

VMware Security

La catena di sicurezza in un attacco hacker

Stefania Iannelli – Mattia Spagnoli

Solution Engineers – Networking & Security

25/5/2022



Agenda

Context, motivations and strategies of the cyber attacks

Let's analyze a typical cyber attack

Defense in depth with VMware Security


Modernize SOC with VMware XDR

Context, motivations and strategies of the cyber attacks

What keeps CISOs up at night ?



What keeps CISOs up at night ?



“ **Malicious** are the No.1 threat keeping security leaders up at night. Even security leaders who are well equipped to handle cybersecurity risk are highly anxious.”

Source: Cybersecurityventures
Source: Clusit Report H1 2021

Cybercrime will cost the world about \$10.5 trillion a year by 2025.*

6% GDP for Cybercrime*

Italy: 180% cyber attacks increase compared to the same period

11 Every seconds

A New Ransomware attack in 2021 (in 2015 every 2 minutes)

Cybersecurity Ventures

59%

Of All Attacks Involve Double Extortion

IBM X-Force Threat Intelligence Index (March 2021)

\$6 trillion

It will cost companies around the world to fix breaches in 2021

Cybersecurity Ventures

77%

Use RDP with either valid accounts or brute-forced credentials to move laterally within networks

2020 VMware Threat Landscape Report (May 2021)



Cybersecurity Ventures (2022)

Ransomware Damages

\$265 bilion expected by 2031

\$20 bilion 2021

\$11.5 bilion 2019

\$325 million 2015

2021: 57X
more than
2015 !

Cybersecurity Ventures (2022)

Cyber Threat Landscape

Actors and Motivations



Cyber Crime

Motivated, for
the most part,
by financial
gain

Cyber
Espionage

Motivated by stealing
trade secrets,
intellectual property,
and confidential
government
information.

Hactivism
and Cyber
Terrorism

Intimidation/
ideological,
political, religious,
or patriotic
reasons

Cyber
Warfare

The use
of cyber
attacks against
an enemy state

These motivations are not mutually exclusive

January - May 2022

<https://konbriefing.com/index-en.html>

ENERGIEVERSORGUNG

Cyberangriff legt Oiltanking-Tanklager deutschlandweit vollständig lahm – Tankwagen-Beladung außer Acht gelassen

Zwei Tochterunternehmen des Hamburger Marquard & Bahls sind Opfer von Hackern Mittelständische Tankstellen, aber auch Konz sind betroffen.

“Effect of cyber attack or Gold Bond will last for weeks,” warns expert

The group which operates terminals as well as a robotic logistics center in the port of Ashdod announced the shutdown of most of its computer systems following a cyber port did not mention a cyber operations

Wisag war Ziel eines Cyber-Angriffs

Der Bodenverkehrsdienstleister Wisag war in der vergangenen Woche Ziel eines Hacker-Angriffs. Zu großen Störungen in den Betriebsabläufen soll es nicht gekommen sein, weil Backup-System hochgefahren wurden. Dennoch arbeitet man bis jetzt an der Entstörung.

Sophisticated cyber-attack targets Red Cross Red Crescent data on 500,000 people

A sophisticated cyber security attack against computer servers hosting information held by the International Committee of the Red Cross (ICRC) was detected this week.

Tschechisches Fernsehen kämpft mit Cyber-Attacken wegen Olympiaübertragen

11.02.2022



Das öffentlich-rechtliche Tschechische Fernsehen (ČT) hat seit Freitagmorgen mit einem weiteren Cyberangriff zu kämpfen. Er legte die Webseiten des Sportkanals lahm, während dort das Eishockeyspiel Tschechien-Schweiz bei den Olympischen Winterspielen in Peking übertragen wurde. Die Sendung musste auf eine Notseite verlagert werden. Darüber informierte der Sender auf Twitter.

ÄHNLICHE ARTIKEL



Aufsichtsbehörde warnt vor Cyberangriffen auf tschechische Krankenhäuser



Hackerangriffe auf tschechische Webseiten

Cyberprzestępcy włamali się do pajęczańskiego ZOZu

Przez Redakcja 11 lutego 2022

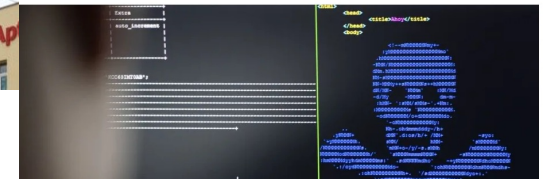


Cyberatacka auf Entsorger in MV

90

Hacker greifen Otto Dörner an und fordern Lösegeld

Von Marco Dittmer | 15.02.2022, 15:43 Uhr



Cyber-attack disrupts Slovenia's top TV station

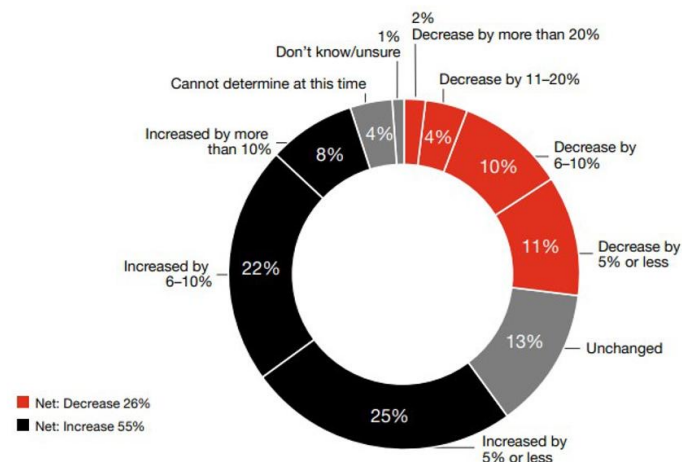
A cyber-attack has disrupted the operations of Pop TV, Slovenia's most popular TV channel, in an incident this week believed to be an extortion attempt.

The attack, which took place on Tuesday, impacted Pop TV's computer network and prevented the company from showing any computer graphics for the evening edition of 24UR, the station's daily news show.

Cybersecurity is an unfair battle

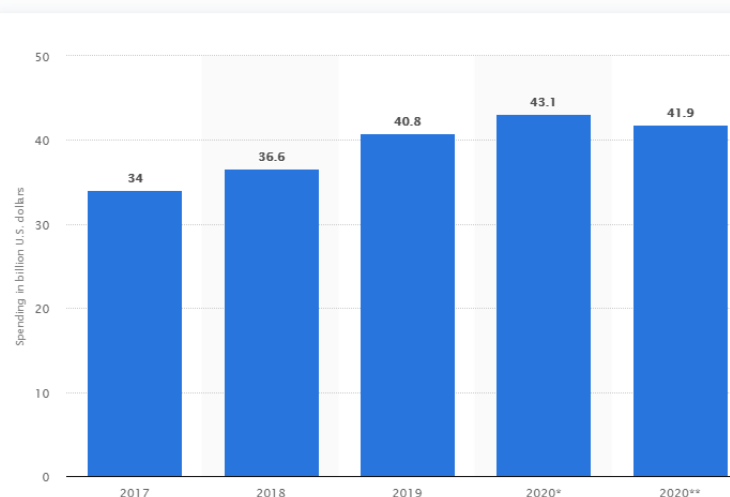
We're spending more, but are we better protected?

More are increasing cyber budgets than decreasing them in 2021

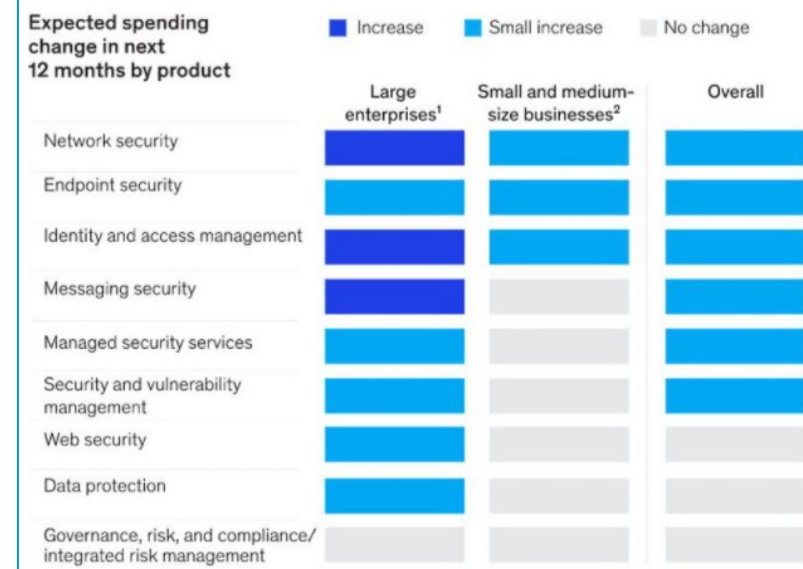


Source: PwC, Global Digital Trust Insights Survey 2021, October 2020; base 3,249
Q: How is your cyber budget changing in 2021? base 1,414

Spending on cybersecurity worldwide from 2017 to 2020
(in billion U.S. dollars)



Expected spending change in next 12 months by product



<https://www.forbes.com/sites/louiscolombus/2020/12/15/the-best-cybersecurity-predictions-for-2021-roundup/?sh=5aef426f5e8c>

PwC, Global Digital Trust Insights 2021, October 5, 2020. <https://digitalguardian.com/blog/what-does-data-breach-cost-2020>

<https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf>

<https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/>

Let's analyze a typical cyber attack

MITRE ATT&CK Matrix

Tactics and Techniques



Tactics

MITRE Tactics is the outcome the attacker wants to achieve

An attacker tactic might be to **collect** personal identifiable information.

There are currently 12 tactics identified any attacker might want to achieve.



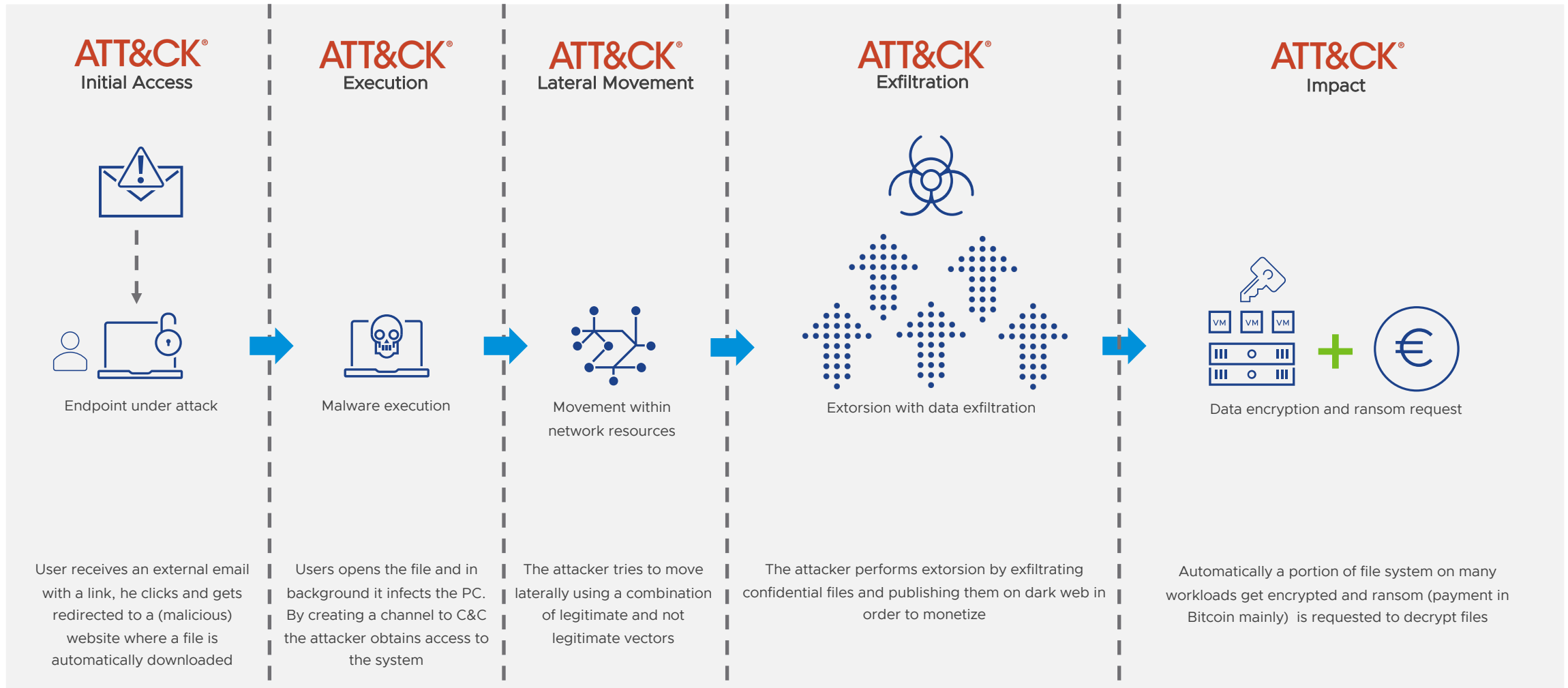
Techniques

MITRE Techniques are a series of steps used to achieve one or more of the 12 identified tactics.

There are techniques an attacker can carry out to achieve the collection of personal identifiable information.

There are currently 314 techniques identified that help achieve the 12 tactics.

Tactics of the Attacker



Demo

Defense in depth with VMware Security



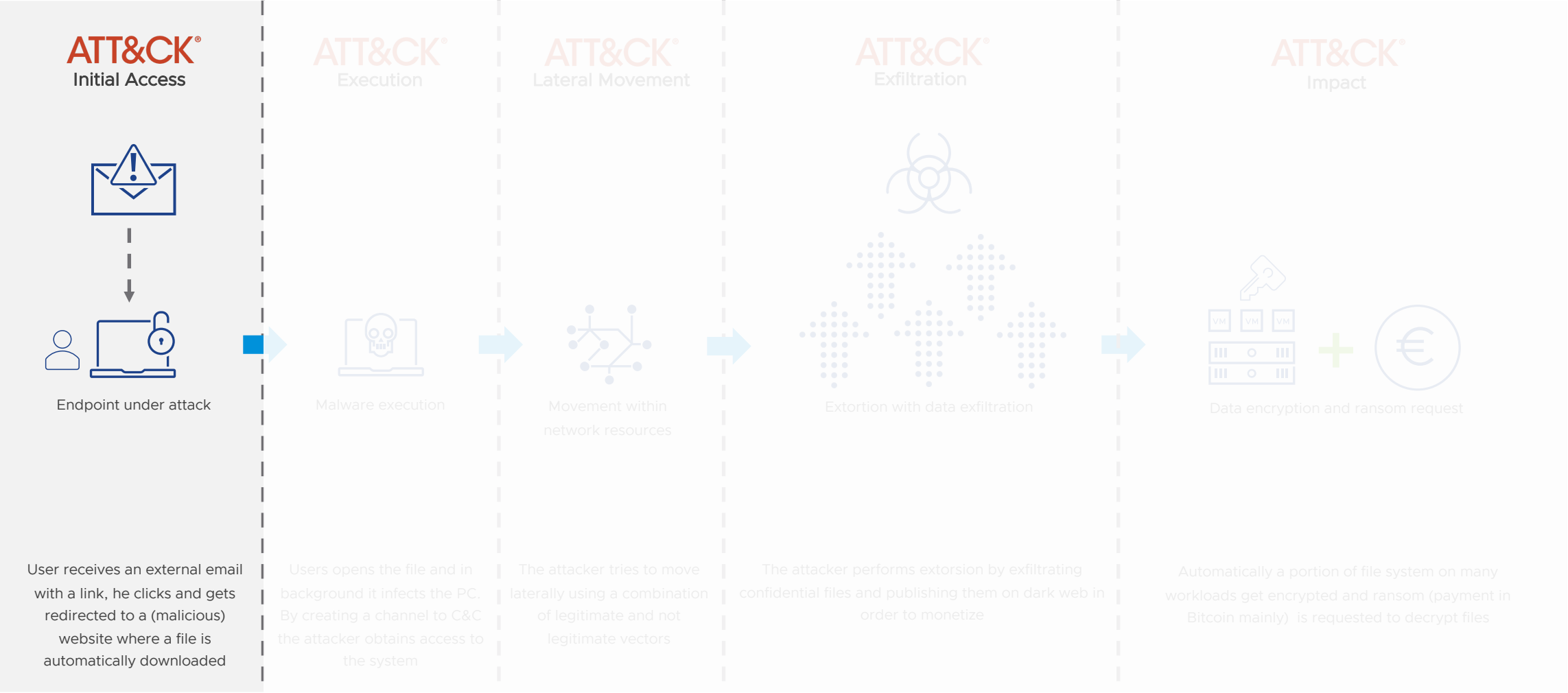
4% business email
contained malicious
components²

1 Source: IBM X-Force Threat Intelligence Index 2021

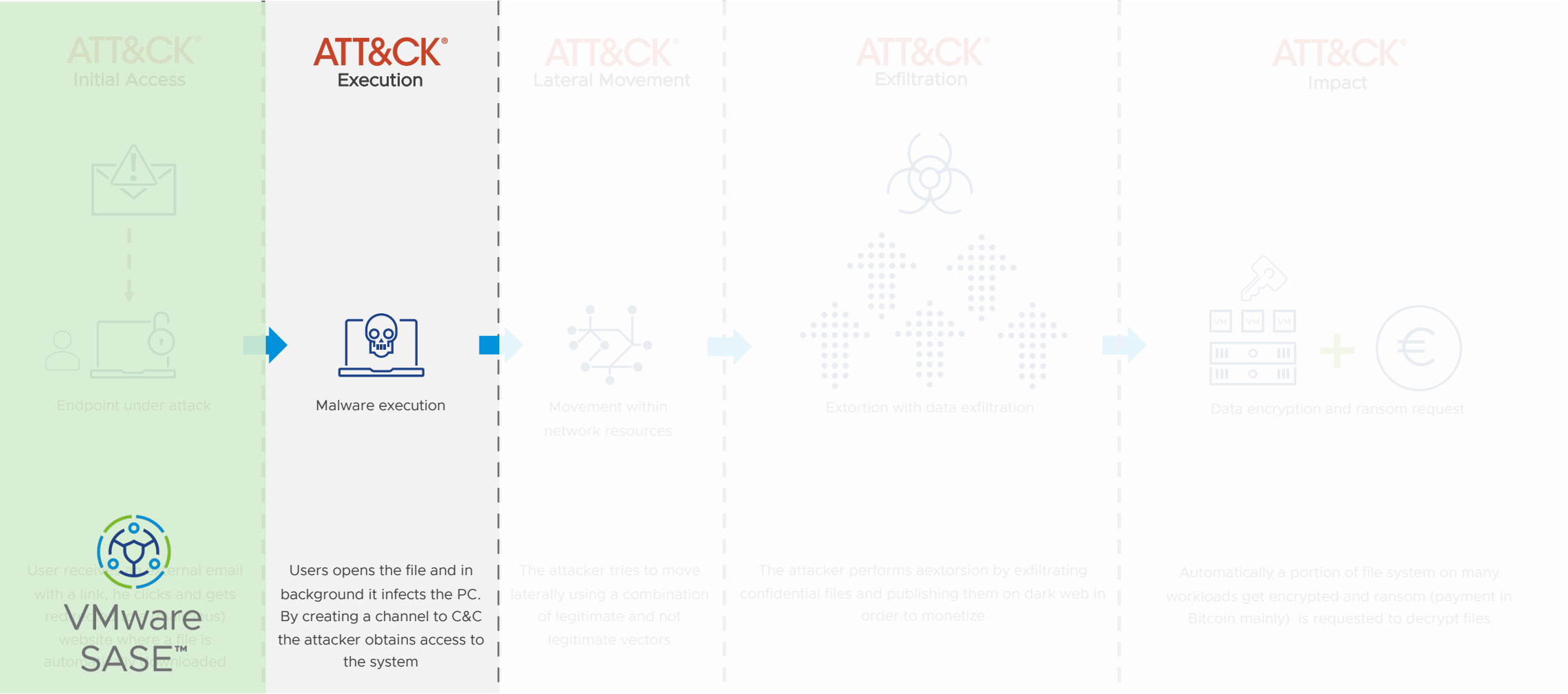
2 Source: VMware Threat Landscape Report 2021

HUMAN ERROR

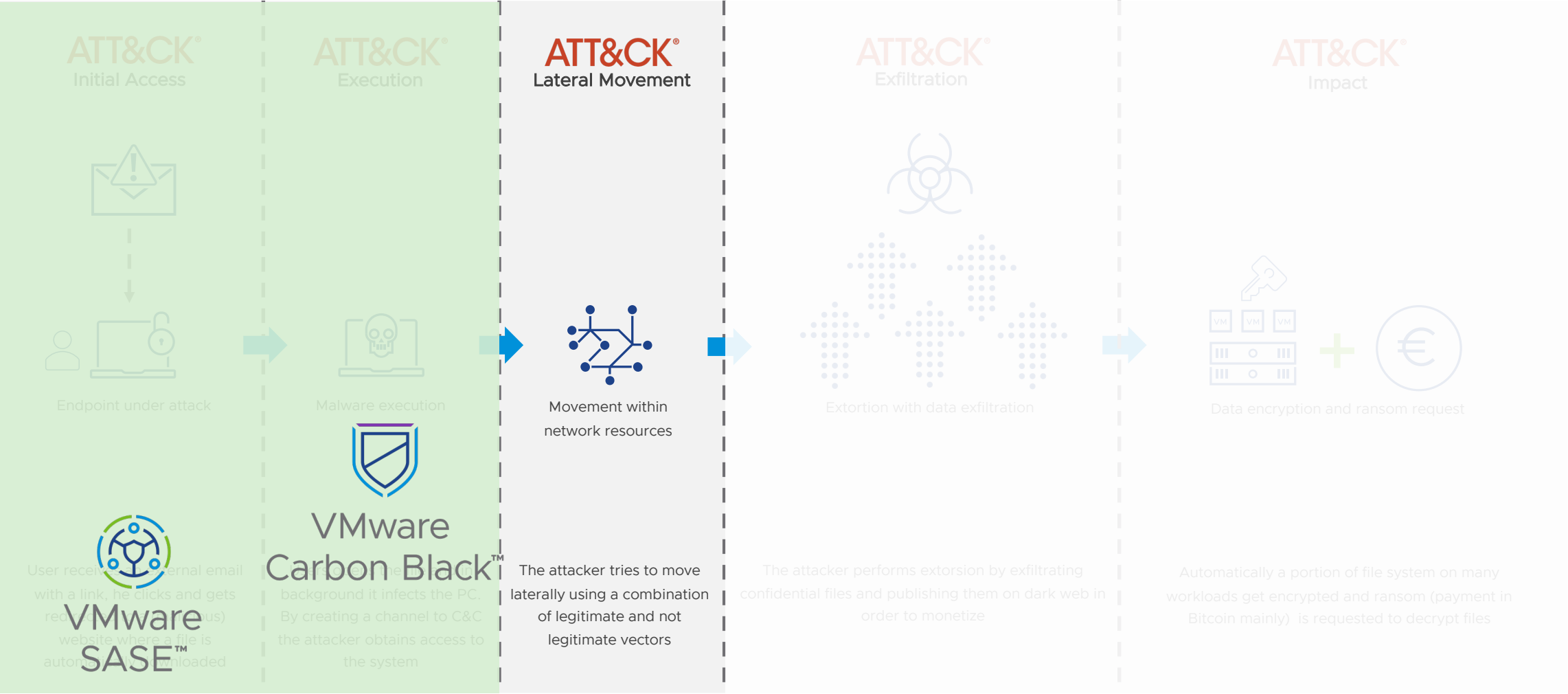
Defense in Depth with VMware



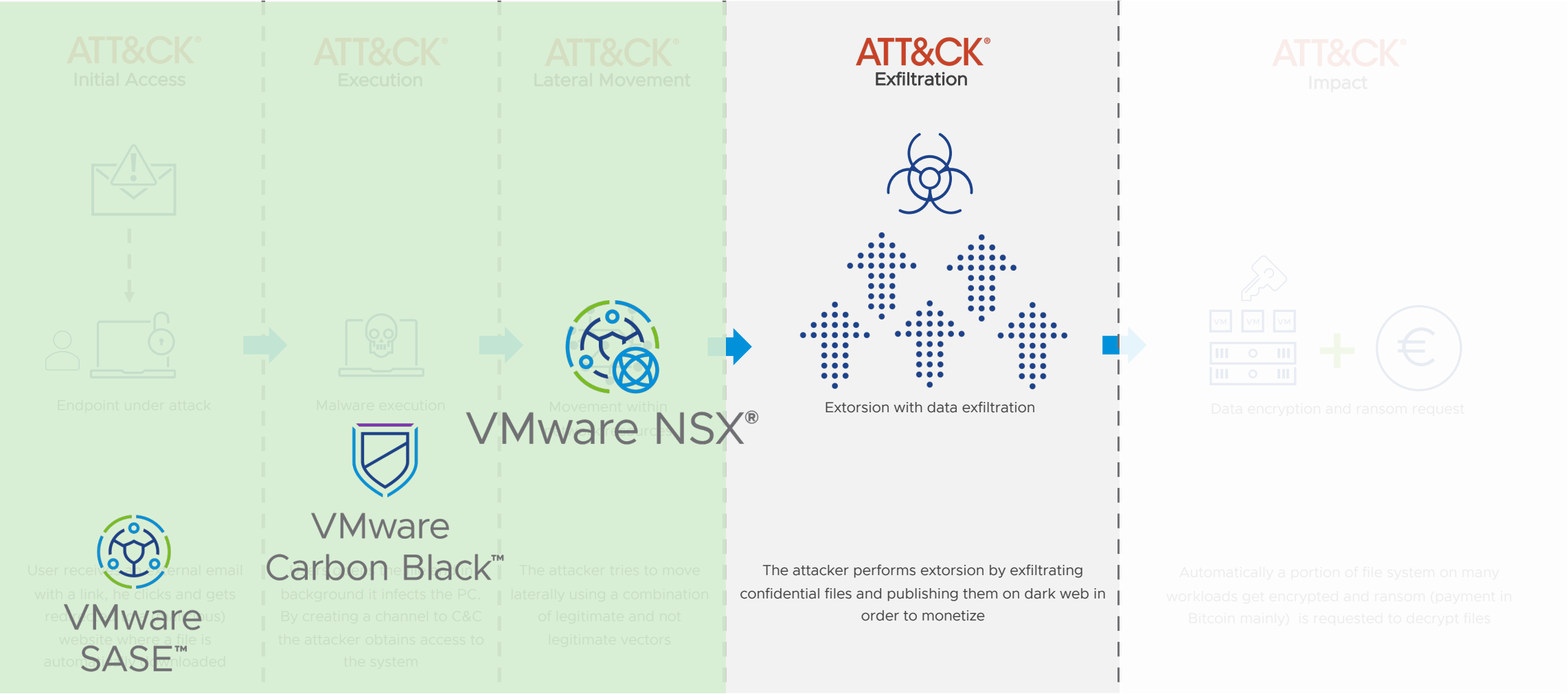
Defense in Depth with VMware



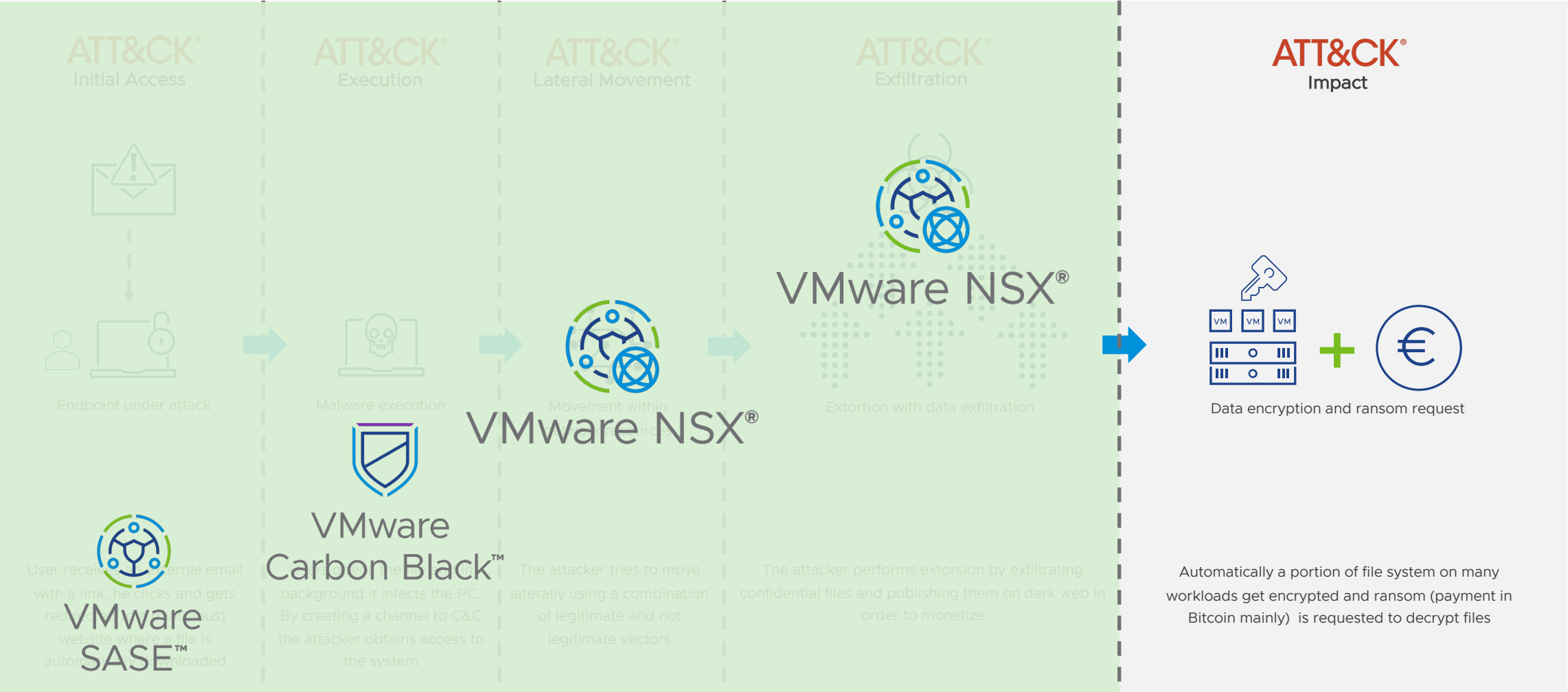
Defense in Depth with VMware



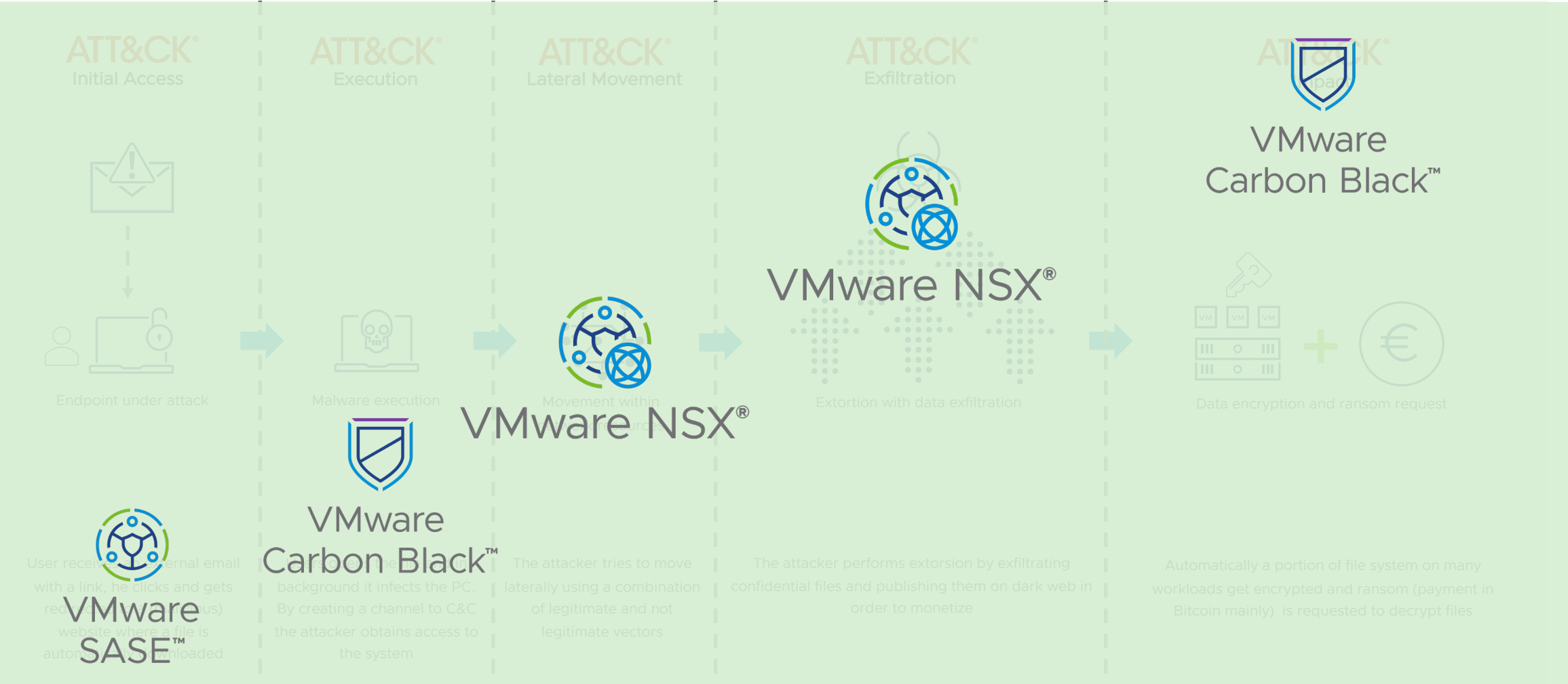
Defense in Depth with VMware







Defense in Depth with VMware



Defense in Depth with VMware



Innovations Securing the Host + Network = Win!

	Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	Command and control	Exfiltration	Impact
 VMware Carbon Black	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
 NSX Advanced Threat Protection	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
   VMware Carbon Black + NSX Advanced Threat Protection	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>

SE Labs Breach Response Detection Test

VMware NSX Network Detection and Response

August 2021

RATINGS



Total Rating **100%**

Detection Accuracy **100%**

Legitimate Accuracy **100%**

LEGITIMATE ACCURACY

False Positives **0%**

THREAT RESPONSE DETAILS

Threat	Target	Score	Overall Score
FIN7 & Carbanak		100%	100%
OilRig		100%	
APT3		100%	
APT29		100%	

This is a summary of the full test report available selabs.uk/vmware.

Detection scores represent the product's behaviour when encountering network-specific threat techniques.

SE Labs helps advance the effectiveness of computer security through innovative, detailed and intelligence-led testing, run with Integrity. We support businesses that are researching, buying and deploying security solutions. We are able to test a wide range of products and services using cutting edge testing methodologies that lead the security testing industry. SE Labs focusses on achieving detailed results, integrity in the testing process, useful threat intelligence and test innovation.

Licensed for republication by VMware, Inc.

© 2021 SE Labs Ltd

Critical Preventions in 100% of the Cases Tested

VMware Delivers Comprehensive Endpoint & Network Visibility in Latest MITRE Engenuity ATT&CK® Evaluation

March 31, 2022



MITRE Engenuity has just released the latest round of ATT&CK® Evaluation results once again proving why VMware leads the industry in threat prevention, detection, and response across endpoints, workloads, and networks. VMware is excited to announce critical preventions in 100% of the cases tested, as well as robust coverage with correlated, high confidence alerting at each and every step of the detection testing. These results were achieved with zero configuration changes, meaning VMware's security solutions worked out of the box with no extra tuning to stop two of the most sophisticated threats out there today.

Endpoint and
Workload Protection

East-West
Security

Carbon Black
Cloud

Carbon Black
Workload

Network Detection and Response (NDR)

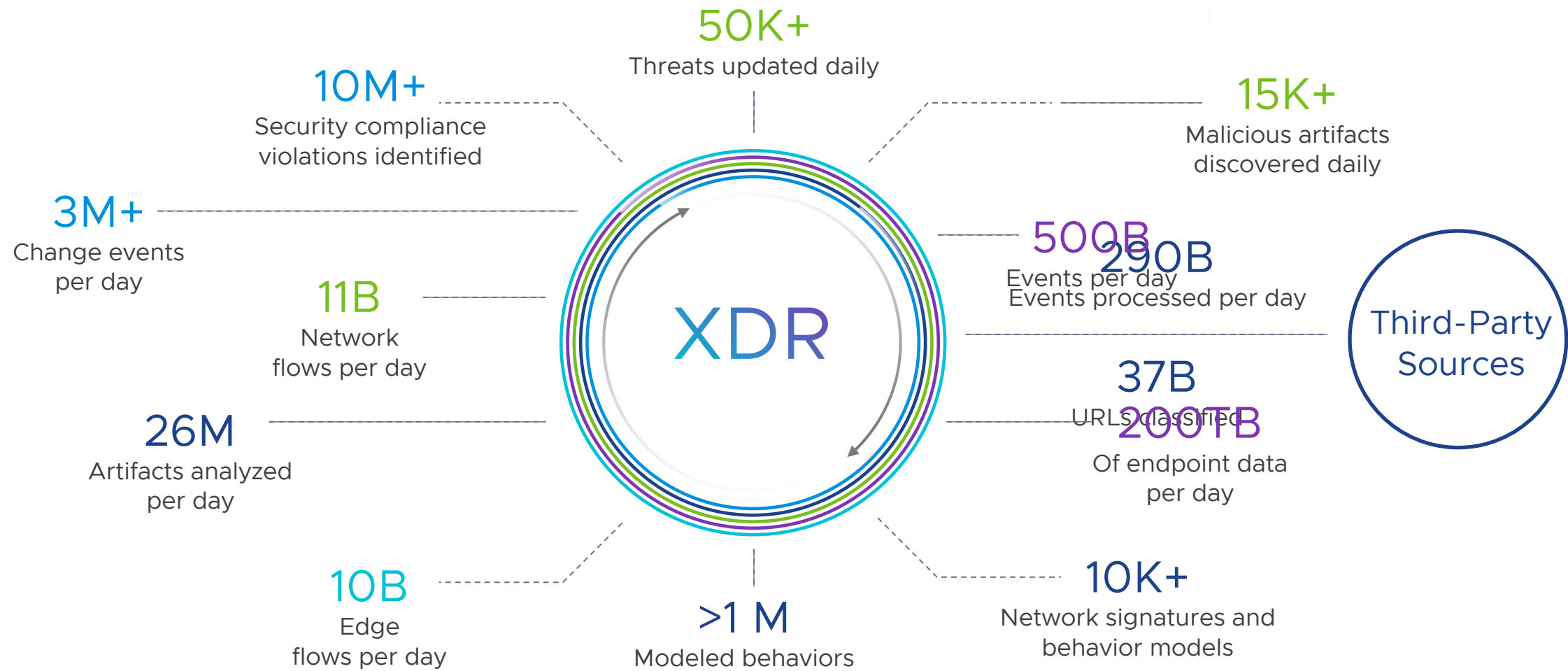
Multi-hop Network Traffic Analysis (NTA)

Network Segmentation & Micro-segmentation

Best of Breed Standalone

Better Together

Broadest and Deepest Data





Thank You