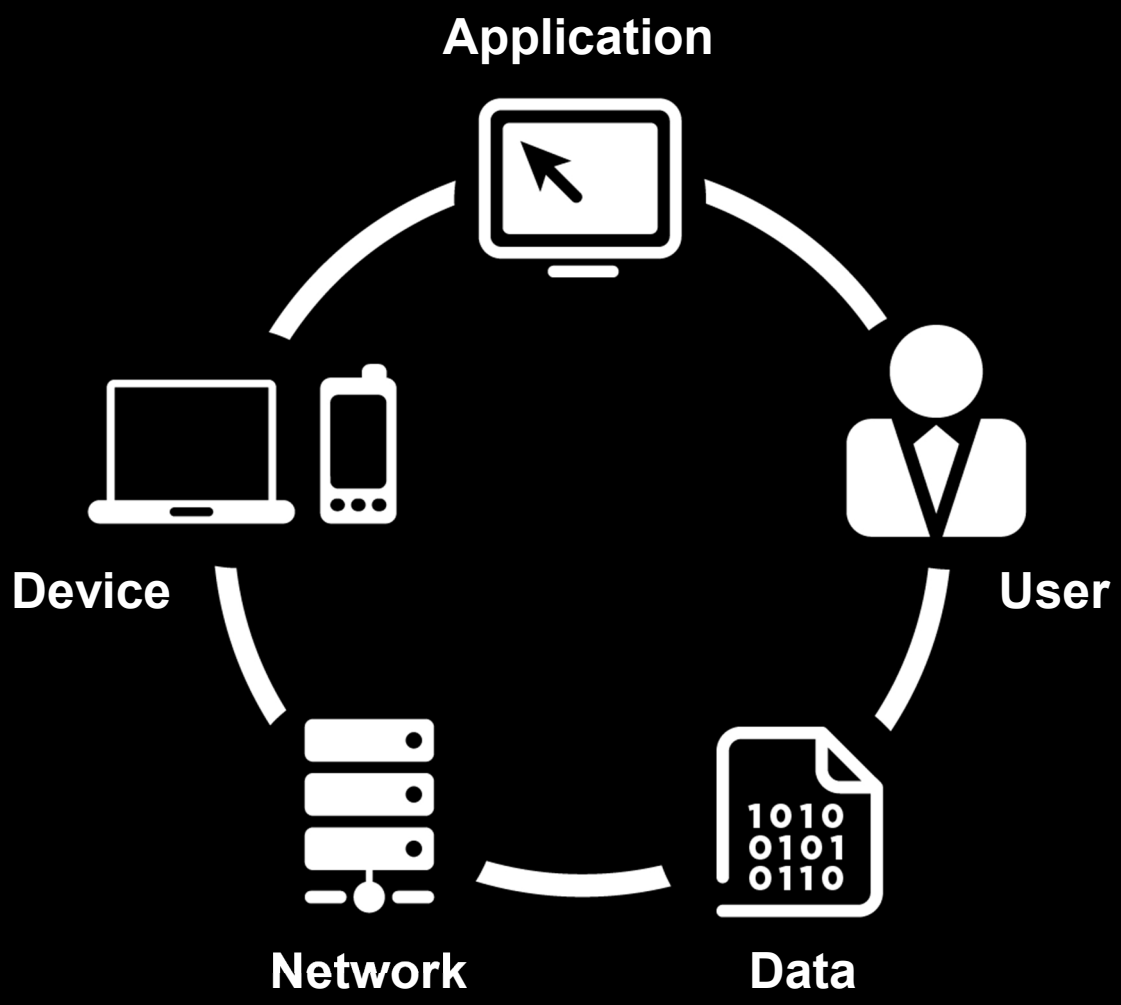
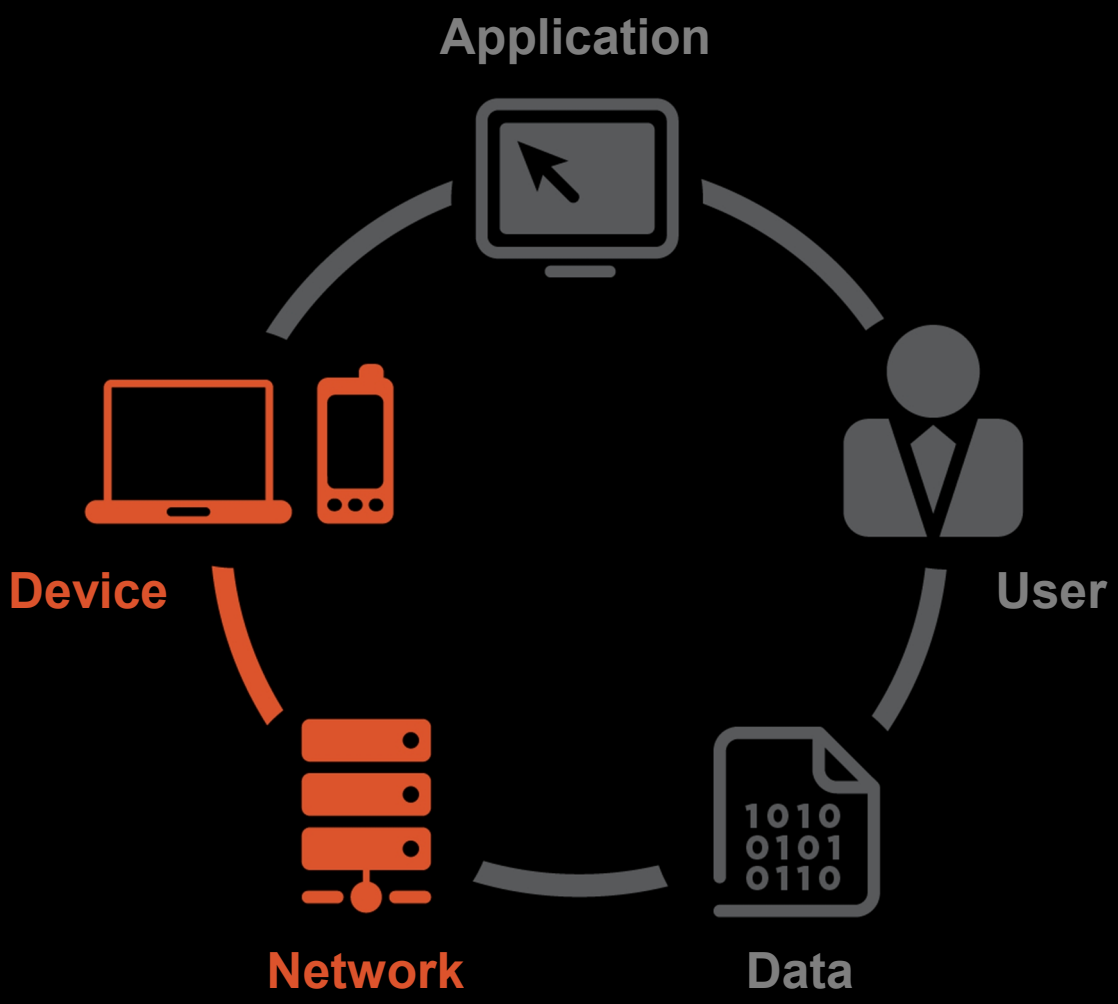

websense
DEFENDING YOUR BUSINESS FROM
NEXT-GEN CYBERSECURITY THREATS
Ben Tan, Regional Sales Manager
TRITON STOPS MORE THREATS. WE CAN PROVE IT.
websense
TRITON



HOW WE SECURE THE PERIMETER TODAY

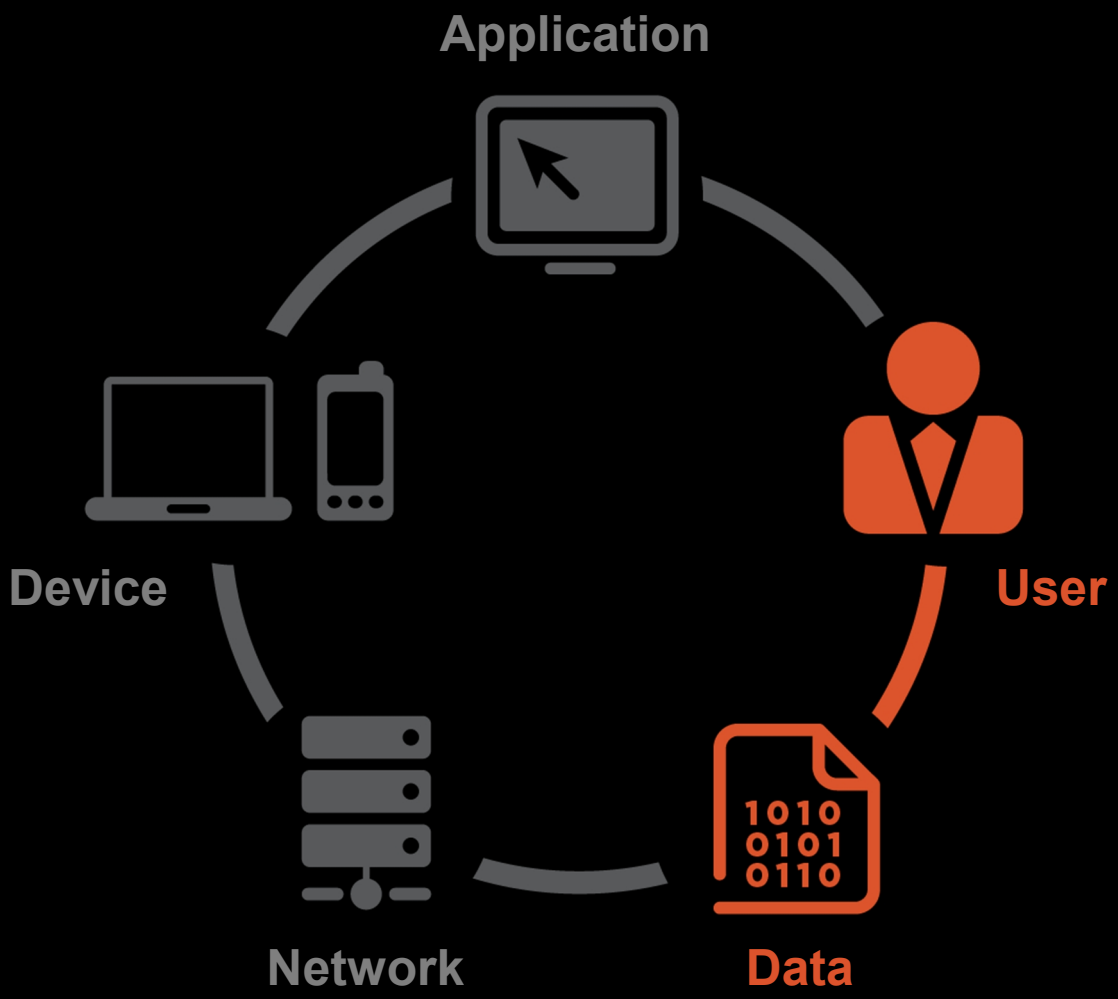
websense®



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.

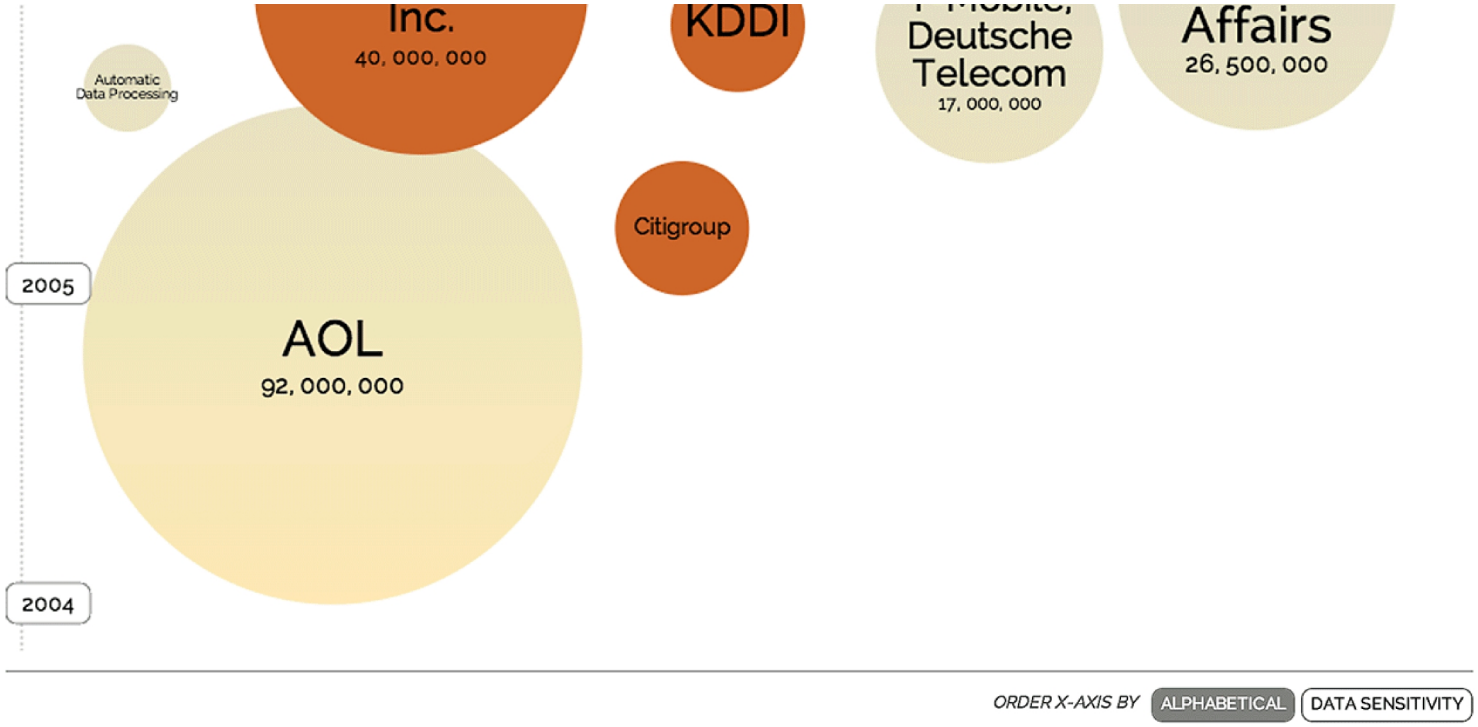
websense®



HOW WE SECURE THE PERIMETER TODAY

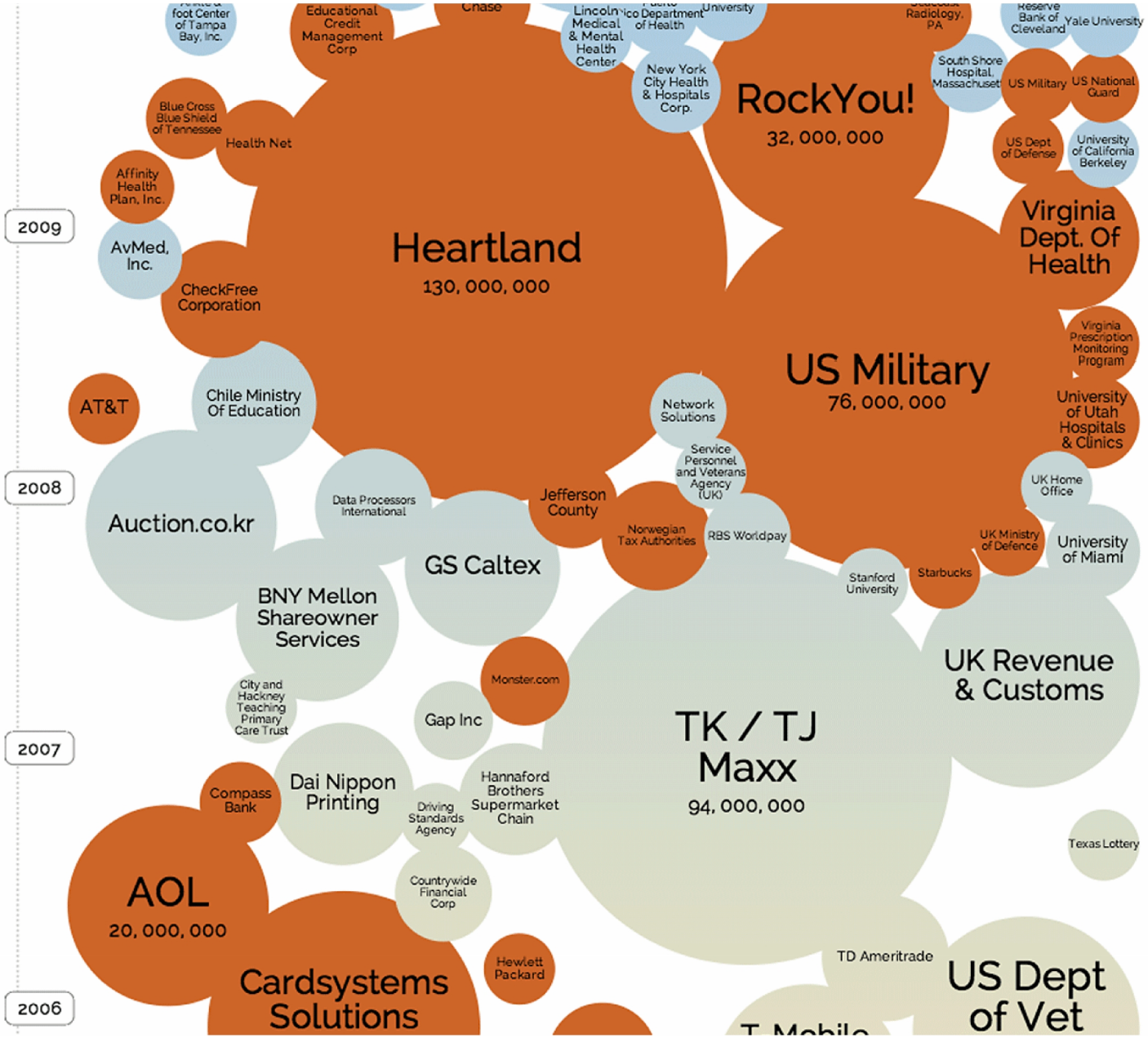
IN COMPARISON LITTLE SPEND HAS BEEN PUT TOWARDS USER ACTIVITY AND DATA PROTECTION. MOST ORGANIZATIONS ARE IMMATURE IN UNDERSTANDING USER AND DATA BEHAVIOR.

websense®



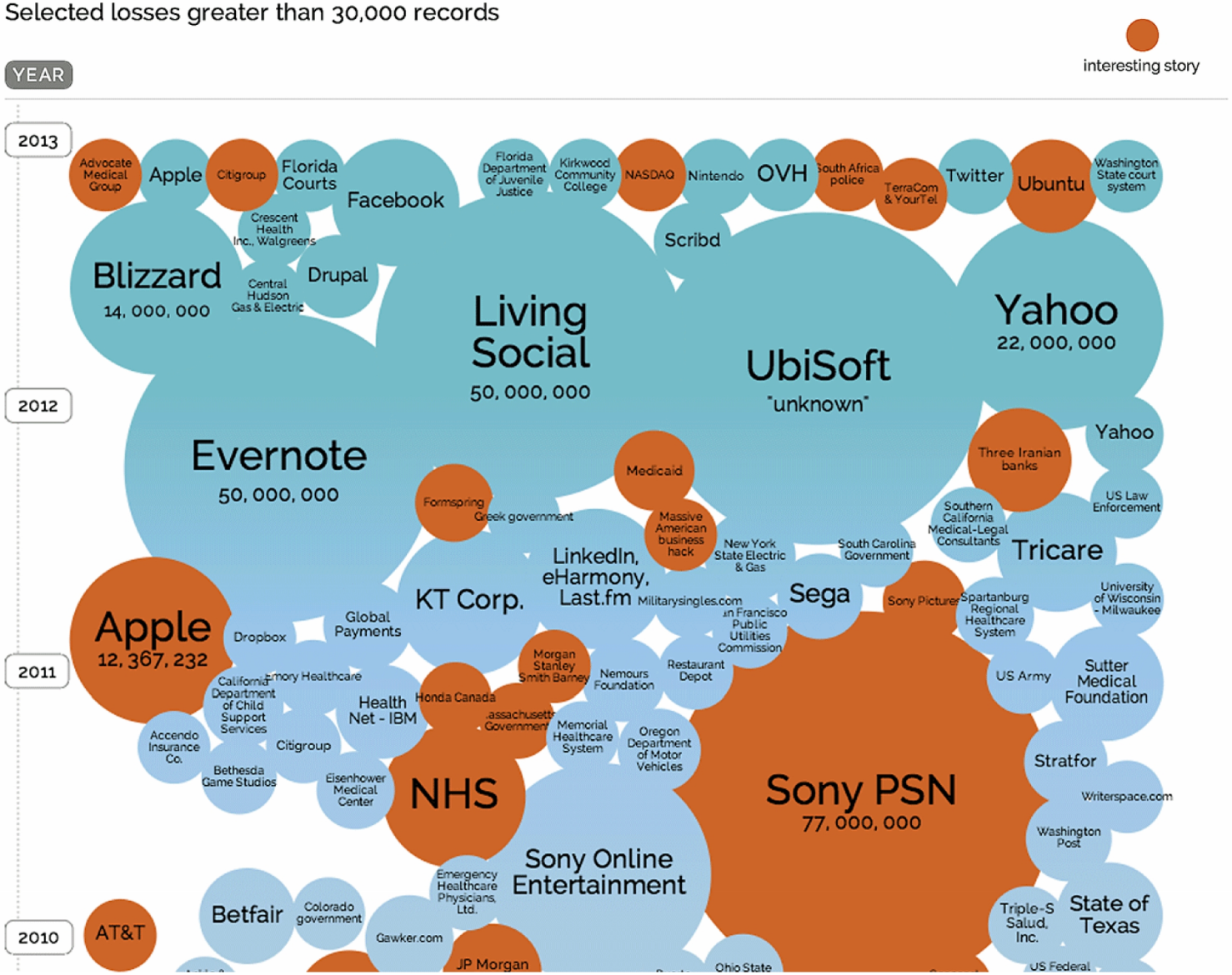
CONSIDER THE WORLD'S LARGEST DATA BREACHES

websense®


2009
2008
2007
2006
Heartland
130, 000, 000
RockYou!
32, 000, 000
US Military
76, 000, 000
TK / TJ Maxx
94, 000, 000
AOL
20, 000, 000
Cardsystems Solutions
Auction.co.kr
GS Caltex
BNY Mellon Shareowner Services
Dai Nippon Printing
UK Revenue & Customs
Virginia Dept. Of Health
US Dept of Vet
Chase
Educational Credit Management Corp
Lincoln Medical & Mental Health Center
New York City Health & Hospitals Corp.
Blue Cross Blue Shield of Tennessee
Health Net
Affinity Health Plan, Inc.
AvMed, Inc.
CheckFree Corporation
AT&T
Chile Ministry Of Education
Data Processors International
Jefferson County
Network Solutions
Service Personnel and Veterans Agency (UK)
Norwegian Tax Authorities
RBS Worldpay
Stanford University
Starbucks
UK Home Office
UK Ministry of Defence
University of Miami
University of Utah Hospitals & Clinics
Virginia Prescription Monitoring Program
US Military
US National Guard
US Dept of Defense
University of California Berkeley
South Shore Hospital, Massachusets
Yale University
Reserve Bank of Cleveland
Monster.com
Gap Inc
City and Hackney Teaching Primary Care Trust
Compass Bank
Driving Standards Agency
Hannaford Brothers Supermarket Chain
Countrywide Financial Corp
Hewlett Packard
TD Ameritrade
Texas Lottery

World's Biggest Data Breaches

Selected losses greater than 30,000 records

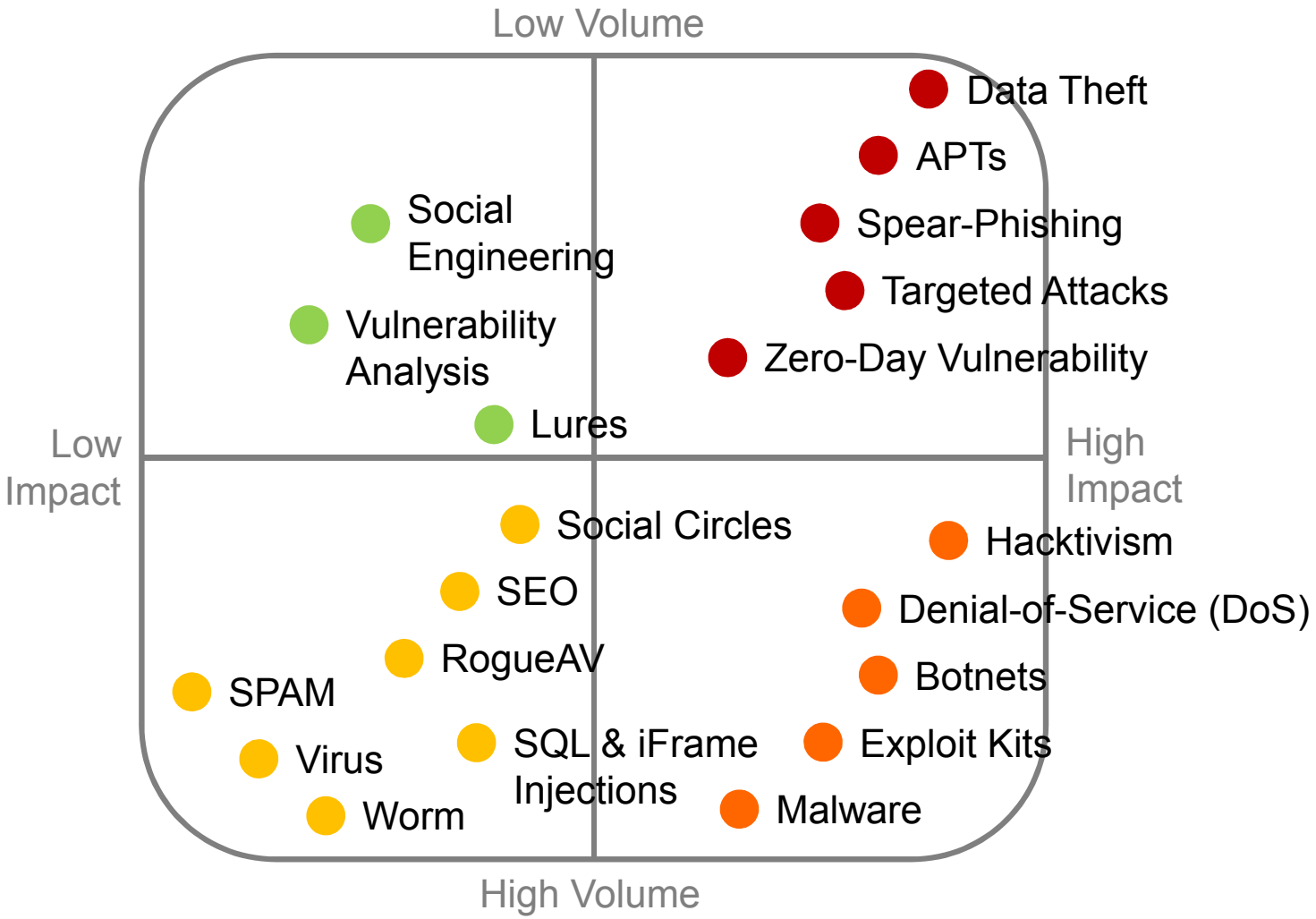


Shift in Attack Methods

websense

PAST
High volume
Short lifespan
Visible/news
Infection/deface
Limelight

PRESENT
Low volume
Persistent
Targeted/focus
Data theft
Profit



The Need to Know What You Don't Know

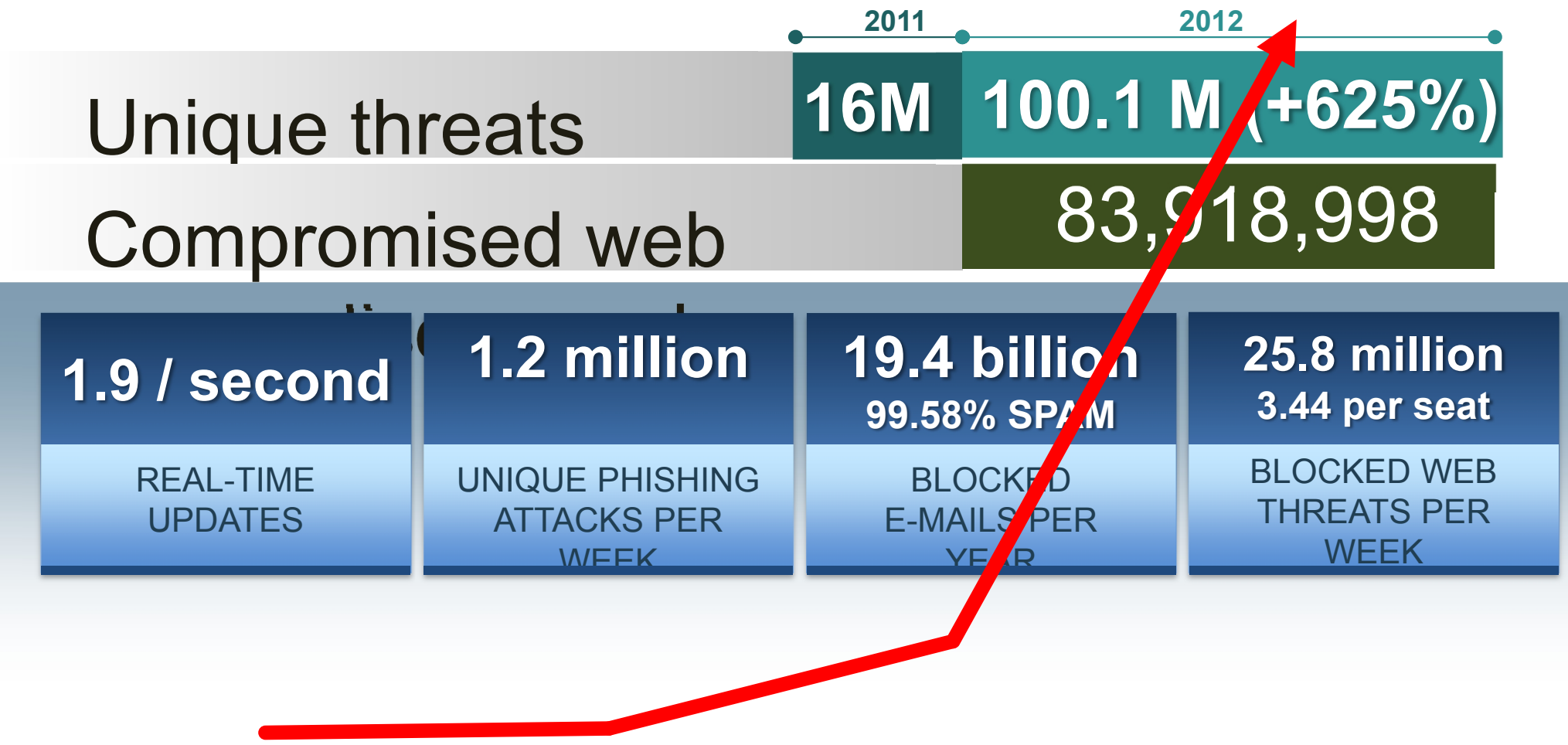
websense

- **Existing Security Deployments based on signature based technology.**
- **Insight into advanced (signature-less) threats is crucial.**
- **Threat monitoring provides insight into previously invisible threats.**

YOU CAN'T PROTECT AGAINST INVISIBLE THREATS

More, more and more

websense

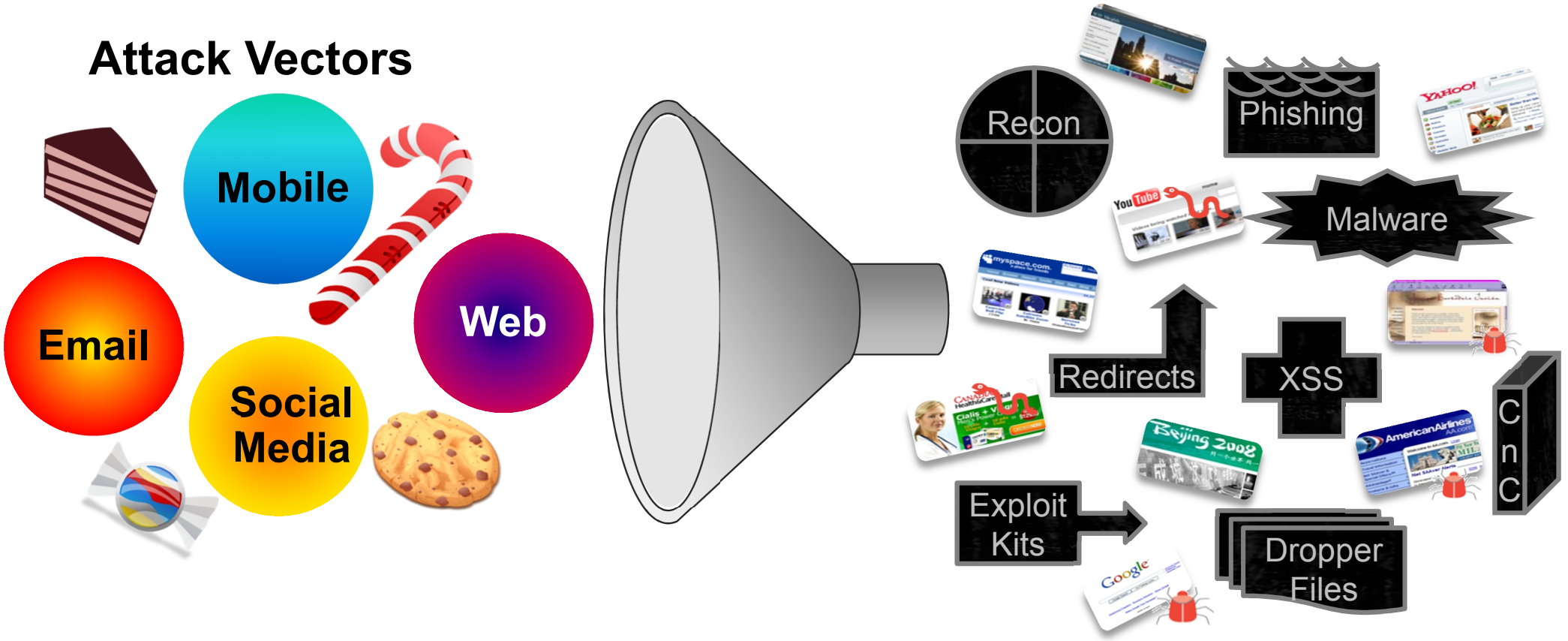


The Nature of Advanced Persistent Threats

websense®

Victims are funneled to the Web

websense



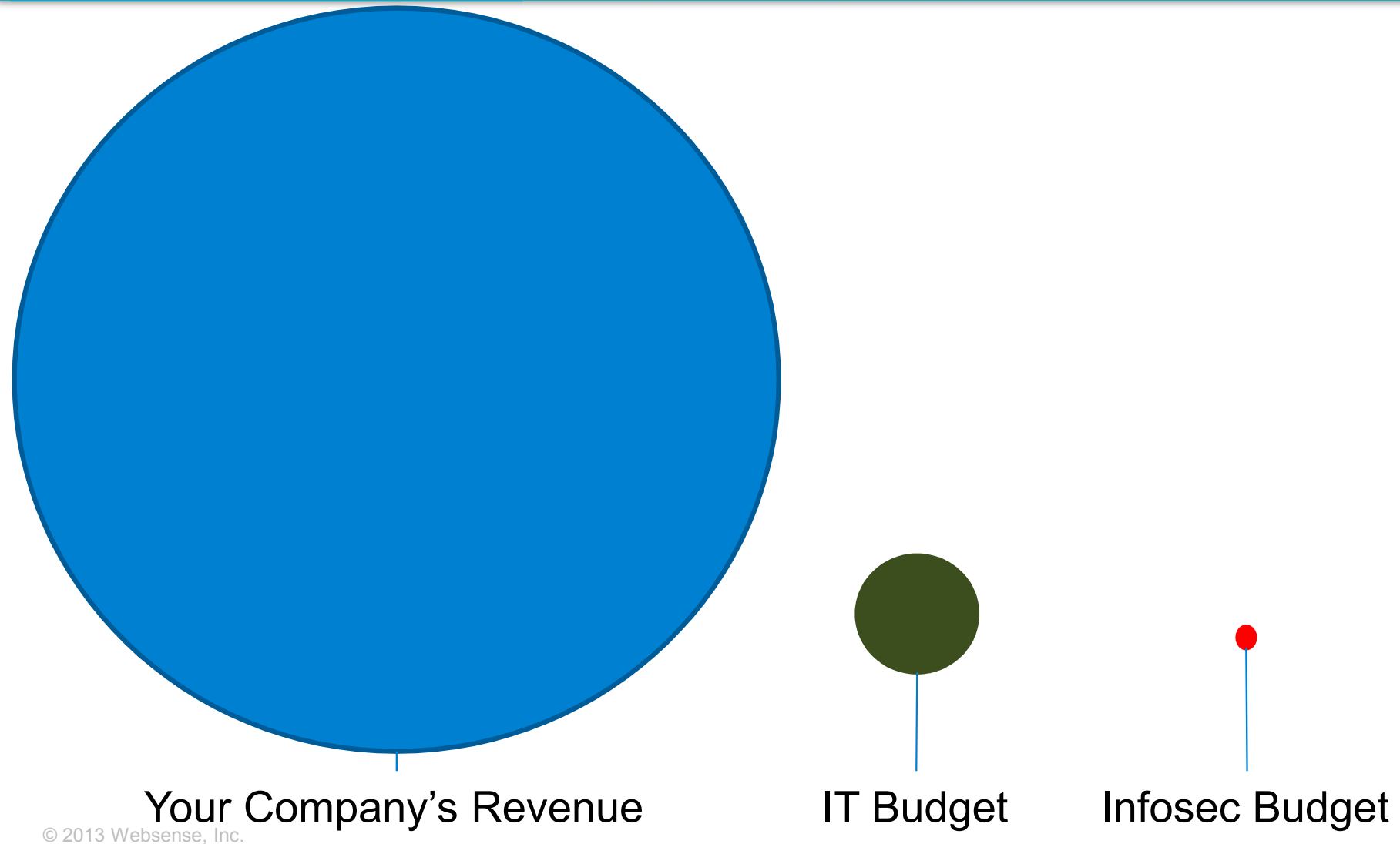
What's on the IT Executive's mind

websense®

- Targeted Attacks / APT
- Spear phishing
- Data Theft
- Mobility
- Attack Preparation (IRP)
- Business Enablement
- Advanced Malware
- Cloud
- Intelligence
- Compliance
- Insider Threats
- Hactivist

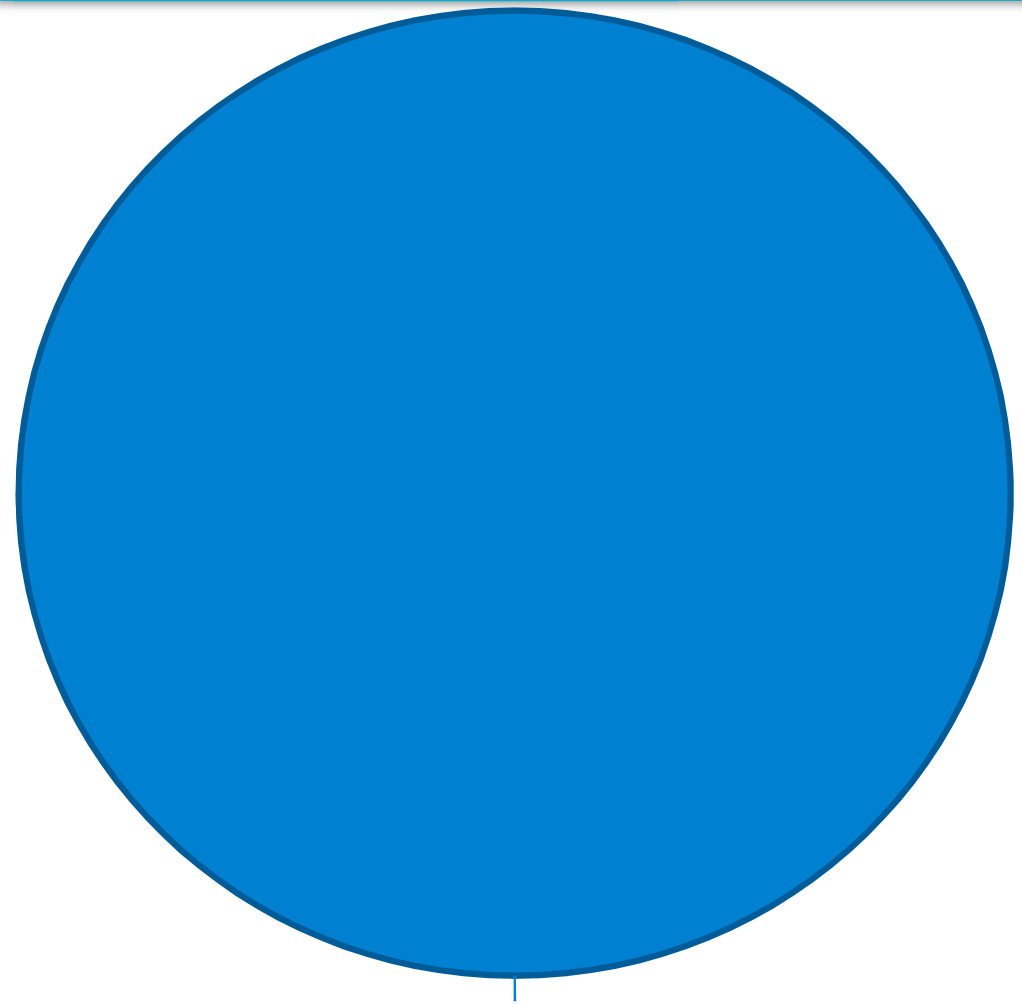
Office of the CSO

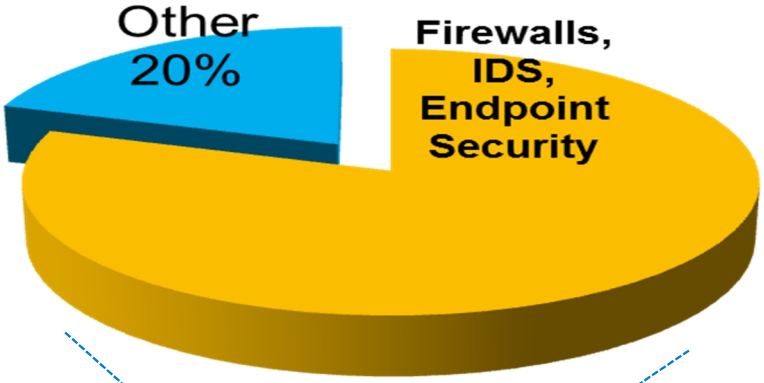
websense

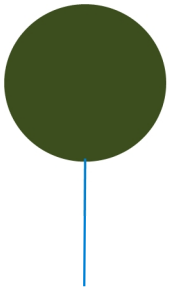


Office of the CSO

websense







Your Company's Revenue

IT Budget

Infosec Budget

80% OF THE SPEND IS 30% EFFECTIVE AT SECURING THE BUSINESS.

Changing Threat Landscape

websense

Advanced Threats

THEN	NOW
Signature Based	Zero Day
High Volume	Low Volume
Mass Distribution	Trusted Entry

Data Theft

THEN	NOW
Goal: Damage	Goal: Financial gain
Inbound focus was enough	Assume holes in security
Data was easily identifiable	Theft can easily be hidden

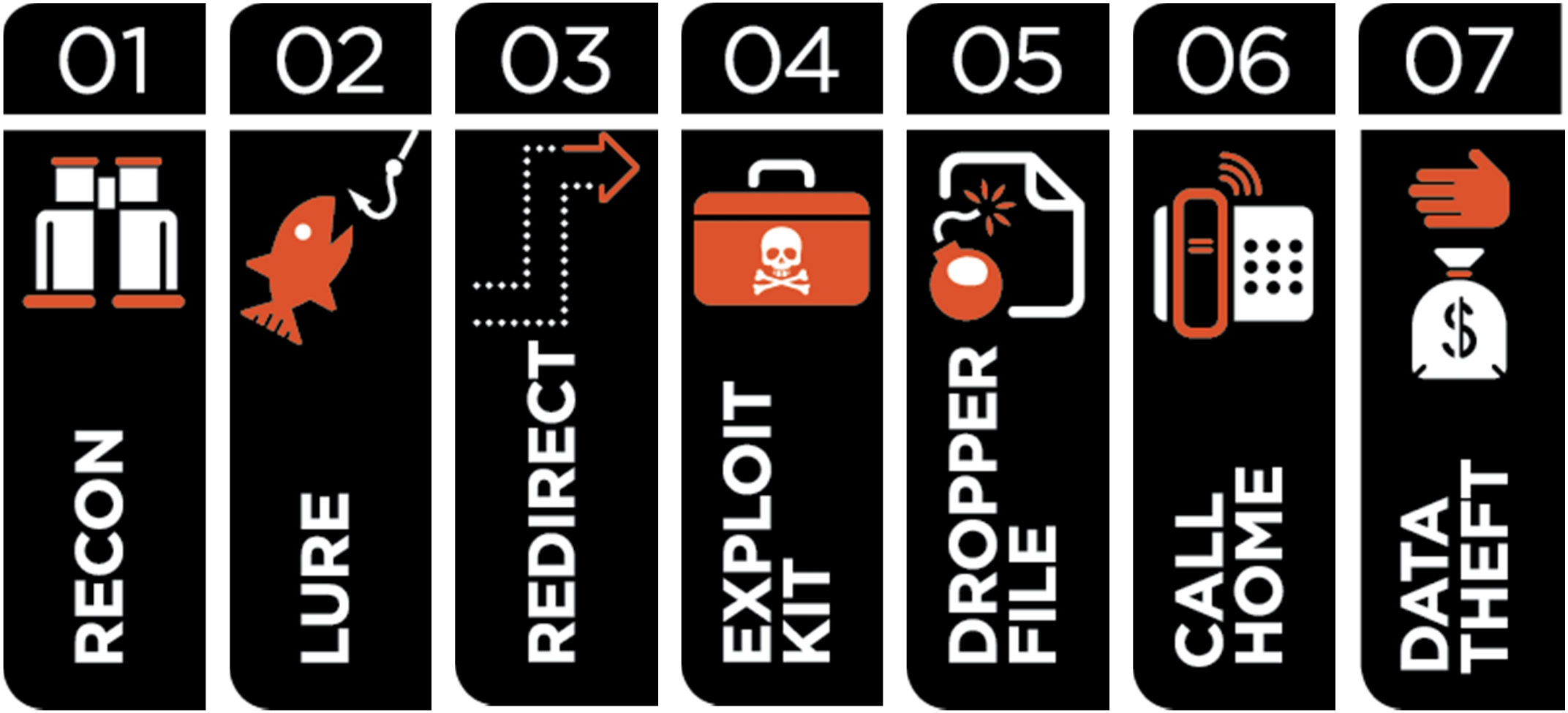
Attack & Malware Forensics

THEN	NOW
Hands-Off	Hands-on
Reactive	Proactive
Focus on intrusion prevention	Holistic View


TIME FOR A CHANGE

The Seven Stages of Advanced Threats

websense®



Reposition our Active and Passive Defenses

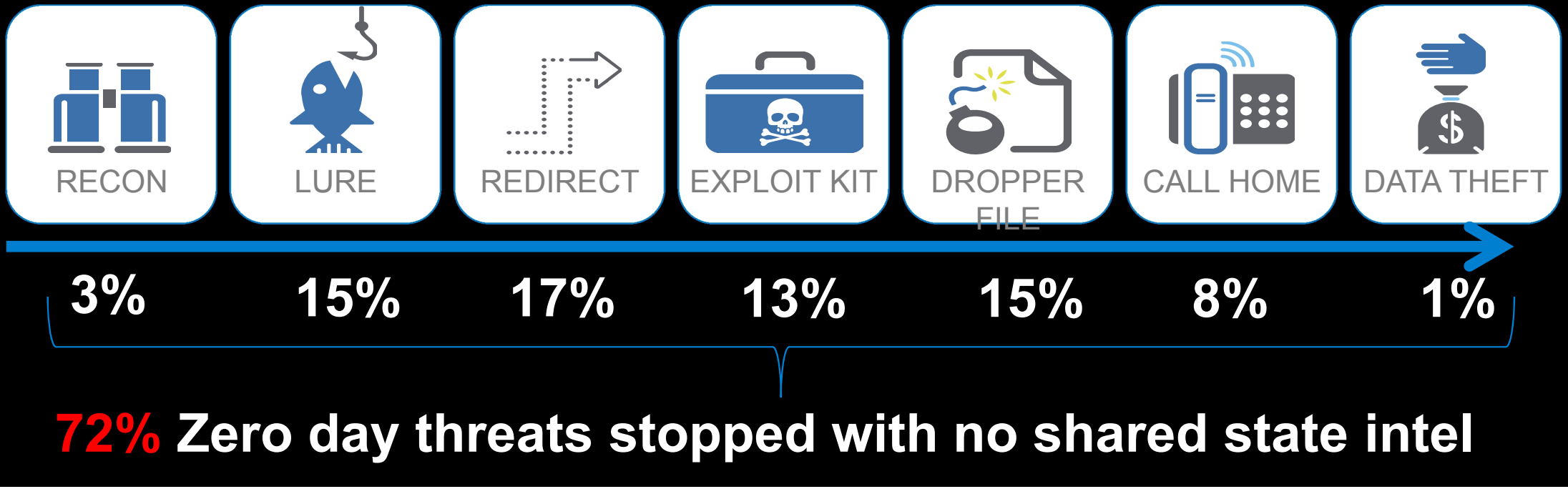
websense

Stages of Advanced Attack

RECON | LURE | REDIRECT | EXPLOIT KIT | DROPPER FILE | CALL HOME | DATA THEFT

Advanced threat effectiveness of point solutions

websense



72% Zero day threats stopped with no shared state intel

Advanced threat effectiveness by sharing intelligence

websense

RECON	LURE	REDIRECT	EXPLOIT KIT	DROPPER FILE	CALL HOME	DATA THEFT
~~3%~~ 3%	~~15%~~ 17%	~~17%~~ 20%	~~13%~~ 17%	~~15%~~ 20%	~~8%~~ 17%	~~1%~~ 7%

99% Zero day threats stopped with horizontal sharing


WHY PROTECTIONS FAIL

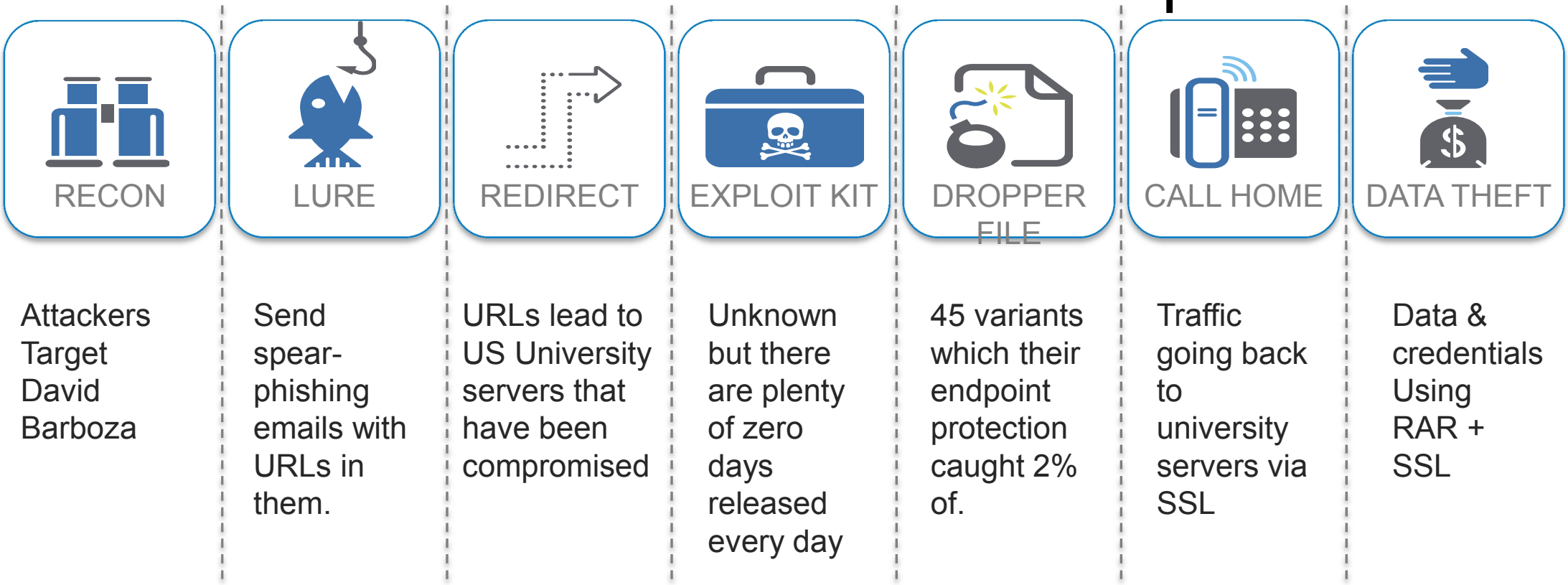
THE FAILURE OF "TRADITIONAL" SECURITY

websense

Know your enemy: How they attack

websense

2013 NY Times Attack Example

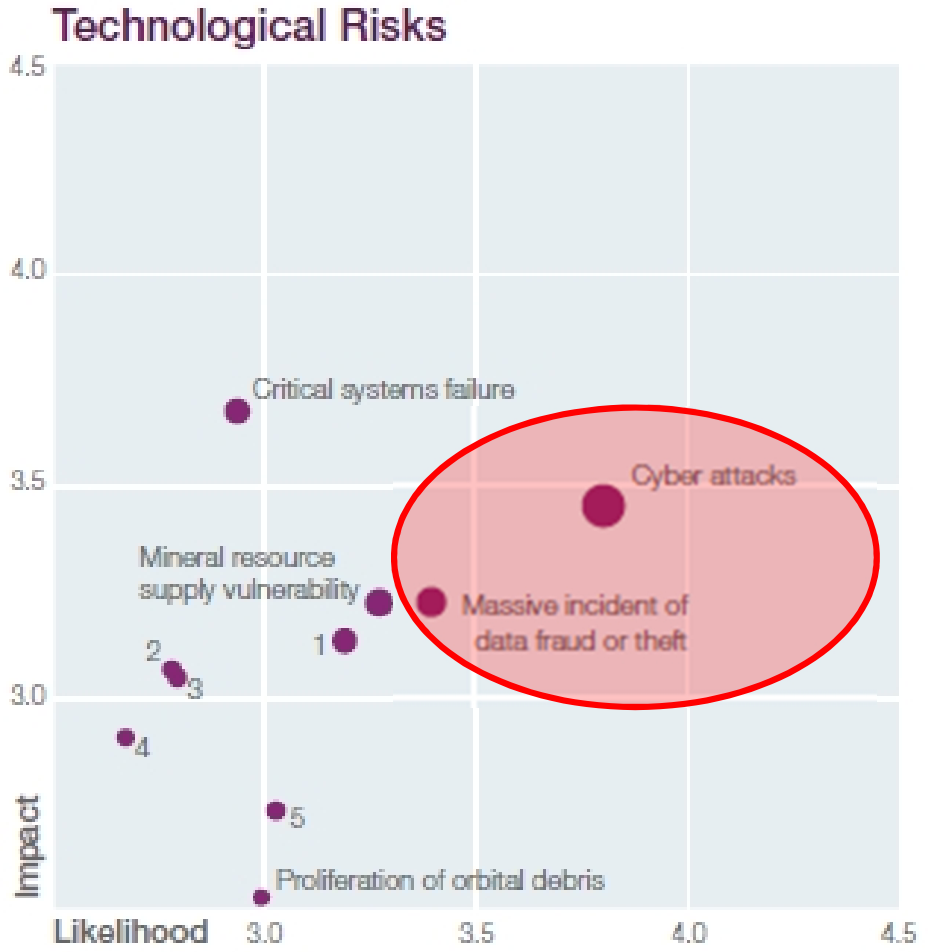


© 2013 Websense, Inc.

Who is At Risk?

websense

- **Government Agencies and Vendors**
- **Financial Sector and Vendors**
- **News Agencies and Vendors**
- **Multiple Industries**
- **Targeted Attacks include compromising legitimate domains**



Source: World Economic Forum

A Cocktail Of Essential Defenses

websense

Who Has The Right Mix ?

websense

Tier	Technology	Product/Solution			Primary Mechanism	Stages
		NGFW	UCS	AMD		
CC	SI Firewall	✓			rules	1*
CC	IDS/IPS	✓			signatures	4,5
2G	Traffic analysis	✓			anomaly	1,6,7
2G	Application control	✓	✓		rules	1,2,3
CC	Gateway AV	✓	✓		signatures	4,5
CC	URL filtering	✓	✓		rules, reputation	1,2,3
CC	Reputation filtering		✓		reputation	4,5
2G	Email security		✓		signatures. reputation, heuristics	most
2G	Web security		✓		signatures, reputation, heuristics	most
AD	Real-time analysis		✓		heuristics	4,5
AD	Gateway DLP		✓		signatures, rules	1,7
AD	Call-home	✓	✓	✓	anomaly	6
AD	Sandboxing		✓	✓	anomaly/behavior	5
AD	Intelligent coordination		✓		correlation, composite scoring	2,3,4,5

Notes:
NGFW = next-generation firewall
UCS = Unified content security
AMD = advanced malware defenses
* refer to Footnote 2 below

WHAT WE CAN DO

Threat Changes Require New Defenses

websense

Changing Threat Landscape

- Advanced Threats
- Data Theft
- Attack and Malware Forensics

7 Stages of Advanced Threats

New Security Requirements

- Protection from advanced threats
- Containment against data theft
- Threat dashboard / Severity alerting
- Forensic reporting / SIEM integration
- Malware analysis sandboxing & services
- Performance & availability of defenses

A Balanced View on Security

websense

Inbound

- Advanced Malware Payload Detection
- Potentially Exploited Documents
- Mobile Malware
- SSL Traffic Inspection
- Cloud Sandboxing of Email Links
- Application Control

Outbound

- Criminal Encrypted Uploads
- Password File Theft Detection
- Dynamic Malware Command and Control
- Unauthorized Mobile Market Places
- OCR (Optical Character Recognition
- Drip (Stateful) DLP
- Geo-Location

Analysis Tools

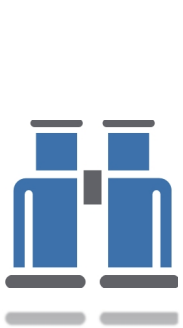
- Sandboxing Service
- Advanced Threat Dashboard
- Forensic Reporting

Websense – Protecting Against Advanced Threats

websense

Who Can Cover All The 7 Advanced Threat Stages ?

websense®



RECON

LURE

REDIRECT

EXPLOIT KIT

DROPPER FILE

CALL HOME

DATA THEFT

websense®
TRITON

Analysts Recognize Websense

websense

Gartner

- 2013 **Secure Web Gateway MQ:** Leaders Quadrant
- 2013 Content-Aware **Data Loss Prevention MQ:** Leaders Quadrant
- **Secure Web Gateway Software** 2012 Worldwide Market Share Leader

INFO~TECH research group

- **2012 WCF Vendor** Landscape: Champion
- **2012 DLP Vendor Landscape: Champion & Trend Setter Award**

FROST & SULLIVAN

- 2012 **Global Web Content Filtering** Competitive Landscape: Sole Market Leader
- 2012 **Global Web Content Filtering** Market Share Leader

FORRESTER®

- 2012 **Email Content Security Wave:** Leader

Gartner

- 2013 **Secure Email Gateway MQ:** Visionaries Quadrant

EMA

- **Hosted Message Security Services** Radar Report: Value Leader
  Best Hybrid Strategy Award

INFONETICS RESEARCH

- **Integrated Content Security Gateways** CY12 Worldwide Market Share Leader

IDC *Analyze the Future*

- 2012 **IDC MarketScape: WW Web Security Products:** Leader
- **Web Security Software** 2012 Worldwide Market Share Leader

THE RADICATI GROUP, INC. A TECHNOLOGY MARKET RESEARCH FIRM

- 2013 Corporate **Web Security** Market Quadrant: Top Player
- 2013 Content-Aware **Data Loss Prevention** Market Quadrant: Top Player

APAC Customers That Trust Websense

websense

websense®

TRITON stops more threats.

We can prove it.