

# BUSINESS CONTINUITY OUTSIDE THE PERIMETER

EYAL ESHEL | VP LATAM

[eyal.eshel@cybereason.com](mailto:eyal.eshel@cybereason.com)

# BUSINESS CONTINUITY IN THE NEW NORMAL

**COVID-19:  
TOWARDS A NEW  
WORLD ORDER?**

## The world has changed

- Economies are under stress, some sectors are suffering more than others
- The entire workforce is disrupted, many businesses switched to 100% work from home
- The “perimeter” as we know it does not exist, home Wi-Fi is more risk, VPNs don’t scale up
- Security teams are overwhelmed, budgets are frozen
- Do you have a Business Continuity Plan (BCP) ?

## In this presentation we will cover

- What can you do immediately, with the resources you have
- What are the latest attack trends and risks that we should be aware of
- What solutions and technologies can improve business continuity in the “new normal”

**THINGS THAT YOU CAN DO.. NOW**



# “securing the enterprise when no-one works from the office”

**Identity:** Do you use strong authentication in all cases and, if you suddenly switch it on, will people be able to do the things they are supposed to do?

**Remote Access:** Consider by department what data types are accessed and what the data exposure might mean from a risk perspective.

**Endpoint Security:** The endpoint is about to become the newest, most distributed place where your corporate data exists.

**Mobile:** The post-crisis day is coming where mobile is likely to be the hottest new risk area for many businesses.



**Laptops and Desktops:** In a very real way, every employee will be working on data that is outside the perimeter

**Security Operations:** Can your employees discuss ideas, talk, chat, meet *ad-hoc*, and exchange data securely?

**Physical Security :** Remember, not all employees have a home office and personal workspace outside the office like yours.

**Business Continuity:** If tomorrow you are attacked by ransomware, Do you know what to do, what not to do, who to call?



Cloudify your physical office culture



Business continuity: Think also Internal communication, team engagement, emotional support

# PRACTICE GOOD CYBER HYGIENE

- » Having secure passwords (12-16 characters, digits, letters, caps, special characters)
- » Storing your secure password
- » Two factor authentication
- » Not use work devices for personal activities
- » Only using secure routers
- » Never use public Wi-Fi
- » Beware of smart phishing campaigns (e-mail + text)
- » Beware of free Mobile APPs and free PDF Converters, etc.

**RISKS THAT YOU SHOULD BE AWARE OF**

A black and white photograph of a sandy beach. In the foreground, several sets of footprints are visible, leading away from the viewer towards the ocean. The footprints are arranged in a line that curves slightly to the right. The sand is light-colored and shows some texture. In the background, the ocean is visible, with a dashed line indicating the water's edge. The overall scene is serene and suggests a path leading to a destination.

# Phishing, Ransomware, Brute-force Attacks



## COVIDLock Ransomware

In Costa Rica, a ransomware app called COVIDLock spread across the country in the second half of March, targeting individuals and companies. COVIDLock relied on the people's fear of the pandemic, claiming to prevent contagion by providing interactive maps of the virus' spread. Instead, the application hijacked victims' devices and demanded a ransom in the cryptocurrency bitcoin. The ransomware even tripped the alarms of

## SLOCKER, ANDROID LOCKING TROJAN

“Congratulations! Your phone is blocked! You have 20 minutes to enter the code, otherwise the phone will not turn on again ...Don't see this as an arbitrary message, it will be difficult for you 😊 Unlock password Exact time To unlock the code, call +998 998 910 312 Make 8000 paynet and get the code. (Don't ask for the code without Paynet, I won't tell you anyway)

Ransomware targets: Hospitals, school districts, state and local governments, law enforcement agencies, small businesses, large businesses, Coronavirus vaccine university research



# MOBILE- GEDDON (ALREADY HERE?)

2020

Iran Launched an App That Claimed to Diagnose Coronavirus. Instead, It Collected Location Data on Millions of People.

TrickBot App Bypasses Non-SMS Banking 2FA

CovidLock: Mobile Coronavirus Tracking App Coughs Up Ransomware

Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike

#COVID19 Drives Phishing Emails Up 667% in Under a Month

About the security content of iOS iPadOS 13.4

About Apple security updates

2019

PEGASUS SPYWARE WAS SOLD TO GOVERNMENT TO FIGHT CRIME AND TERRORISM

check m8

Android ransomware is back

146 New Vulnerabilities All Come Preinstalled on Android Phones

SIB BROTHER Iran may be spying on Brits using "weaponised" phone apps downloaded from Apple and Google's app stores, report claims

StrandHogg

iPhone warning: Apple blunder spurs new jailbreak, security threats

60% MOBILE



40%  
LAPTOPS

1/4 COMPANY OWNED  
3/4 BYOD

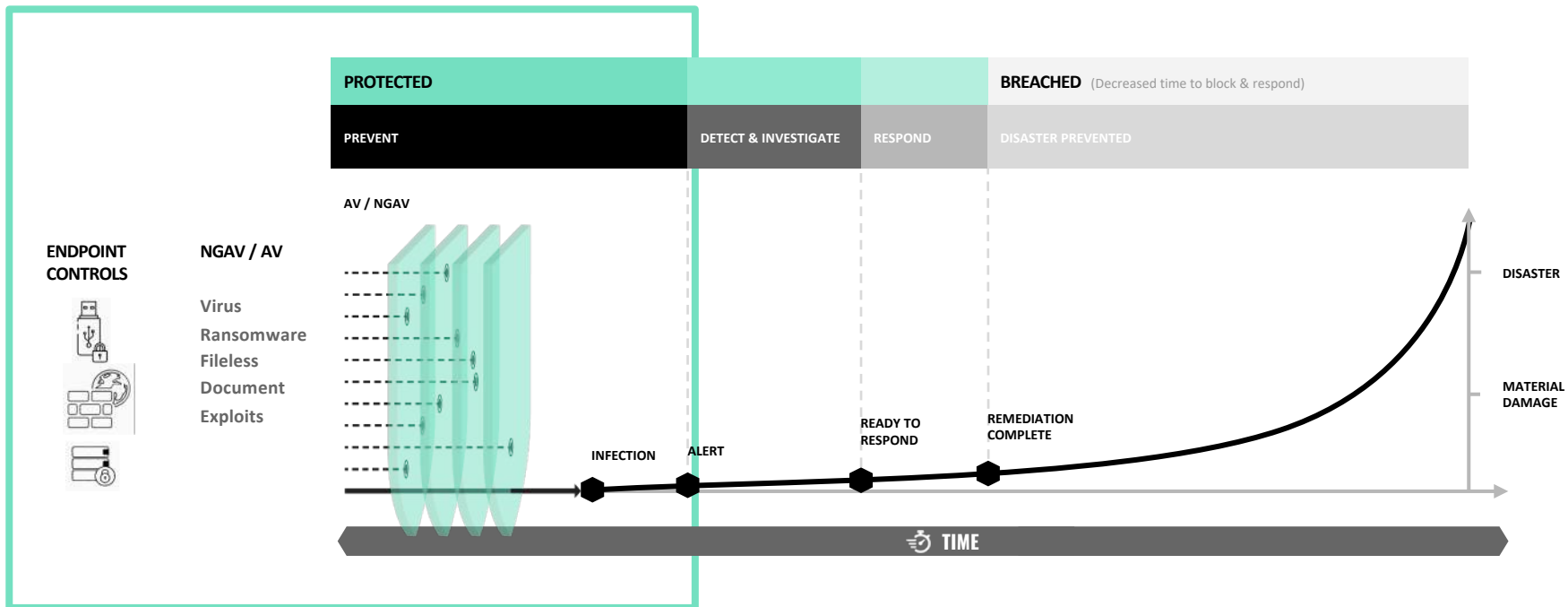
MOBILE MALWARE IS  
30% OF ALL MALWARE

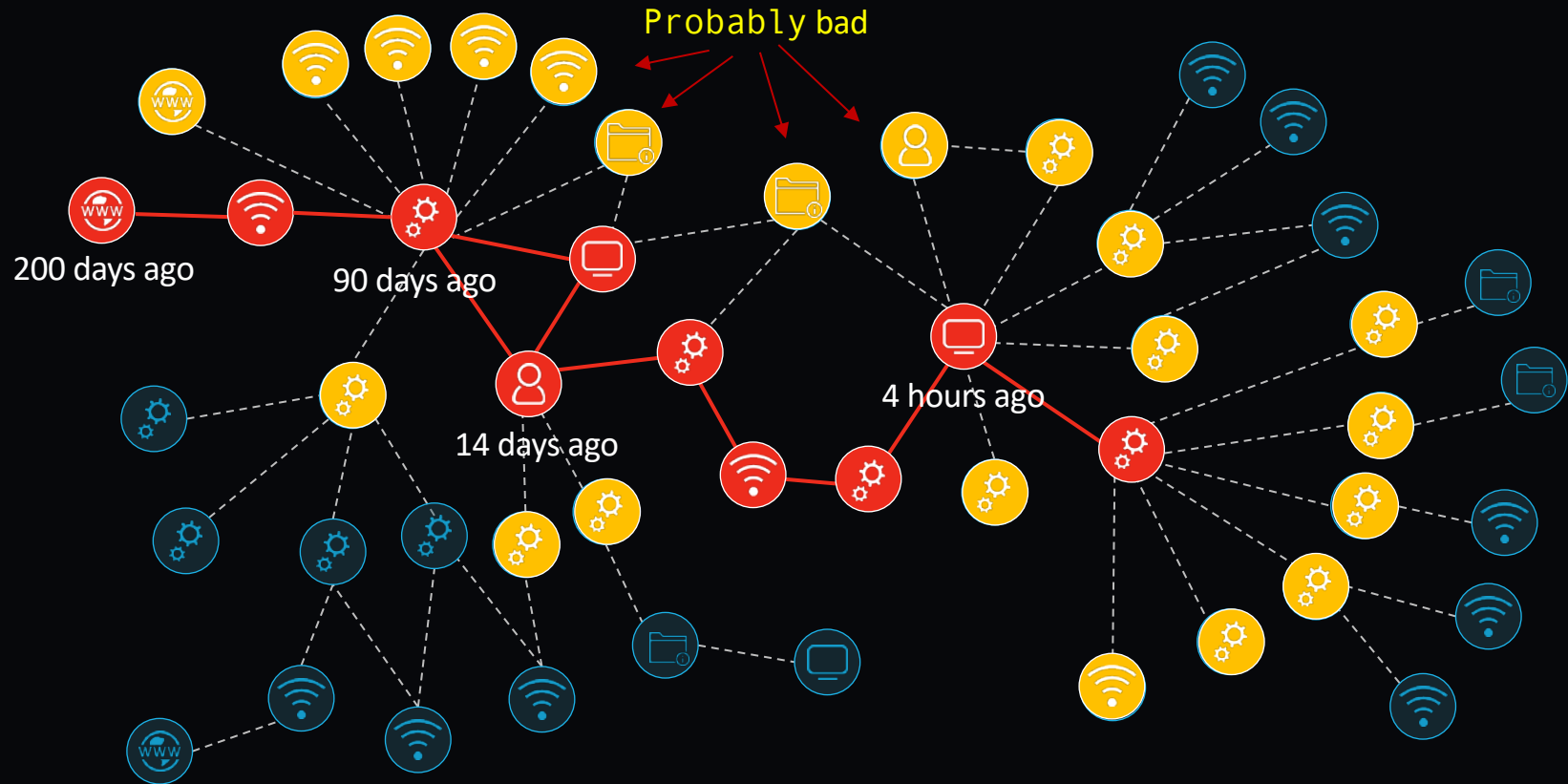
2 OUT OF 3  
EMAILS ARE OPENED ON  
A MOBILE DEVICE



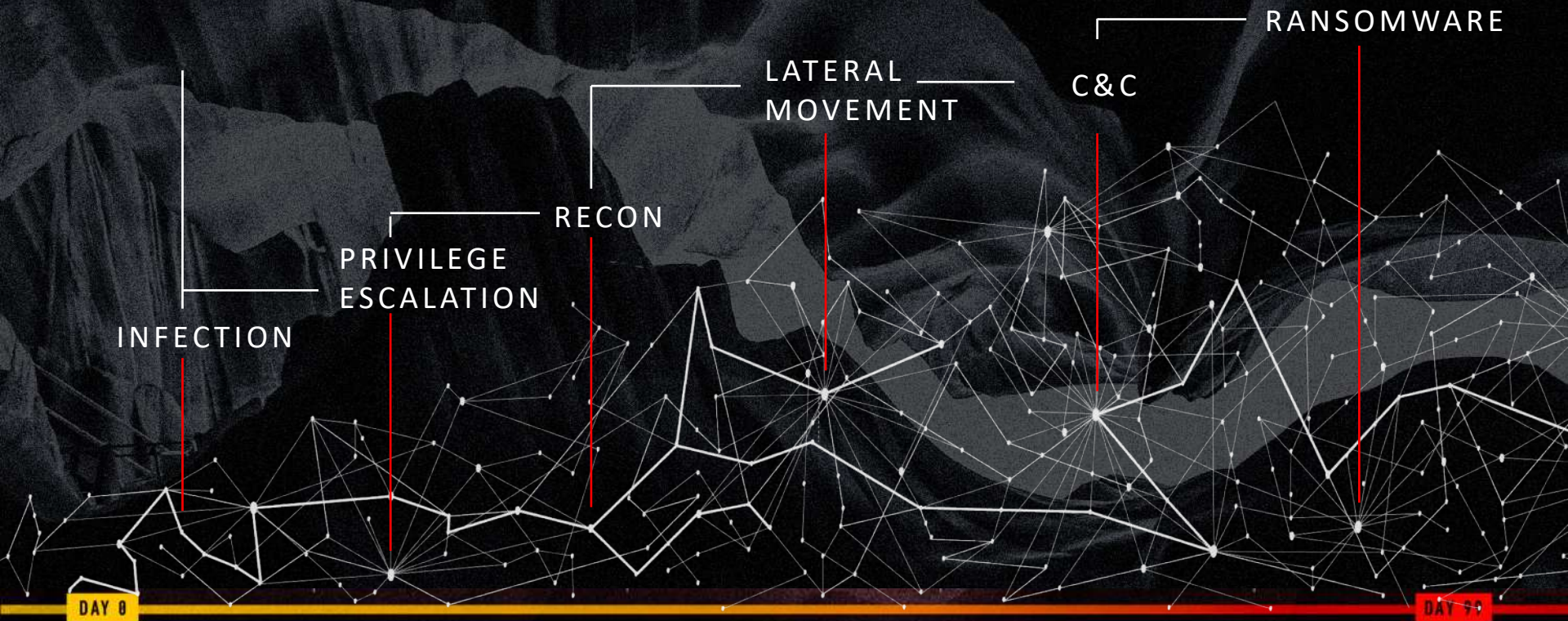
**STEPS THAT YOU CAN TAKE TO PROTECT**

# GAIN THE UPPER HAND: *MULTI-LAYERED PREVENTION*





# THE IMPORTANCE OF DEEP ATTACK SIGNALS AUTOMATED



INITIAL INFECTION



RECON // C&C



LATERAL MOVEMENT



PRIVILEGE ESCALATION



DISRUPTION & DAMAGE

# Manufacturing Under Attack → Resolved in 36H

Ransomware stands no chance vs. Cybereason



## INDUSTRY

Manufacturing

## CURRENT SOLUTIONS

EDR, AMS

## Time to Resolution

36 hours

## SIZE OF SECURITY TEAM

4 full-time staff

## NUMBER OF ENDPOINTS

18,000

## Situation

7pm Sunday | Hit by Ransomware

- “My entire server infrastructure is down we need help”
- 700+ Servers encrypted
- Breach originated in part of network not covered by Cybereason
- Attempt to contain by internal SOC failed
- AMS alerted customer and IR team

## Result

- Breach 2 Board Room with Remediation Complete in 36 hours
- Expanded Cybereason deployment to protect entire infrastructure

## Action

7am Monday

- We knew what data was exfiltrated
- Who the actors were
- Contained + TI Report

7am Tuesday

- Full Remediation Complete
- Attack Story & Timeline Sent
- Critical Infrastructure Secured
- Report shared with customer on details of the breach & necessary actions to take to protect this from happening again

# REMOTE WORKFORCE PROTECTION BUSINESS CONTINUITY

NEXT GENERATION  
ANTIVIRUS

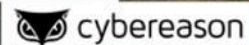
ENDPOINT DETECTION  
& RESPONSE

MANAGED DETECTION  
& RESPONSE

MOBILE  
DEFENSE

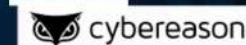
REMOTE INCIDENT  
RESPONSE

# Q&A + FREE RESOURCES



## ADDRESSING RANSOMWARE'S EVOLUTION WITH BEHAVIORAL PREVENTION

JOIN US ON MAY 20TH AT 11:00 AM  
(EDT) | 4:00 PM (BST)



## RANSOMWARE DECODED UNDERSTANDING AND PREVENTING MODERN RANSOMWARE ATTACKS

JOIN US ON JULY 8TH AT 11:00 AM  
(EDT) | 4:00 PM (BST)

[Webinars](#) [Blog](#) [Malicious Life Podcast](#)

Eyal Eshel: [eyal.eshel@cybereason.com](mailto:eyal.eshel@cybereason.com)

E-mail me for a  
Business Continuity  
Emergency Checklist

