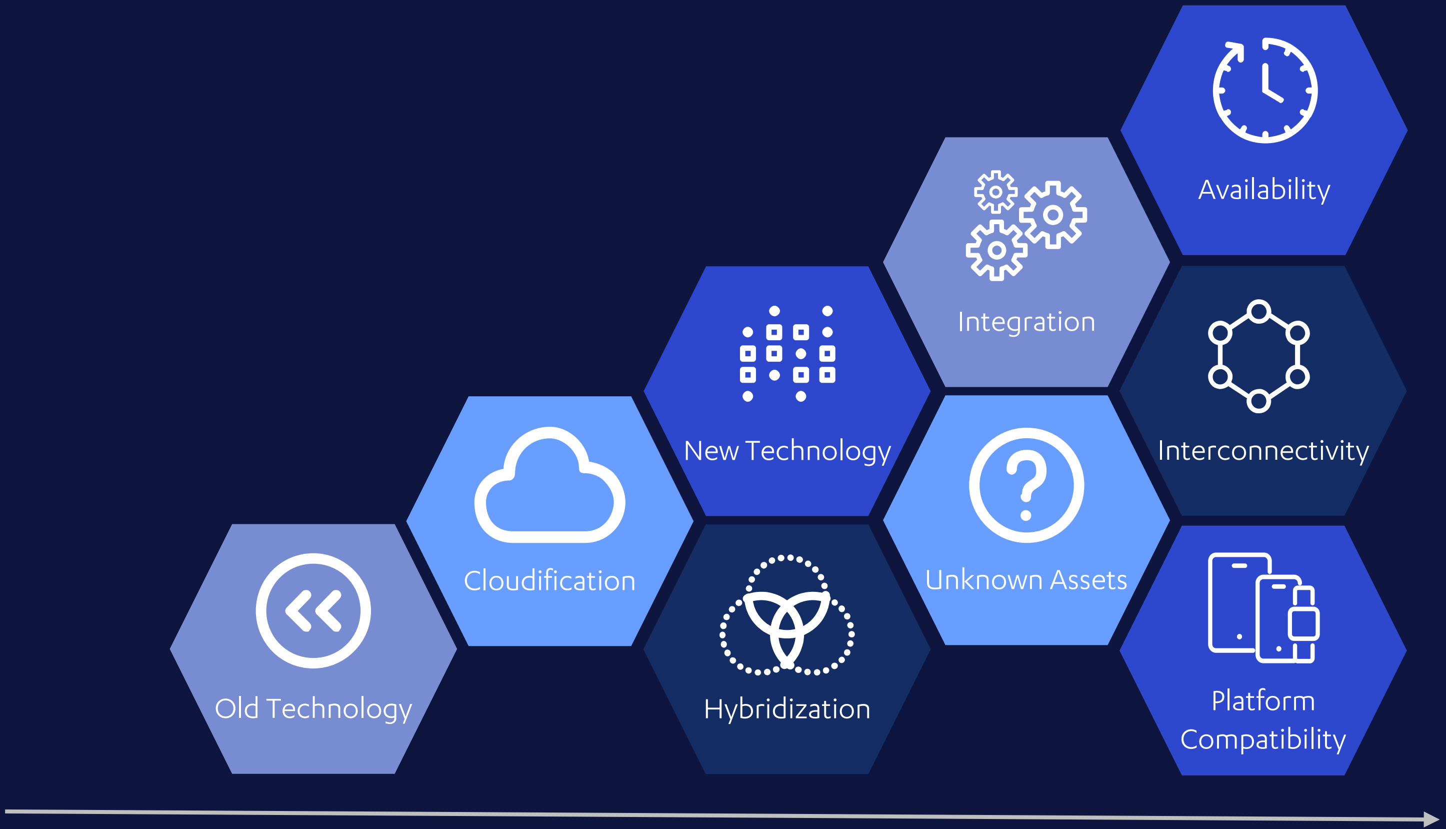
Accelerating the Transition to Outcome-Based Security

Christine Bejerasco

CTO

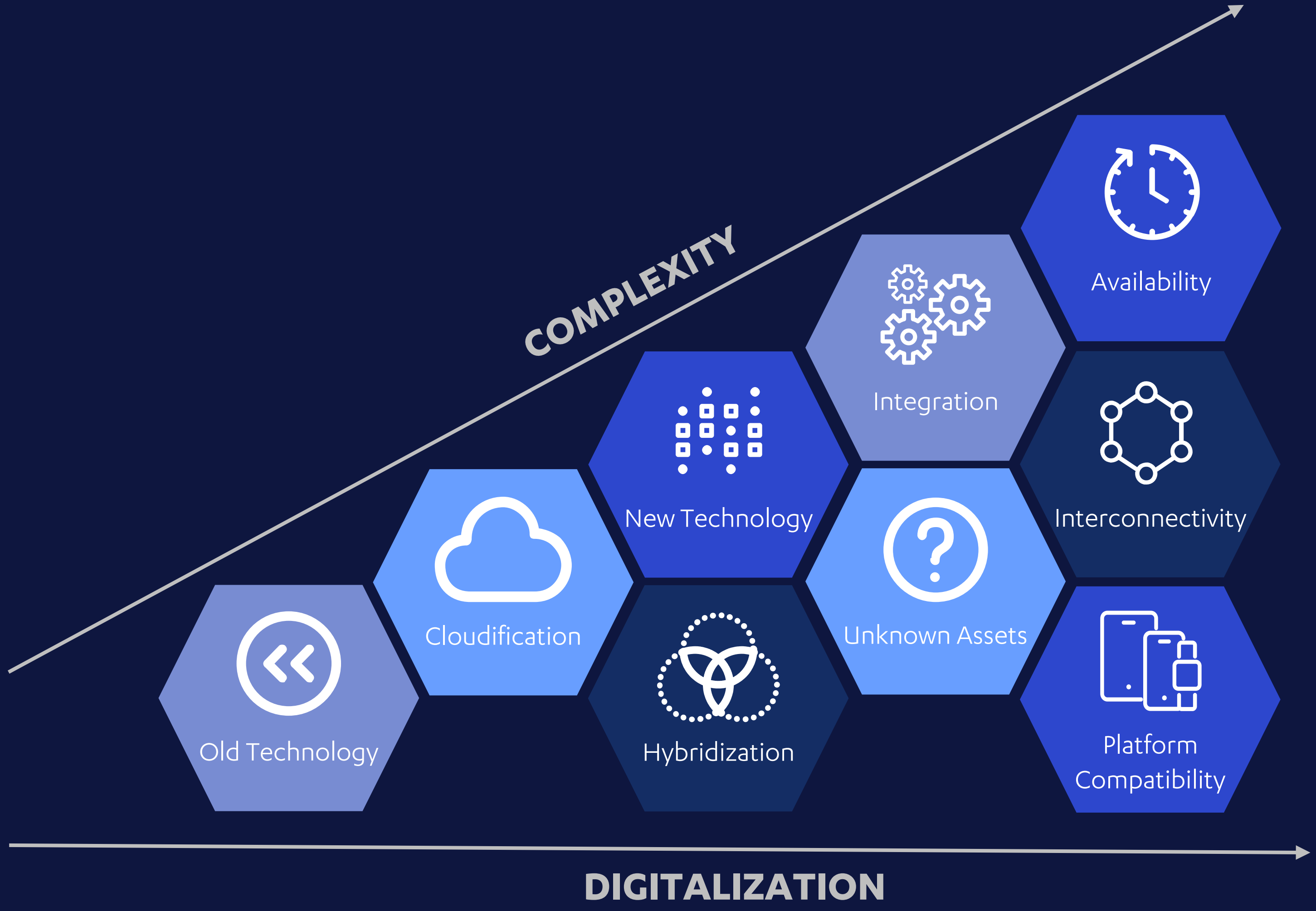
W / T H secure

Effects of Digital Transformation



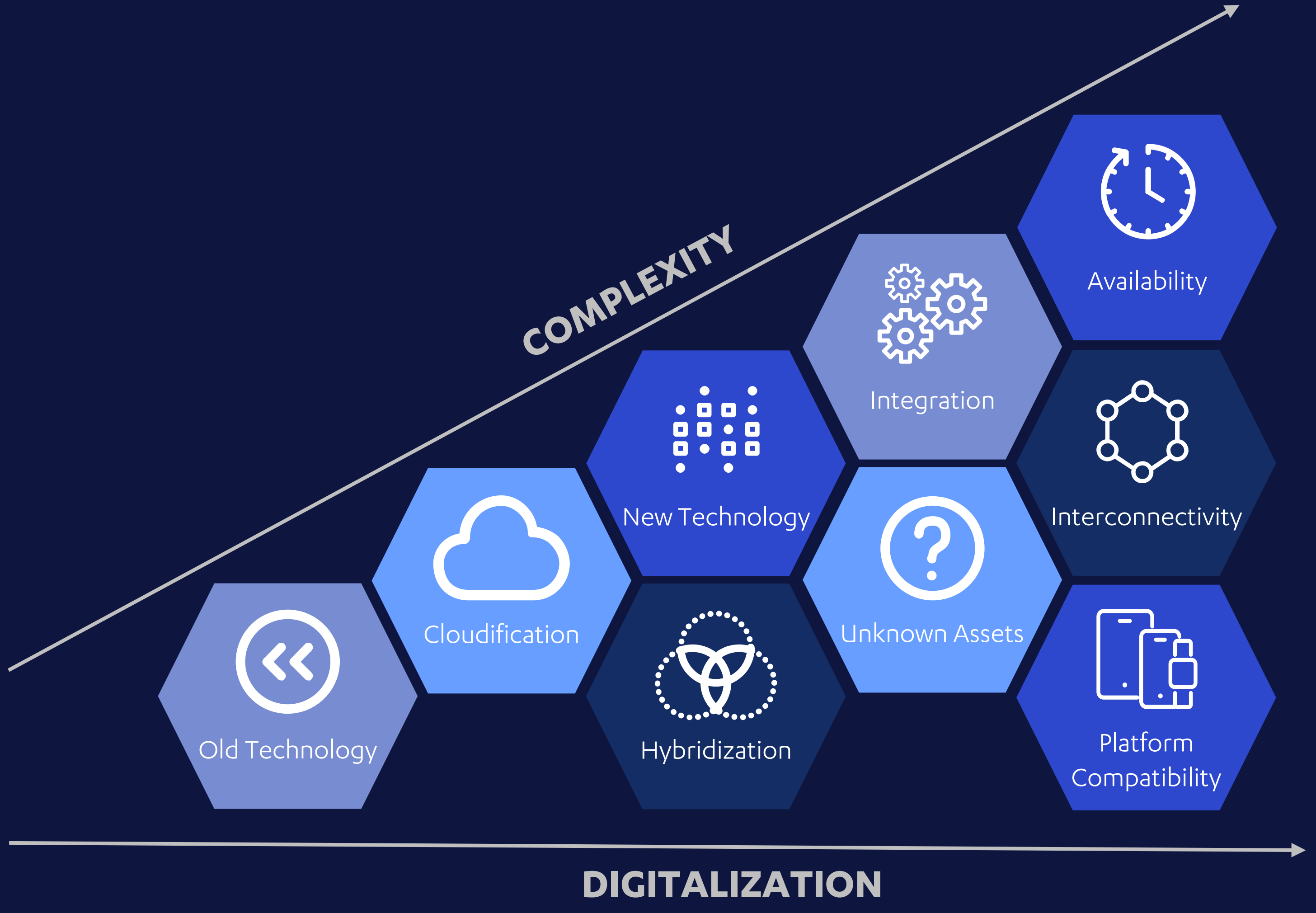
DIGITALIZATION

Effects of Digital Transformation



W/TH secure

Effects of Digital Transformation



COMPLEXITY

Old Technology

Cloudification

New Technology

Hybridization

Integration

Unknown Assets

Availability

Interconnectivity

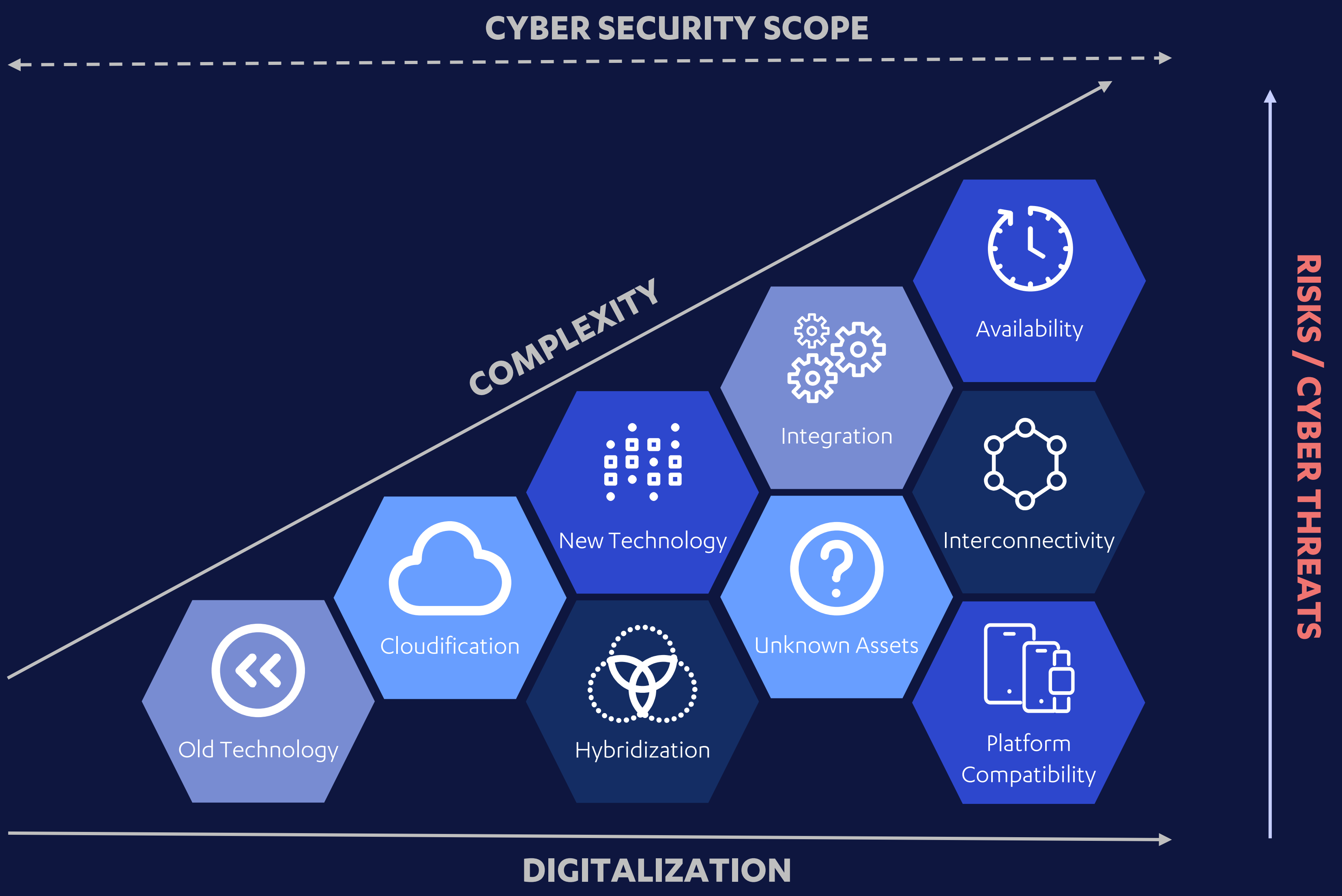
Platform Compatibility

DIGITALIZATION

RISKS / CYBER THREATS

- Hybrid Attacks
- Data Leaks
- Data Theft
- Ransomware 2.0
- Business Email Compromise
- Targeted Attacks
- DDoS
- Cryptojacking
- Commodity Threats
- Phishing
- Malicious spam

Effects of Digital Transformation



CYBER SECURITY SCOPE

COMPLEXITY

Old Technology

Cloudification

New Technology

Hybridization

Integration

Unknown Assets

Availability

Interconnectivity

Platform Compatibility

DIGITALIZATION

RISKS / CYBER THREATS

- Hybrid Attacks
- Data Leaks
- Data Theft
- Ransomware 2.0
- Business Email Compromise
- Targeted Attacks
- DDoS
- Cryptojacking
- Commodity Threats
- Phishing
- Malicious spam

Supply Chain Attacks

Noteworthy Supply Chain Attacks

2011

ESTsoft ALZip software
(Threat: Backdoor.Agent.Hza)
Computer game publisher
(Threat: Winnti)

2013

Simdisk (Threat: Castov)

2014

GOM Player (Threat: Miancha)
ICS/SCADA manufacturer sites
(Threat: Havex)

2015

League of Legends & Path of Exile
(Threat: PlugX)
EvLog (Threat: Kingslayer)
Xcode (Threat: XcodeGhost)

2016

Transmission
(Threats: OSX Keranger & OSX Keydnap)
MSP (Threat: CloudHopper)
Linux Mint (Threat: backdoor)
FossHub (Threat: MBR writer)
Ask Partner Network
(Threat: banking trojans)

2017

M.E.doc (Threat: NotPetya)
UltraEdit (Threat: WilySupply)
HandBrake (Threat: OSX Proton)
Leagoo (Threat: Android Triada)
NetSarang (Threat: ShadowPad)
CCleaner (Threat: Floxif)
PyPI repository (Threat: typosquatting)
Elmedia Player (Threat: OSX Proton)
IBM Storwize (Threat: Reconyc)
WordPress repository (Threat: backdoors)

2018

MediaGet (Threat: Dofoil)
MEGA Chrome extension
(Threat: cryptocurrency stealer)
Magecart attacks
PDF Editor application
(Threat: cryptominer)
Remote support solutions provider
(Threat: 9002 RAT)
Webmin (Threat: backdoor)
event-stream npm package
(Threat: cryptocurrency stealer)
Docker Hub (Threat: cryptominer)

2019

Asus live update
(Threat: ShadowHammer)
DoorDash
(Threat: unauthorized access
to user data)

2020

Github (Threat: Octopus Scanner)
RubyGems (Threat: cryptocurrency stealers)
Able Desktop (Threat: backdoors)
VGCA (Threat: PhantomNet)
Websites that support WIZVERA VeraPort
(Threat: Lazarus)
Noxplayer (Threat: backdoors)
Solarwinds (Threats: Sunspot, Sunburst, Teardrop)

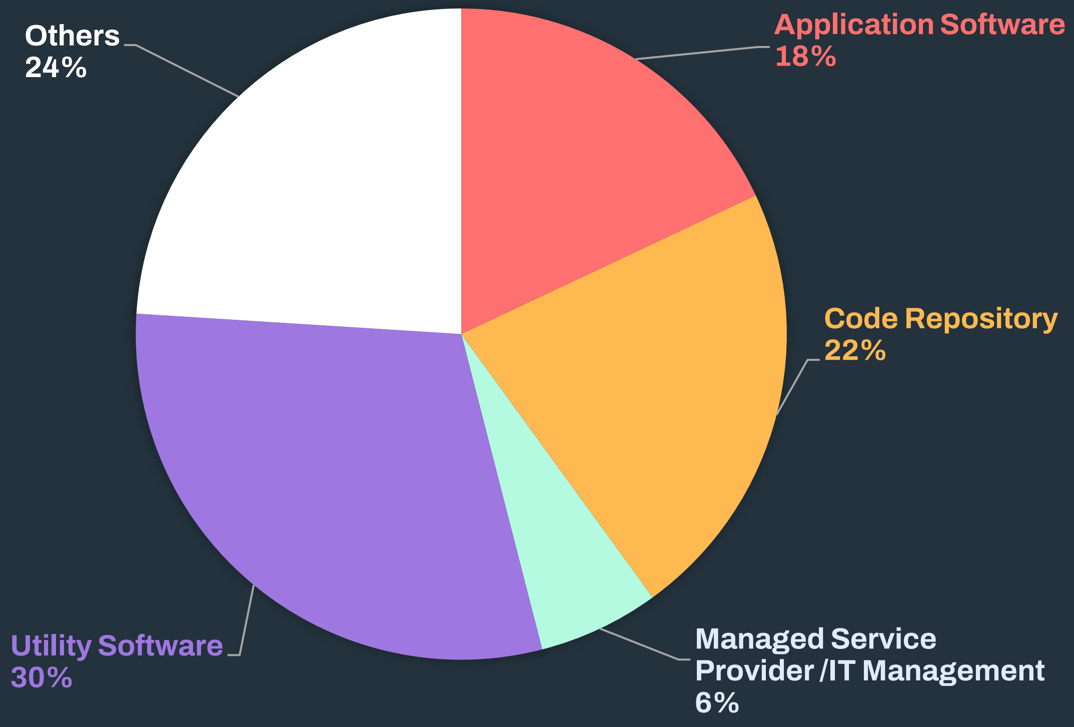
2021

NPM Packages (several)
PyPI (Threat: dependency confusion)
Codecov (Threat: backdoor)
Kaseya VSA (Threat: Revil)
Xcode (Threat: XCodeSpy)
PasswordState
(Threat: infostealer)

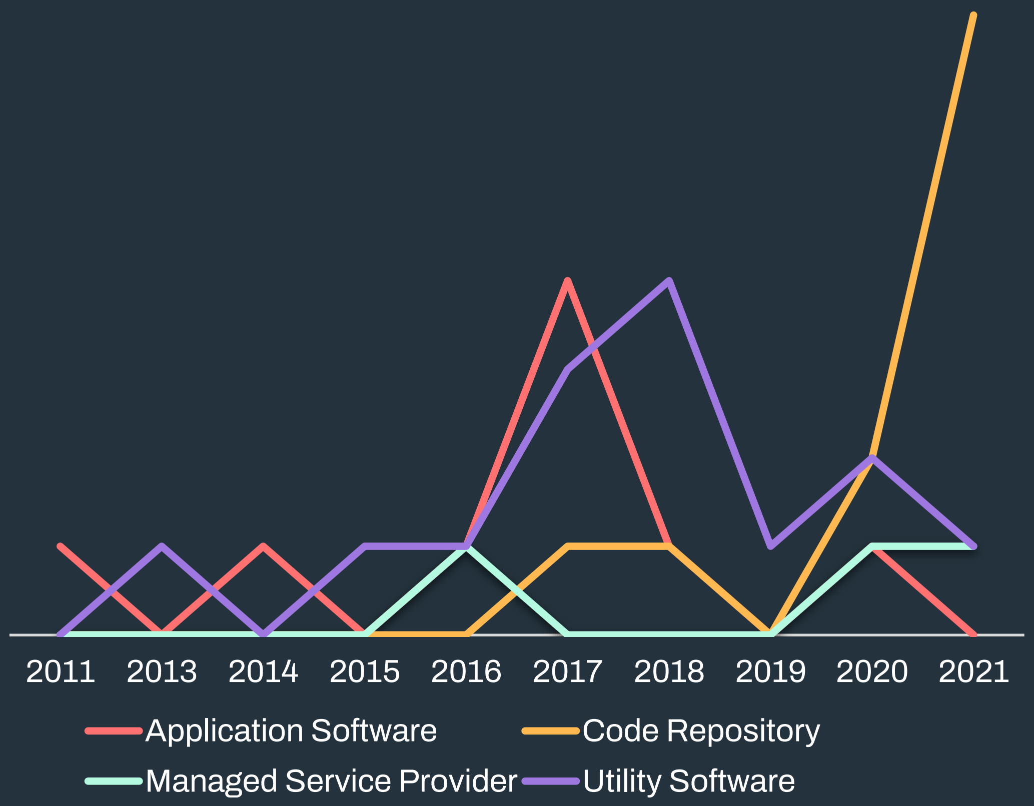
2022

AccessPress (Threat: backdoor)
NPM
PyPI

Supply Chain Attack Target Type



Supply Chain Attack Target Type by year

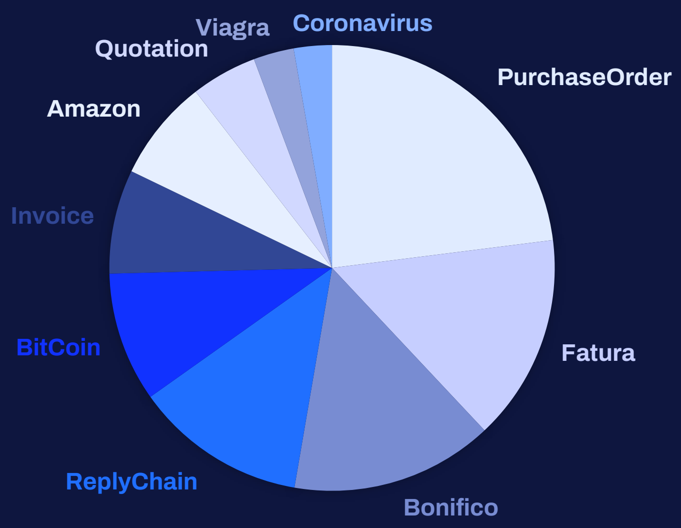


Email-borne Attacks

General Spam & Phishing

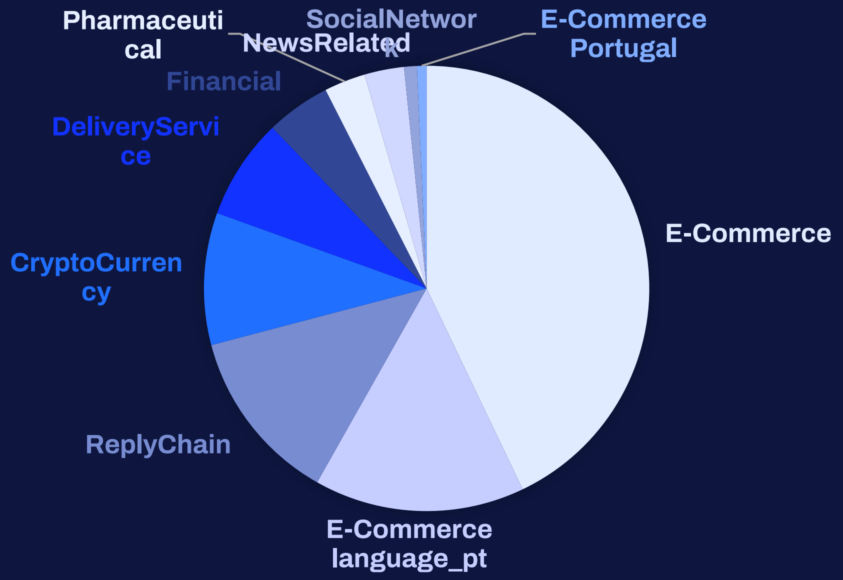
Brands & Topics

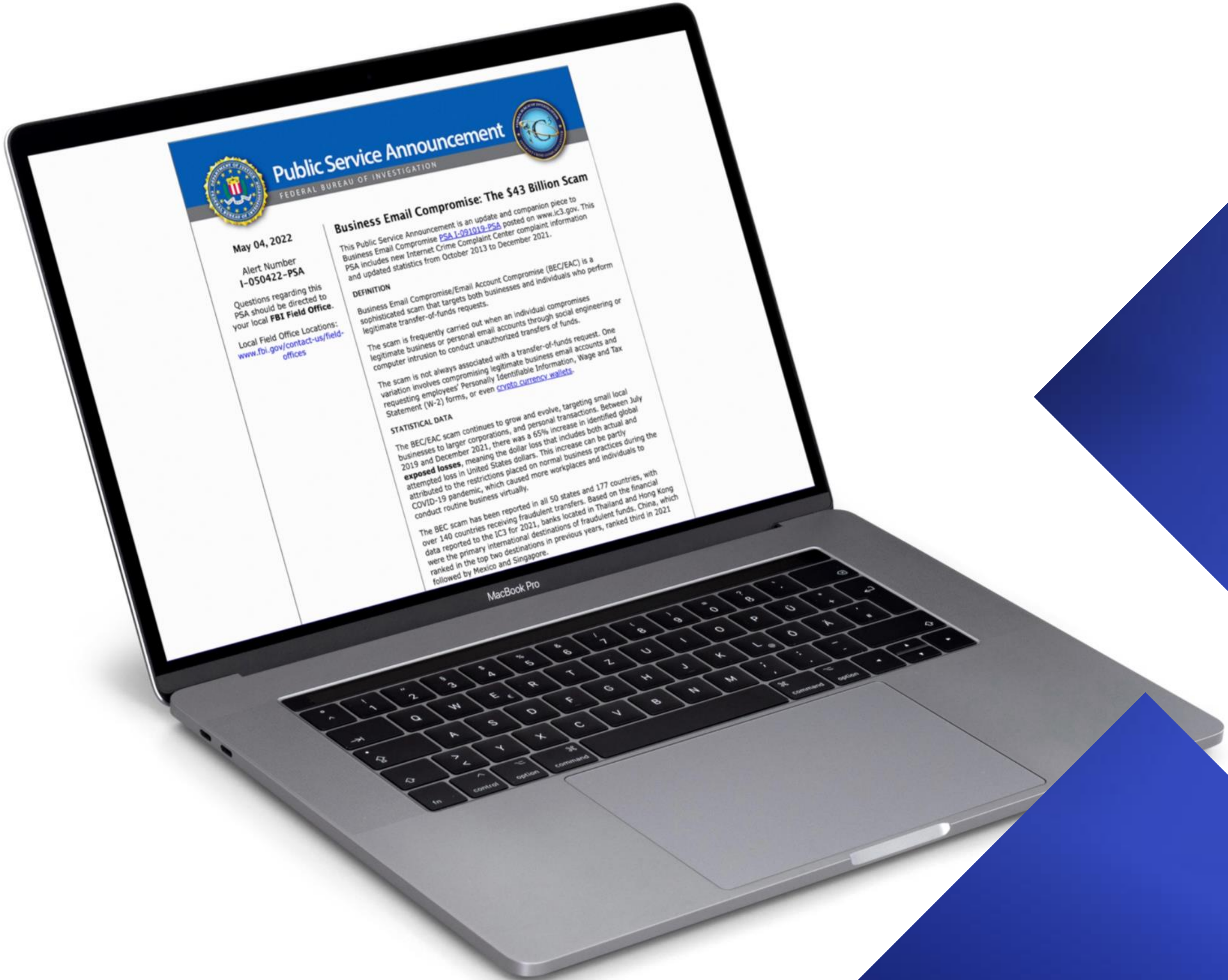
Themes, brands and topics used as part of the email body, subject lines or filename attachments.



Categories

Categories of targeted themes, brands and topics.





Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

May 04, 2022

Alert Number
I-050422-PSA

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

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

Business Email Compromise: The $43 Billion Scam

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA I-091019-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to December 2021.

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 scam is frequently carried out when an individual compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds.

The scam is not always associated with a transfer-of-funds request. One variation involves compromising legitimate business email accounts and requesting employees' Personally Identifiable Information, Wage and Tax Statement (W-2) forms, or even crypto currency wallets.

STATISTICAL DATA

The BEC/EAC scam continues to grow and evolve, targeting small local businesses to larger corporations, and personal transactions. Between July 2019 and December 2021, there was a 65% increase in identified global **exposed losses**, meaning the dollar loss that includes both actual and attempted loss in United States dollars. This increase can be partly attributed to the restrictions placed on normal business practices during the COVID-19 pandemic, which caused more workplaces and individuals to conduct routine business virtually.

The BEC scam has been reported in all 50 states and 177 countries, with over 140 countries receiving fraudulent transfers. Based on the financial data reported to the IC3 for 2021, banks located in Thailand and Hong Kong were the primary international destinations of fraudulent funds. China, which ranked in the top two destinations in previous years, ranked third in 2021 followed by Mexico and Singapore.

Cloud and Server Vulnerabilities

Threat Modelling

How can your application be misused?

Peer Review

More eyeballs can catch more bugs.

Security Awareness Trainings

Phishing, MFA Fatigue Attacks and general cybersecurity hygiene.

Shift Left

Developers are responsible for their code security.

Bug Bounty Programs

Incentivize security researchers to report vulnerabilities of your software.

Multi-Layered Protection Capabilities

If one capability fails, another layer can pick up the slack.

SAST, DAST & SCA

Perform due diligence on the safeness of your code before it goes to production.

EASM

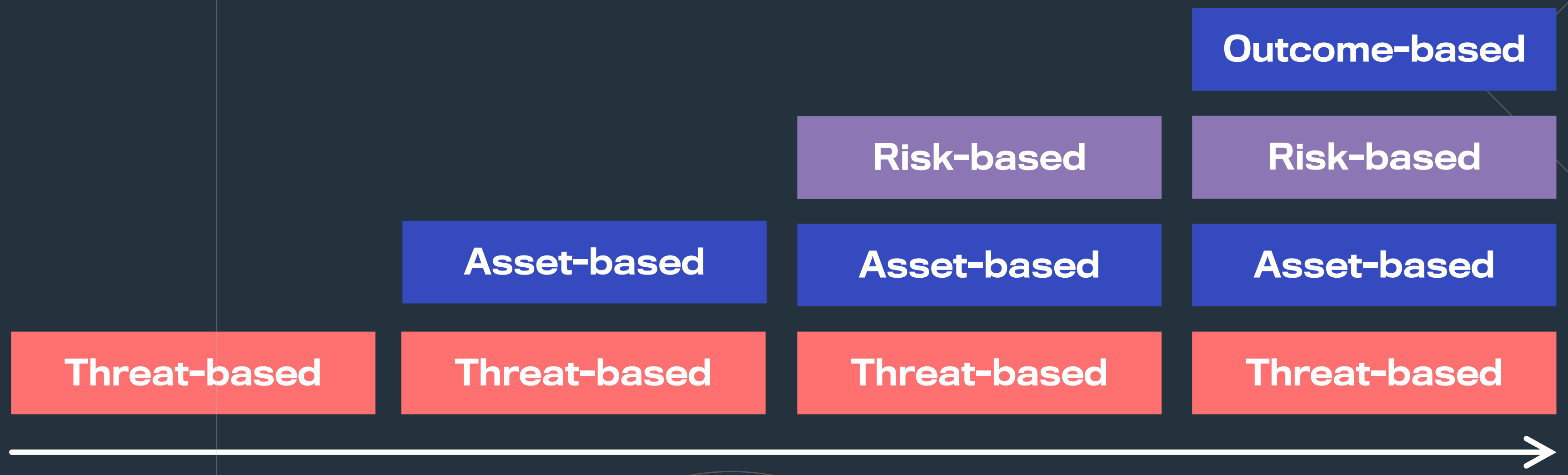
External Attack Surface Management (EASM) helps to understand and monitor the changes in your external attack surface and minimize them where you can.

MFA

Raise the bar for credential compromise

Outcome-based security:

A paradigm shift towards a “Yes, and...” mentality



Threat-based

Asset-based

Threat-based

Risk-based

Asset-based

Threat-based

Outcome-based

Risk-based

Asset-based

Threat-based

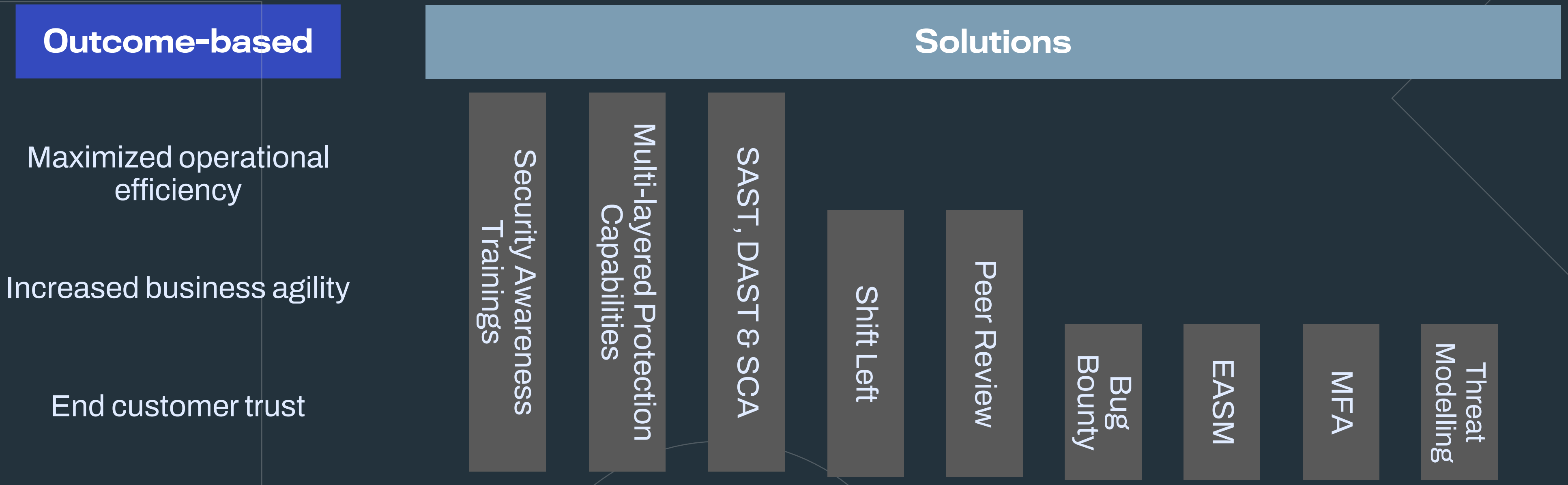
Outcome-based security:

A paradigm shift towards a “Yes, and…” mentality

Outcome-based	Risk-based	Asset-based	Threat-based
Maximized operational efficiency	Cloud autoscaling causes high opex	Webserver in Azure	Cryptominers
Increased business agility	Customer data in insecure SaaS provider	Customer PII in SaaS provider’s estate	Exposure via data breach
End customer trust	Introduction of malware to customer’s estate	Applications	Supply Chain Attacks

Outcome-based security:

A paradigm shift towards a “Yes, and...” mentality



Outcome-based

Maximized operational efficiency

Increased business agility

End customer trust

Solutions

Security Awareness Trainings

Multi-layered Protection Capabilities

SAST, DAST & SCA

Shift Left

Peer Review

Bug Bounty

EASM

MFA

Threat Modelling

Cyber security as an enabler of business outcomes.

WITH®

secure