



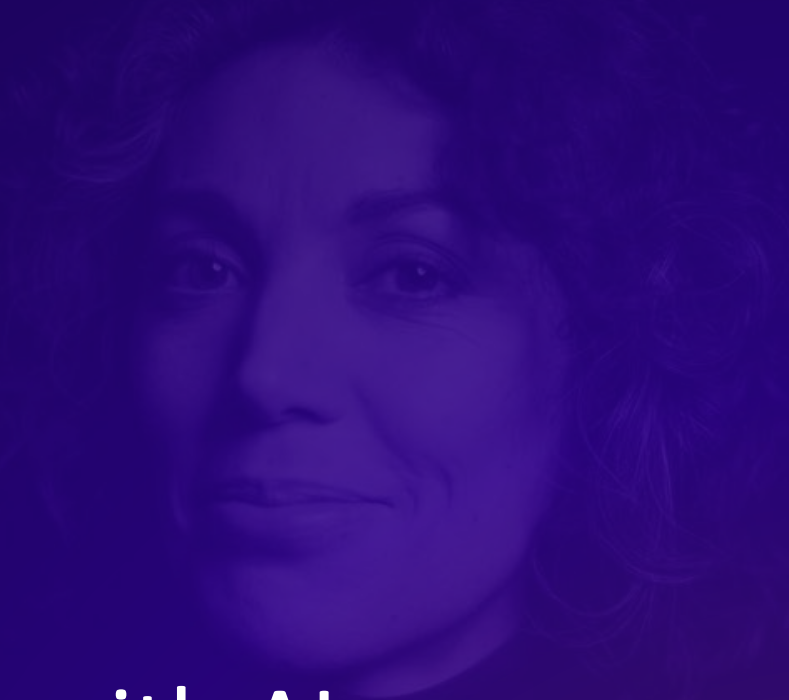
Armorblox

Security Powered by Understanding

Balancing Security and Privacy with AI

Melinda Marks

Armorblox





You Can't Secure What You Can't See



Technology Advances

Devices are cheaper and
better, so we can use them
for security

Security Cameras



Increasing security with technology

1. Need people to look at footage
2. Identify suspicious behavior



REPORT: San Francisco Considers Installing Cameras with Microphones



Thursday, March 21st, 2019

SAN FRANCISCO (KGO) -- Smart city or invasion of privacy? More surveillance cameras may soon be installed in San Francisco streets.

According to the Examiner, the city considering a sweeping installation of devices with cameras, microphones.

The \$19 million proposal to buy the devices comes after San Francisco began testing 60 of them in select areas of the city since last May.

The devices are raising privacy concerns.

Technology to catch criminals





State Data Law Heightens Privacy Protection for Virginians



By Meredith Mason, Strategic Communications Manager , ACLU of Virginia

APRIL 4, 2019 | 4:00 PM

TAGS: [Automatic License Plate Readers](#), [Location Tracking](#), [Privacy & Technology](#)



Powerful new technologies make mass surveillance easier than ever for law enforcement. One such technology, automatic license plate readers (ALPRs), capture location data that can reveal people's religious, political, sexual, medical, and social activities. For years, law enforcement agencies across the country have collected and stored this data with very little oversight and few legal constraints.

For the ACLU of Virginia, taking on this major privacy issue has been a four-year fight that began with efforts

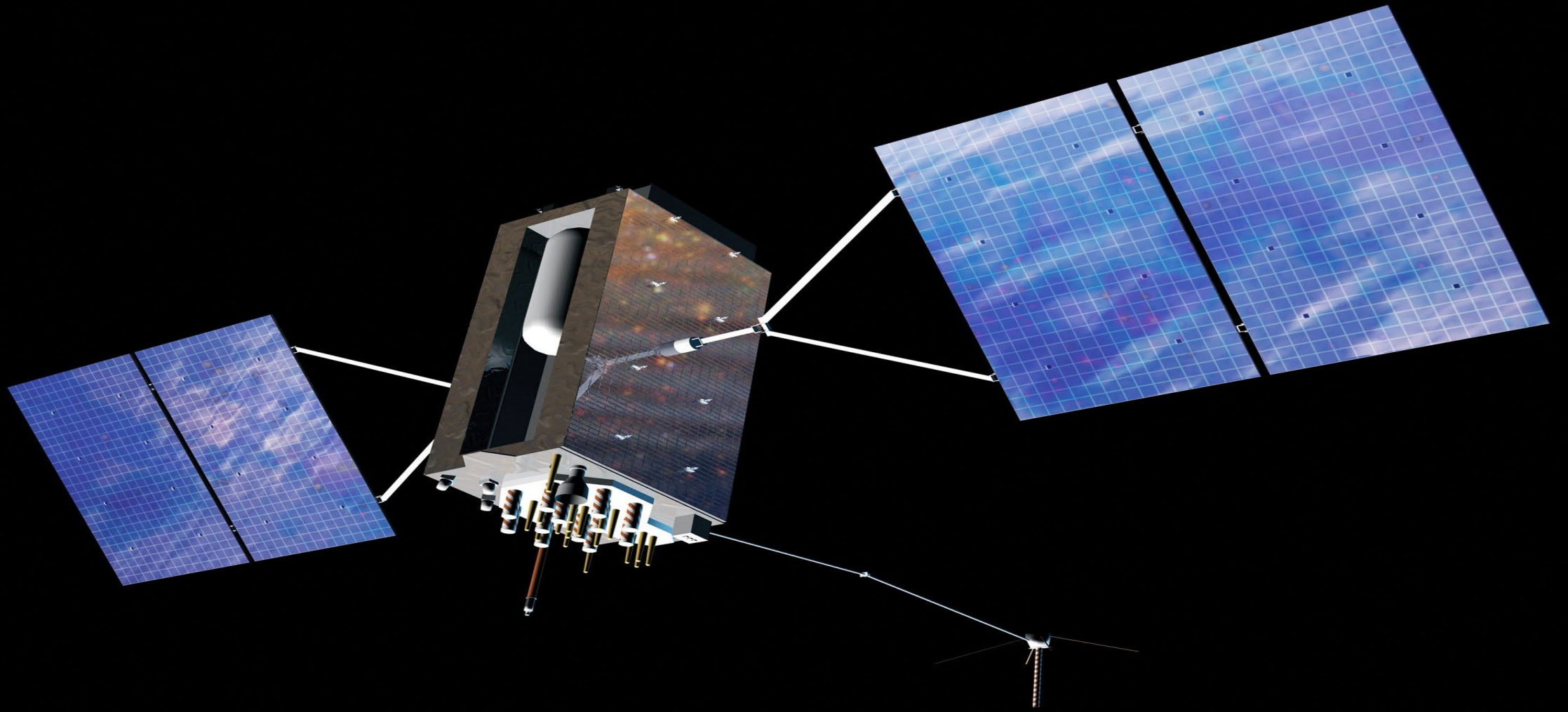




Increasing Productivity

We are interested in giving up security and privacy for technology that enables increased efficiency

GPS Systems

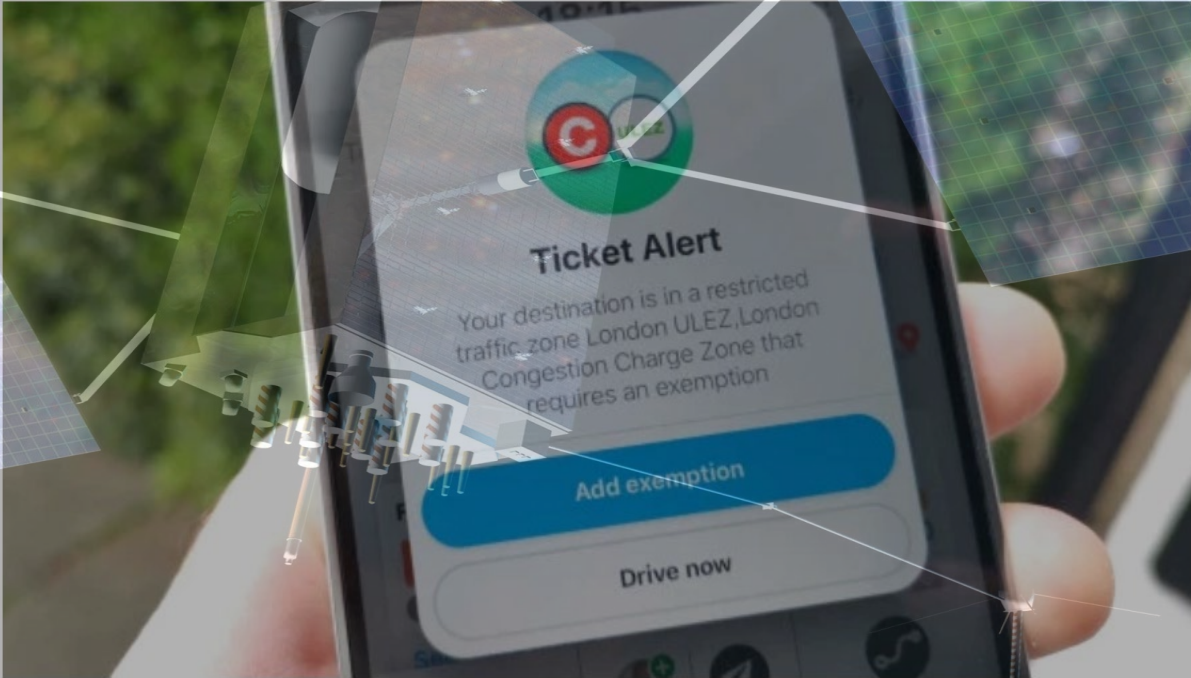


GPS Systems – But what about security and privacy?

TRANSPORTATION FEATURE

How Waze is using data pacts, beacons, and carpools to win over cities

PAUL SAWERS @PSAWERS APRIL 5, 2019 10:03 AM



Above: Waze has integrated with TfL's new ULEZ traffic pollution system in London
Image Credit: Paul Sawers / VentureBeat

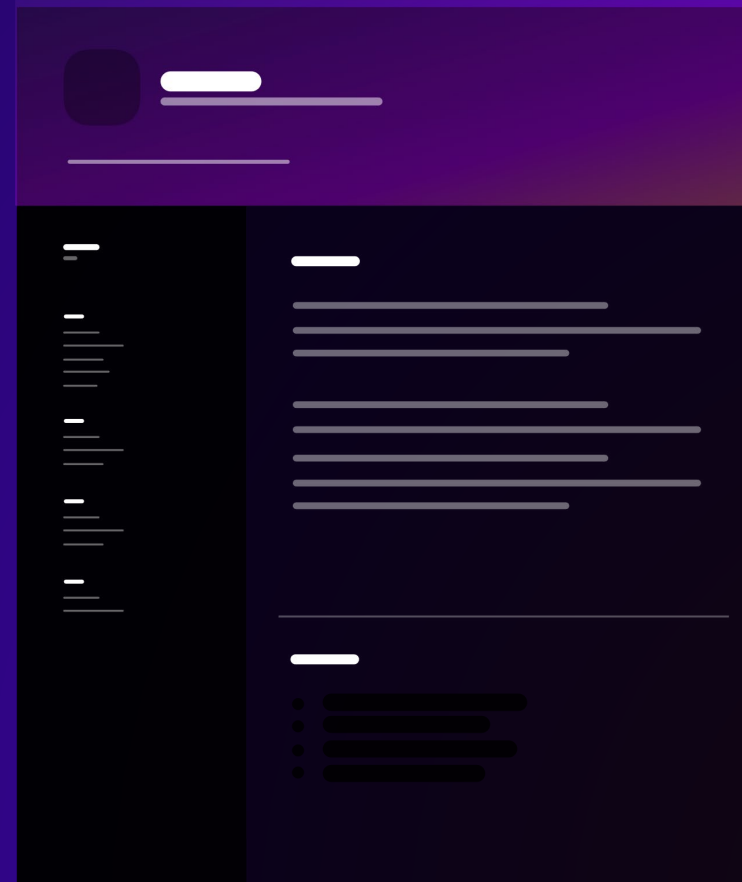
AI Means the Machines Do the Work

- Facial recognition
- Identify when unauthorized people enter
- Identify when items appear or disappear
- Humans going through data is not scalable or reliable, and there are privacy issues, AI can do the above without these issues
- Gain the benefit of real-time



What About Enterprise IT Security

- Top Threat vectors are through human communication
- Monitoring human communications brings privacy issues
- AI lets machines do the work



Spending on cybersecurity is at an all time high

- The **2018 U.S. State of Cybercrime survey** is conducted annually by CSO in partnership with the US Secret Service and CERT at the Software Engineering Institute at Carnegie Mellon University. The survey covers the time period of June 2017 to May 2018.
- Of the 515 respondents, 34 percent identified themselves as IT management, 20 percent said they were in security management, 14 percent said they were business management, and the remainder said they were staff or other. The average company size was 10,874 people, and 51 percent of respondents said they worked for small-to medium-sized companies while 49 percent worked at enterprise-level organizations.
- **Average spend: \$15m, up from \$11m in 2017**

Multiple security tools are in place

CYBER RANGE ATTACK IQ SENSATO	NETWORK SECURITY tenable TEMPERED BlueLock PROFICIO corelight BAYSHORE FUDDO TRUSONA STELLAR WUIVEX cybercheck GRIFONITE BANDJIRA VERSA REDSEAL MixMode Fidelis Sempix 802secure VERY GOOD SECURITY VECTRA NewVector BLUE RIDGE secon ISYCCURE Reservoir Labs Attivo SS8 lastline TRAPX FlowTraq PROTECTOR BLUE HEXAGON Babix AWAKE OPAG ecyteck ACALVIO	CLOUD SECURITY FlowTraq cawirin CEQUENCE SECURITY THREATX Reblaze SAVVYNT zeguro TRUSONA SECBERUS ziften Reblaze REDSEAL securix VERA Aporoto WUIVEX lastline JUPITERONE Fortanix POLYVERSE secon STELLAR SS8 anJuna Sempix OPAG ISYCCURE CloudPassage TRAPX Layered Insight FortiMail deepfence Reservoir Labs BLOOMBASE ACALVIO VERSA tenable PROFICIO ecyteck PROTECTOR NewVector VERY GOOD SECURITY TEMPERED FUDDO mHero	IoT - IIoT ISYCCURE tenable BAYSHORE TEMPERED Attivo xage BLUEBASE TRUSONA secon CPDKNOX CRYPTONITE lastline TRUSONA TRAPX VECTRA ICON LABS reform labs AUTHOMATE Digital Security CYBERICAL 802SECURE MixMode SS8 eNTHITYID wafarm	CYBER INTELLIGENCE SENSATO CHEQ PROFICIO TRU*STAR SayChack BANDJIRA GRAY NOISE Pulsedive digital shadows POLARITY CYCOGNITO SecurityHybrid Yulsec REVERSING LABS ecyteck			
COMPLIANCE & DLP BLOOMBASE BlueLock FlowTraq AUTHOMATE BOTDOC-10 Ignite zeguro VERY GOOD SECURITY VUIVEX cybercheck VERA jonrain ALLGRESS secon cawirin JUPITERONE ISYCCURE SECURONIX 802secure SENSATO CloudPassage EXOSTAR mHero kriptos SAVVYNT Layered Insight R-sam	WEB SECURITY CEQUENCE SECURITY CHEQ Reblaze TRUSONA Aporoto VERY GOOD SECURITY CONTRAST TRON SECURITY ARXAN THREATX SHARA Digital Shadows wafarm SEWORKS Layered Insight CYCOGNITO AUTHOMATE TALA Cabot OPAG	ENDPOINT SECURITY tenable SentinelOne NYOTRON BlueLock ISYCCURE ARXAN AUTHOMATE POLYVERSE TRAPX depenstact CRYPTONITE TRUSONA Fidelis TRON SECURITY OPAG sparkognition RocketCyber 802secure ziften	MOBILE SECURITY AUTHOMATE TRUSONA BOMCHESSENDER UNIFYID VERY GOOD SECURITY appknox ARXAN depenstact Cabot SEWORKS BETTER	AI CHEQ THETARAY SEWORKS Babix CENASA SYSTEMS Armorbox FUDDO depenstact secon kriptos SEMPURIFY depenstact	IAM BlueLock AUTHOMATE Kount Nive.id Hivemind jonrain colsign TRUSONA SAVVYNT nok nokia EXOSTAR pre-empt	FRAUD THETARAY CHEQ Kount Nive.id calsign UNIFYID SECURONIX TRUSONA SayChack SEMPURIFY SENSATO	
INFORMATION PRIVACY BlueLock NITRO Security Ignite BOTDOC-10 Yulsec VERY GOOD SECURITY NIVEID SEMPURIFY ALLGRESS DataCloudFlow jonrain UNIFYID ISYCCURE BOMCHESSENDER R-sam FUDDO REVEALINK mHero a-b	APPLICATION SECURITY AUTHOMATE CEQUENCE SECURITY Reblaze SEWORKS ISYCCURE Aporoto POLYVERSE mHero PROTEGO Cabot wafarm NETSPT TEMPERED tenable ARXAN TALA THREATX anJuna Layered Insight deepfence	DETECTION & PREVENTION NYOTRON BAYSHORE VadeSecure Reblaze raditow NITRO ENCODE CHEQ MixMode depenstact 802secure ACALVIO anJuna CYBERICAL THETARAY Attivo lastline BANDJIRA Bay Dynamics Fidelis STELLAR SECURONIX TRAPX wafarm PROTECTOR zeguro VECTRA UNIFYID kriptos SentinelOne ARXAN SS8 ISYCCURE secon WUIVEX cybercheck GRIFONITE FlowTraq BlueLock FISK mHero ecyteck PROFICIO BLUE HEXAGON OPAG mHero	PHISHING VadeSecure CHEQ nok nok GRAPHUS Curious Armorbox NITRO mHero	SOC TRU*STAR raditow NITRO ENCODE RocketCyber UNIFYID WUIVEX NIVEID SEMPURIFY SENSATO Pulsedive REVERSING LABS STELLAR VECTRA depenstact secon GRAY NOISE JASK SECURONIX POLARITY FLOWTRAQ CYBERICAL Babix SEMPURIFY JUPITERONE ecyteck			
EMAIL SECURITY VadeSecure lastline GRAPHUS Armorbox mHero	UEBA CHEQ SECURONIX UNIFYID Bay Dynamics CENASA SYSTEMS GRAPHUS secon GRAPHUS pre-empt	DECEPTION ACALVIO CHEQ SENSATO POLYVERSE 802secure TRAPX Attivo STELLAR brainlogic Fidelis	CYBER POSTURE NETSPT a-b tenable mHero VUIVEX Yulsec zeguro digital shadows Bay Dynamics 802secure FortiMail Ignite Cyberator SecurityScorecard PREVALENT TRON SECURITY REDSEAL TrustMAP Pre-Cog cyberGRX ALLGRESS CYCOGNITO JUPITERONE Ostendo POLYVERSE NormShield NISOS FISK CloudPassage lastline KENNA Security Balbix ecyteck R-sam	BAS NITRO ENCODE Cymulate MXY CYBER SafeBreach Pre-Cog SCITHE NETSPT ecyteck ATTACK IQ	INCIDENT RESPONSE & FORENSICS CYBERPULSE Ignite BABY7 NITRO ENCODE MixMode REVERSING LABS TRAPX AWAKE Fidelis 802secure POLARITY R-sam CENASA SYSTEMS REDSEAL Attivo DEMISTO VECTRA NISOS cybercheck NIVEID WUIVEX SENSATO SS8 secon SEMPURIFY STELLAR FlowTraq Pulsedive		
INSIDER THREATS Attivo FUDDO jonrain a-b AWAKE secon Armorbox Ignite SS8 anJuna SECURONIX Fidelis Bay Dynamics TRAPX FISK ACALVIO	BLOCKCHAIN hive.id SEWORKS AUTHOMATE Pre-Cog xage BOMCHESSENDER	AUTOMOTIVE ARXAN SENSATO Trillium	AVIATION NYOTRON EXOSTAR PROFICIO UAVs 802secure	RAIL & METRO TEMPERED PROFICIO	MARITIME TEMPERED CUBER MARINER	ICS/SCADA TEMPERED BAYSHORE raditow CYBERICAL MixMode Attivo BLUE RIDGE DRAGON ICON LABS TRAPX tenable xage	HEALTHCARE JUPITERONE NYOTRON BlueLock TEMPERED PROFICIO Attivo Ignite Ostendo WUIVEX EXOSTAR SEMPURIFY FISK 802SECURE R-sam wafarm SENSATO BABY7 TRUSONA

Attacks are Still Getting Through

2019 Verizon Data Breach Investigations Report:

96% of attacks begin with email

2019 Ponemon Cost of a Data Breach Study:

279 days to identify and contain a breach

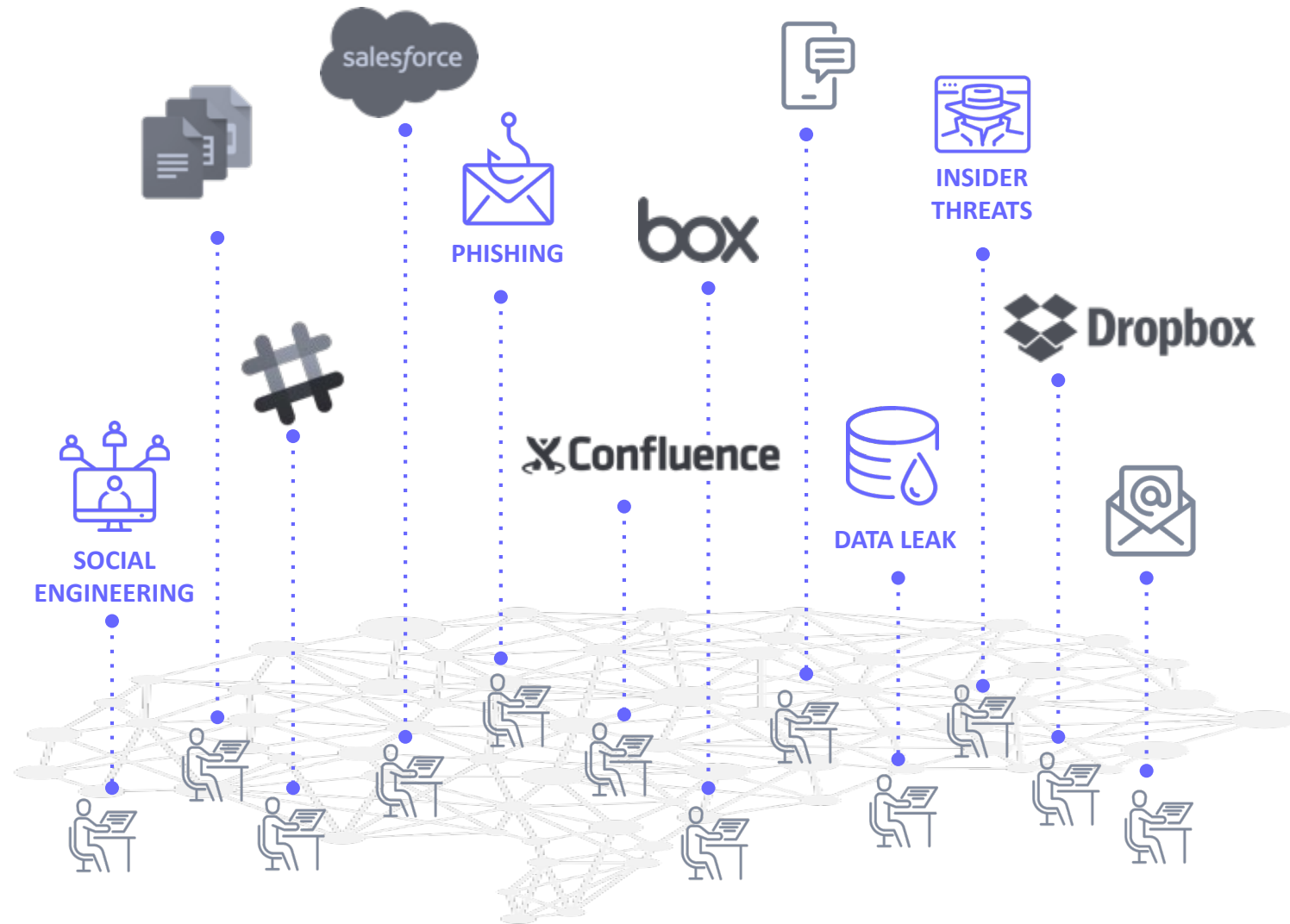
\$3.92M to detect a breach (up 1.5% from 2018)

\$8.19M to detect a breach in the U.S.

Why? Enterprise Security Lacks Understanding

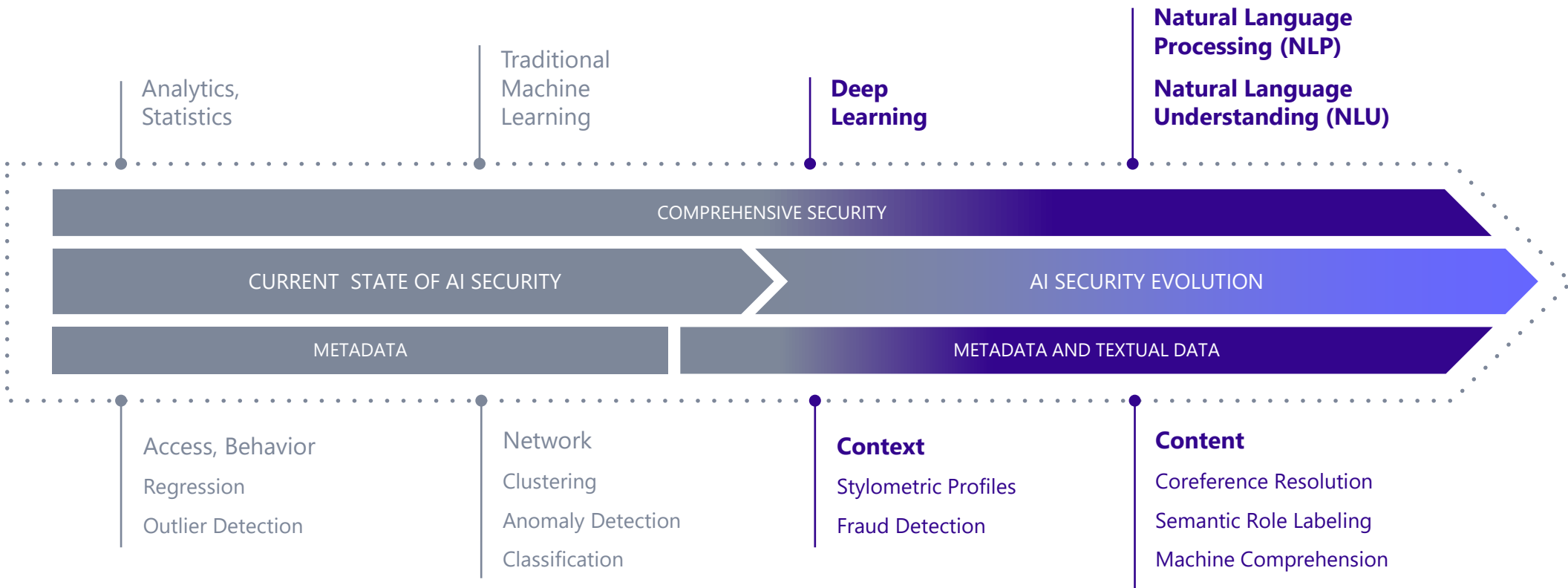
Textual data is everywhere within an enterprise

Emails, Documents, Spreadsheets, Slack, SMS, Salesforce, Confluence & more.



Current security tools focus on metadata. Lack understanding

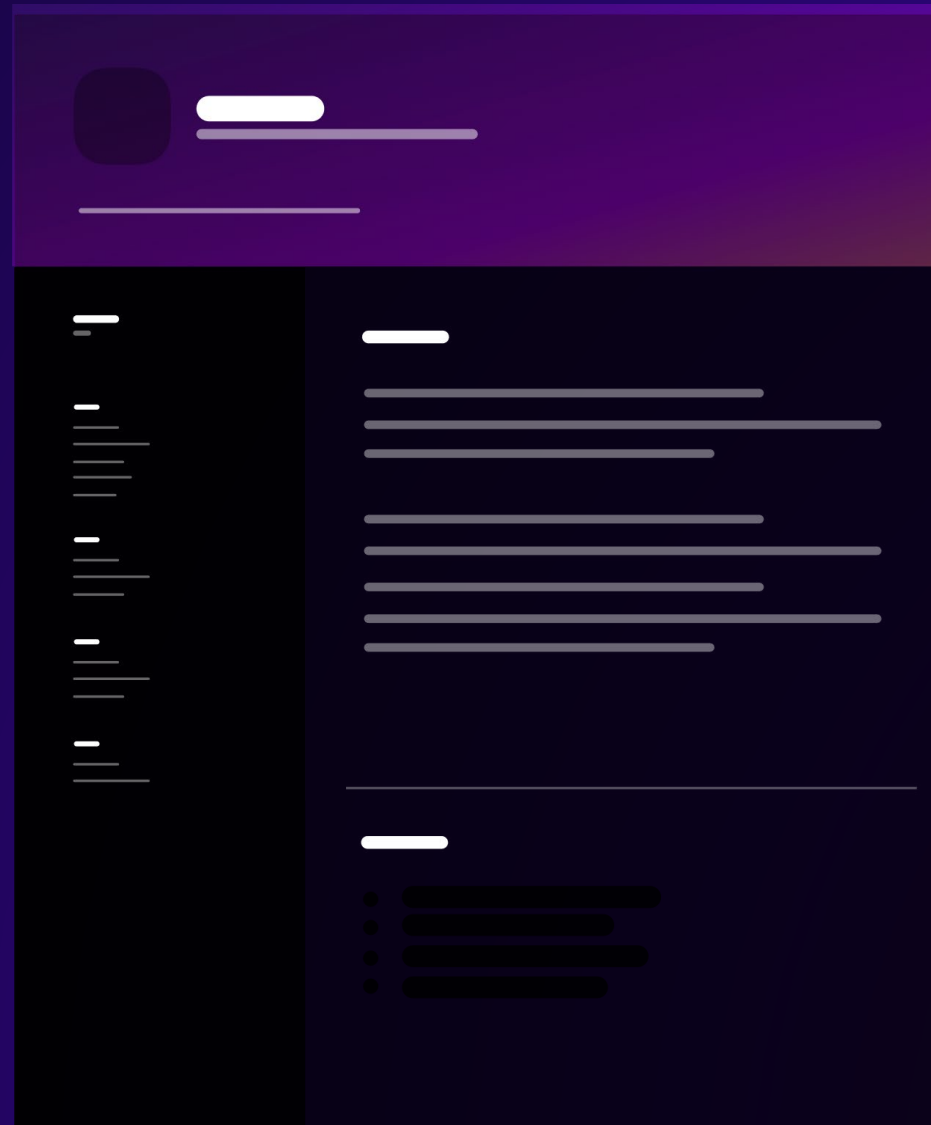
Evolution of AI for Security



Extract Intelligence from Textual Content

Identify sensitive content

Analyze writing styles



Extract topics and entities

Correlate across emails, and documents

Business Email Compromise



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

September 10, 2019

Alert Number
I-091019-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

BUSINESS EMAIL COMPROMISE THE \$26 BILLION SCAM

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA 1-071218-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to July 2019.

DEFINITION

Business Email Compromise/Email Account Compromise (BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

- The Financial Crimes Enforcement Network (FinCEN) July 2019 Analysis
- \$300M/month in attempted BEC thefts

27 FBI: \$1.2B Lost to Business Email Scams

AUG 15

The **FBI** today warned about a significant spike in victims and dollar losses stemming from an increasingly common scam in which crooks spoof communications from executives at the victim firm in a bid to initiate unauthorized international wire transfers. According to the FBI, *thieves stole nearly \$750 million in such scams from more than 7,000 victim companies in the U.S. between October 2013 and August 2015.*

Forbes

3,929 views | Sep 9, 2019, 01:00pm

Toyota Parts Supplier Hit By \$37 Million Email Scam



Lee Mathews Senior Contributor @
Cybersecurity
Observing, pondering, and writing about tech. Generally in that order.

- f The Toyota Boshoku Corporation, a major supplier of Toyota auto parts, reported some distressing news this week. Fraudsters fleeced the company via an email scam to the tune of about ¥ 4 billion (JPY). That works out to just over \$37 million at today's exchange rate.
- t
- in

Minnesota DHS Reports Health Data Breach from 2018 Email Hack

Minnesota DHS recently began notifying lawmakers of a data breach caused by an email hack from March 2018; phishing and malware attacks complete this week's breach roundup.

CYBER SECURITY NEWS

The Phishing Scam That Took Google and Facebook for \$100 Million

Scott Ikeda — On Apr 9, 2019

f Share t Tweet in Share p Pin It +

While what he did was at least equal parts forgery and phishing scam, Evaldas Rimasauskas' social engineering abilities and apparent deep knowledge of corporate invoicing processes allowed him to take two of the world's biggest tech companies for \$100 million using little more than an email account.

\$1.75 Million Stolen by Crooks in Church BEC Attack

By **Sergiu Gatlan**

April 29, 2019 06:49 PM



Image credits: Saint Ambrose Catholic Parish (Editing: BleepingComputer)

Hackers have stolen \$1.75 million from the Saint Ambrose Catholic Parish following a successful BEC (Business Email Compromise) attack which was discovered on April 17 after payments related to the church's [Vision 2020 project](#) were not received by a contractor.

Example: Business Email Compromise (BEC)



From: Joel Allen <Joel.Allen@acme.com>
To: Janice Crenshaw <Janice.Crenshaw@acme.com>
Monday June 18 2016 at 4:45 PM PDT

Everything should be done for closing on the Leander deal on the 29th. I have sent the closing statements via FedEx. Can you set up a wire transfer to go out tomorrow?

Is this message a threat?

Phishing Link Detection

Pass 

DMARC Checks

Pass 

Malware Checks

Pass 

DLP Scan

Pass 

Congratulations.
You've been Phished!



Understand Content and Context

From: Joel Allen <Joel.Allen@acme.com>
To: Janice Crenshaw <Janice.Crenshaw@acme.com>
Monday June 18 2016 at 4.45 PM PDT

<Everything>₁ should be done for closing on the <Leander>₃ <deal>₂ on the 29th. I have sent the <closing statements>₄ via <FedEx>₆. <Can you>₈ set up a <wire transfer>₅ to go out <tomorrow>₇?

<Leander> <deal>

Sensitive topic

<wire transfer>

Request

<tomorrow>

Urgency

<closing statements>

Sensitive content



PHISHING
ATTEMPT

Increased communications across platforms

The image shows a screenshot of a news article from The Wall Street Journal on the left and a text message conversation on the right. The article is titled 'Texting Moves to the Workplace, as Do the Awkward Misfires. 'I'm Here. I Luv U.' and is labeled 'A-HEAD'. The text message conversation includes the following messages: 'Yes', 'Please call me before noon.', 'I'll call you for se', 'What?', 'Sorry! I meant se', 'Sec!', and 'Call you in a sec!! Sorry'.

THE WALL STREET JOURNAL. SIGN IN SUB

A-HEAD

Texting Moves to the Workplace, as Do the Awkward Misfires. 'I'm Here. I Luv U.'

Oversharing colleagues are the least of it; the wrong 'pumpkinbear'

Talk

Yes

Please call me before noon.

I'll call you for se

What?

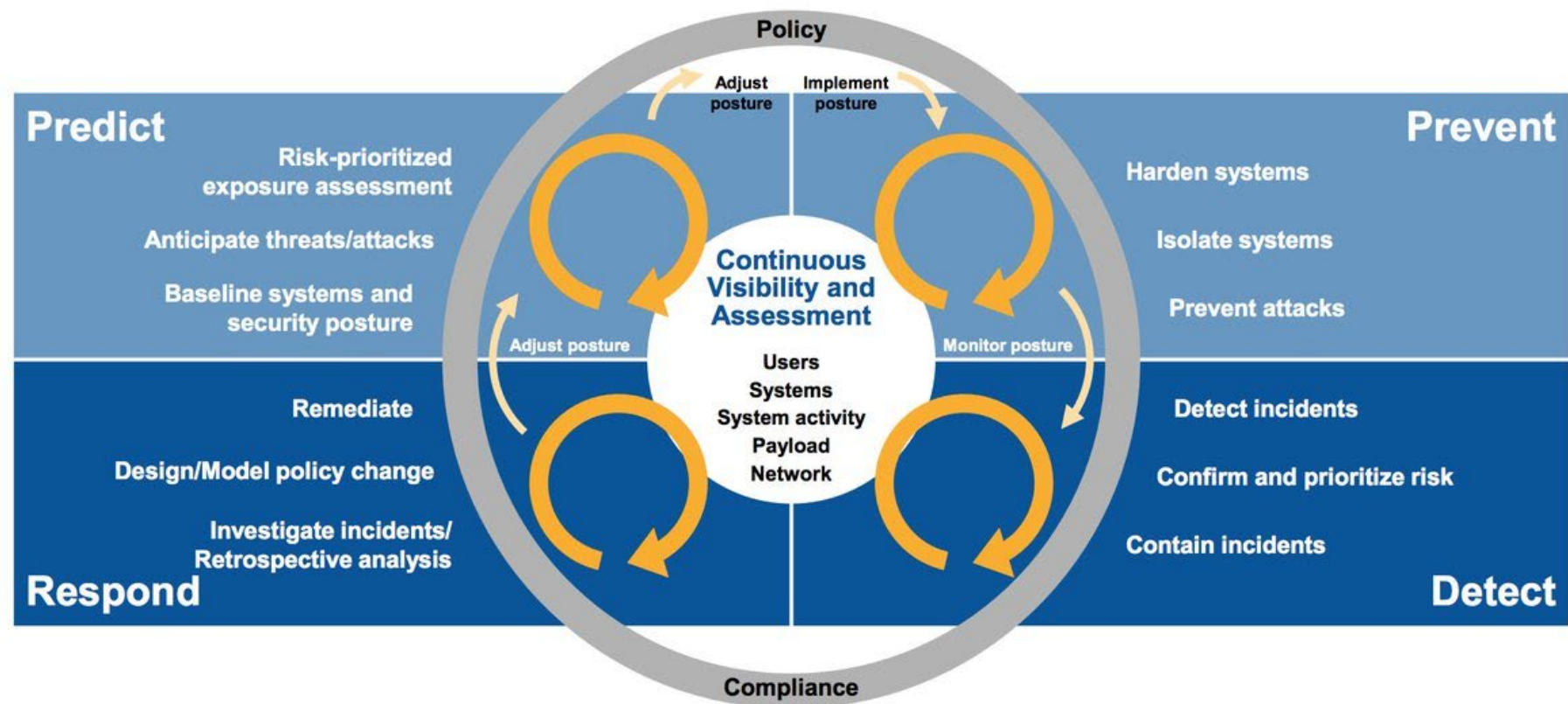
Sorry! I meant se

Sec!

Call you in a sec!! Sorry

Gartner: Continuous Adaptive Risk and Trust Assessment (CARTA)

CARTA Results From the Gartner Adaptive Security Architecture



Continuous, Adaptive Solution



Insider Threats

- Five different “personas” according to Verizon Insider Threat Report¹
 - Careless Worker
 - Inside Agent
 - Disgruntled Employee
 - Malicious Insider
 - Feckless Third Party

Insider Threat Report

Out of sight
should never be
out of mind

verizon✓
business ready



[1] <https://www.verizon.com/about/news/verizon-refocuses-cyber-investigations-spotlight-world-insider-threats>

Insider Threat #1: Careless Worker



- Most common scenarios
 - Misaddressed email recipients
 - Inadvertent content sharing to external and internal persons
 - Poorly configured access and/or security controls
- NLU Platform can potentially address these scenarios, especially the first two

Insider Threat #2: Inside Agent



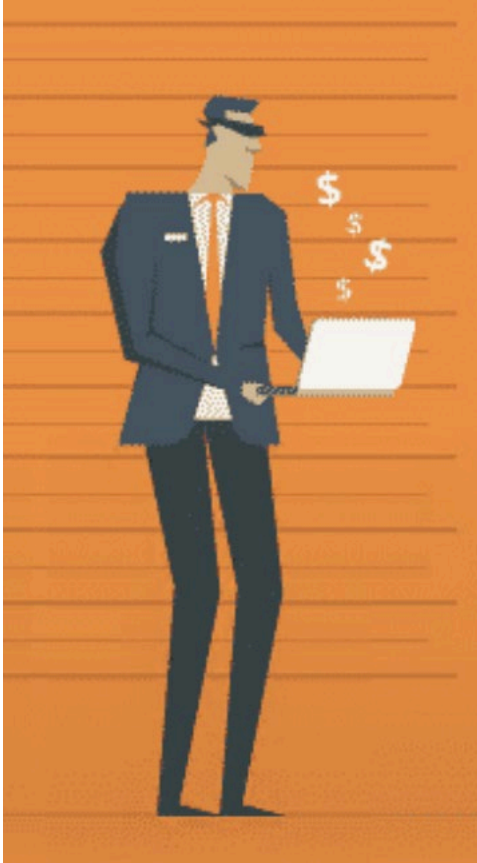
- Most common scenario
 - Corporate espionage through unauthorized access of data
- NLU Platform can go much beyond traditional Data Loss Prevention(DLP) products
 - By understanding context
 - By understanding communication patterns
 - By understanding intent

Insider Threat #3: Disgruntled Employee



- Most common scenarios
 - Disgruntled employee seeks to destroy or incapacitate company assets including digital assets
- NLU platform can help alert to such impending actions
 - By understanding sentiment
 - By understanding intent

Insider Threat #4: Malicious Insider



- Most common scenarios
 - Malicious insider typically steals company data for personal gain
 - Differentiated from Inside Agent
- NLU platform can help alert to such impending actions
 - By understanding context and restricting access to persons who “need-to-know” only

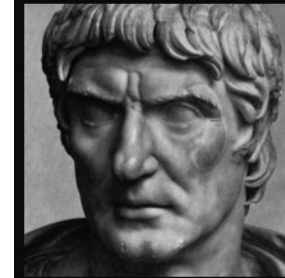
Insider Threat #5: Feckless Third Party



- Most common scenarios
 - Third party with access to sensitive information potentially leaks it inadvertently
- NLU Platform can help in preventing and/or mitigating such scenarios
 - By understanding communication patterns
 - By understanding context (ex: time of expiry)

Keep in Mind for Enterprise Security vs Privacy

- Set expectation that all enterprise communications are/can be monitored
 - Expectation that personal communications are not monitored
 - Avoid personal communication channels when at work
- Use encryption when possible
- Set the appropriate level of privileges for security analysts
 - Using RBAC? Is it effective
- Democratize triage to empower employees and save time for the security analyst
- False positives and machine learning: Use solutions that offer an explanation of why a certain decision was reached, check on whether there is a feedback/learning mechanism, make sure it is recorded for posterity



Who is to guard the guards themselves?

~ Juvenal

Thank You!

Learn more: <https://www.armorblox.com>

Email me:

M@armorblox.com

Follow us on Twitter: @armorblox
@melindamarks



Armorblox

Security Powered by Understanding