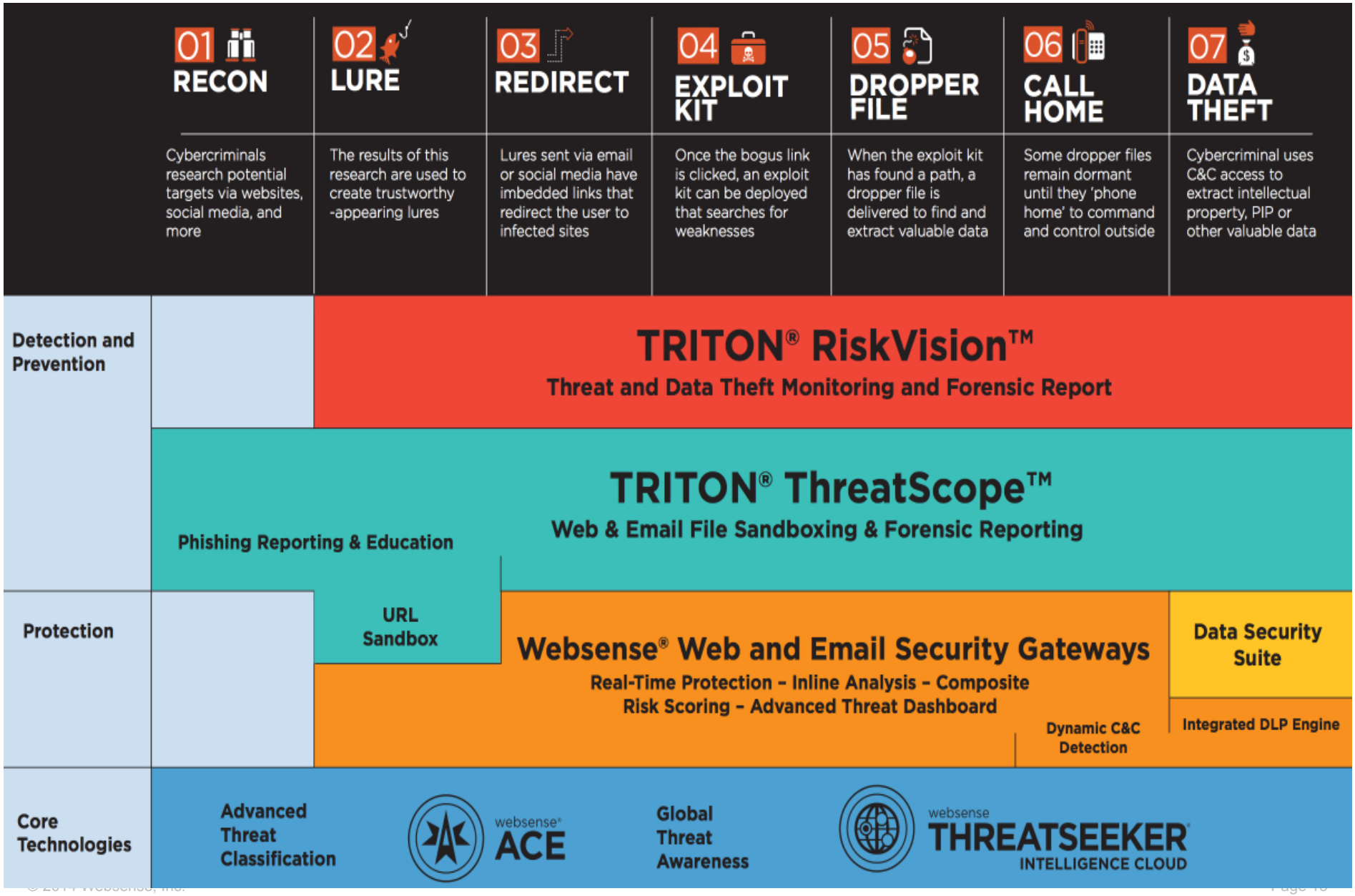
Not All Attacks Use All 7 Stages (Slide 2 of 2)

websense

	1 	2 	3 	4 	5 	6 	7 
News alert / Cool Video / Must-See pic	Very little recon to design lure. Targets general curiosity of people. Recon to design	"Watch this never-before-seen picture/ video!" Lure	Re-direct to infected YouTube site or fake mirror site.	Scan for vulnerabilities	Dropper File with malicious payload (PDF, Adobe Download, Fake Video download, etc)	Call home to ask for further instructions	Data theft of sensitive information
Hidden Video Lure (2012)	Targets Facebook users with certain profiles	Develops private message with URL	Redirects to malware site		"Missing Adobe Flash Player" message triggers download		Malware file searches and transmits sensitive data
Search Engine Poisoning	Recon to design fake web site to rank high in SEO results	Search Engine results entice people to click.		Halloween Costume Designs, Christmas gift ideas, etc	Fake downloads of images or sales coupons	Call home for further instructions	Theft of sensitive data

Layered Security Defense in Depth Model

websense



Behavioral Sandboxing

Real-Time Security Classification

Anti-Spam / Spear-Phishing

Real-Time Content Classification

websense® ACE

Reputation Analysis

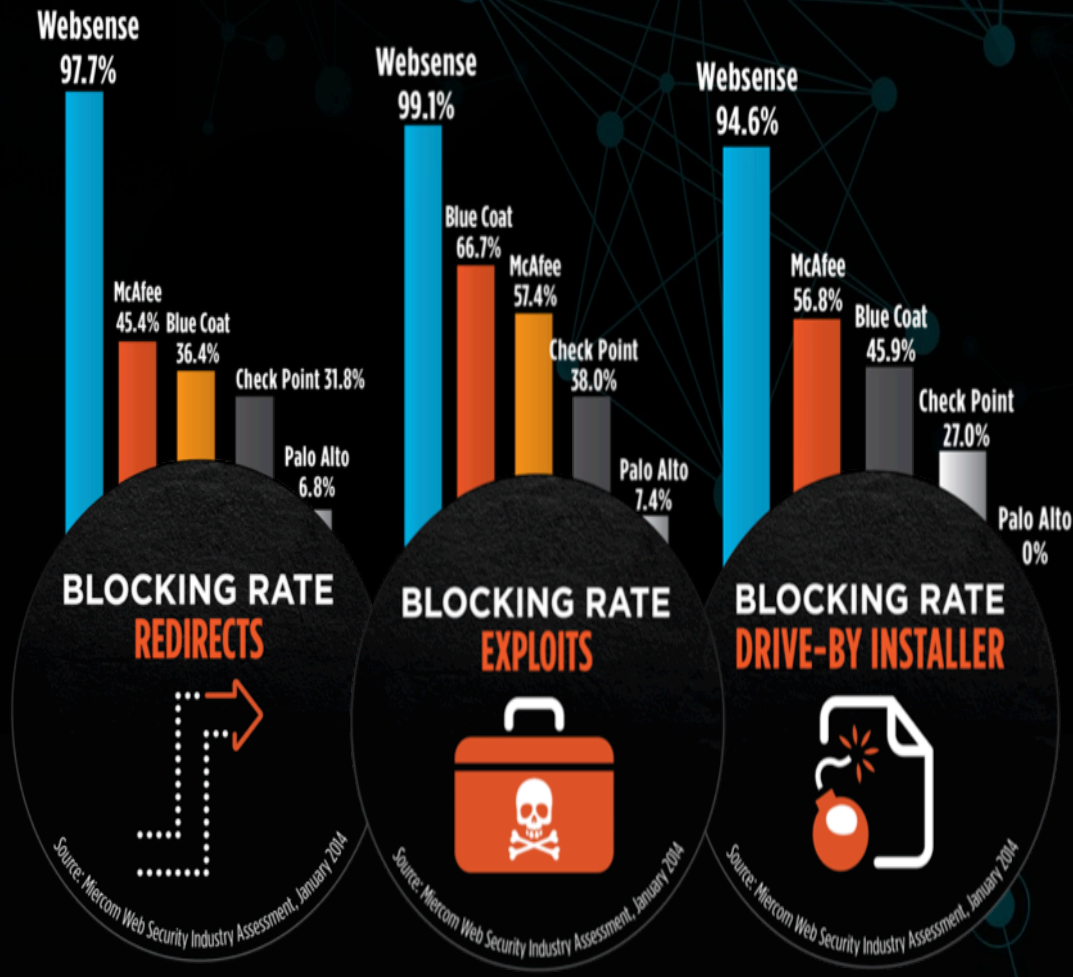
Real-Time Data Classification

URL Classification

Anti-Malware Engines

THE INDUSTRY IS TAKING NOTICE - EVIDENCE OF OUR SECURITY CAPABILITIES

- 2014 Best Advanced Persistent Threat (APT) Protection
- 2014 Best Web Content Management Solution
- 2014 Best DLP Solution-EMEA




websense
THANK YOU
TRITON STOPS MORE THREATS. WE CAN PROVE IT.
websense
TRITON