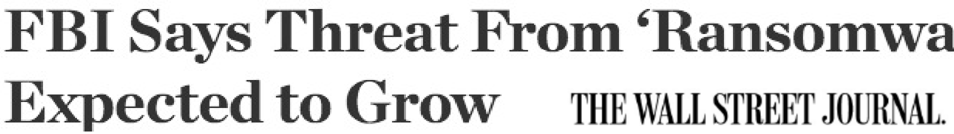
The Rise of Ransomware

Rani Hmayssi

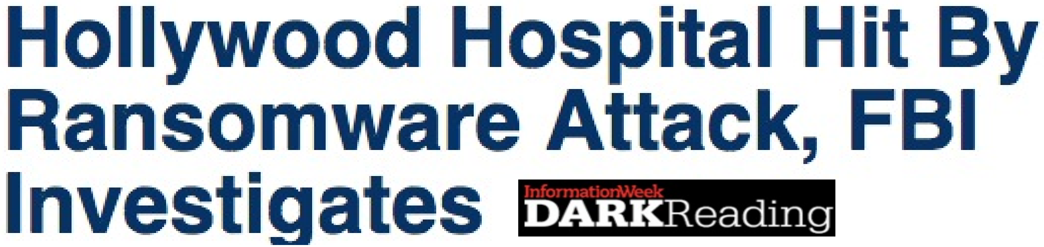
Regional Manager , Emerging markets

Cyber Security Solutions

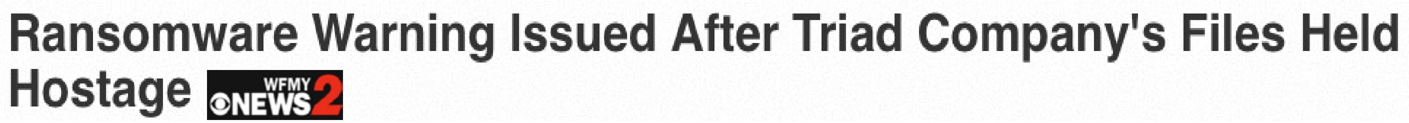
rhmayssi@paloaltonetworks.com



FBI Says Threat From 'Ransomware' Is Expected to Grow THE WALL STREET JOURNAL.



Hollywood Hospital Hit By Ransomware Attack, FBI Investigates InformationWeek DARKReading

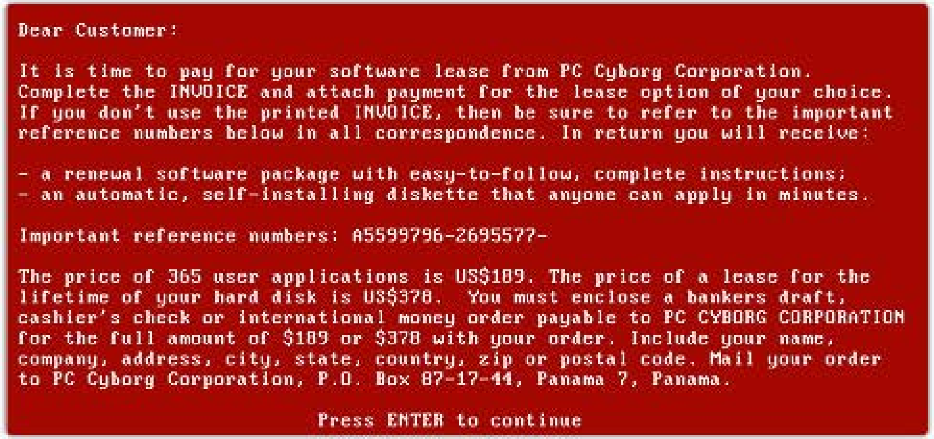


Ransomware Warning Issued After Triad Company's Files Held Hostage WFMY NEWS 2

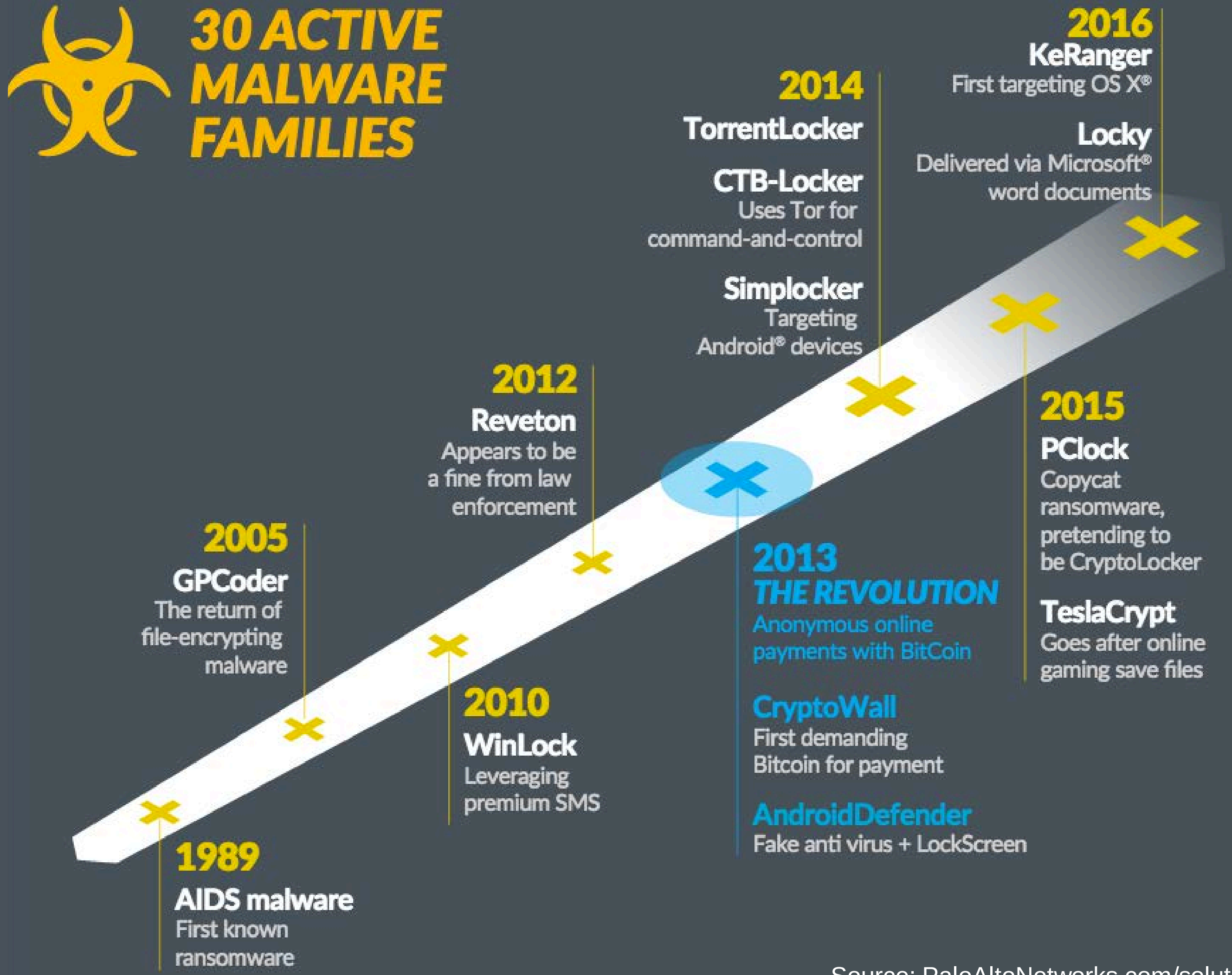
What is Ransomware

Ransomware is not a single family of malware, but a ***criminal business model*** in which malicious software is used to hold something of value for ransom

The First Ransomware Attack – AIDS Trojan



```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378.  You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

                          Press ENTER to continue
```



30 ACTIVE MALWARE FAMILIES

1989
AIDS malware
First known ransomware

2005
GPCoder
The return of file-encrypting malware

2010
WinLock
Leveraging premium SMS

2012
Reveton
Appears to be a fine from law enforcement

2013
THE REVOLUTION
Anonymous online payments with BitCoin

CryptoWall
First demanding Bitcoin for payment

AndroidDefender
Fake anti virus + LockScreen

2014
TorrentLocker

CTB-Locker
Uses Tor for command-and-control

Simplocker
Targeting Android® devices

2015
PClock
Copycat ransomware, pretending to be CryptoLocker

TeslaCrypt
Goes after online gaming save files

2016
KeRanger
First targeting OS X®

Locky
Delivered via Microsoft® word documents

Source: PaloAltoNetworks.com/solutions/initiatives/ransomware

CYBER THREAT ALLIANCE

CryptoWall v3 Investigation

Co-Founded by

Palo Alto Networks

Intel Security

Symantec

Fortinet

$325M

Estimated Damages Across the Globe

44%

Victims Paid Up

30.7%

Exploit Delivery

Source: http://go.paloaltonetworks.com/cryptowall

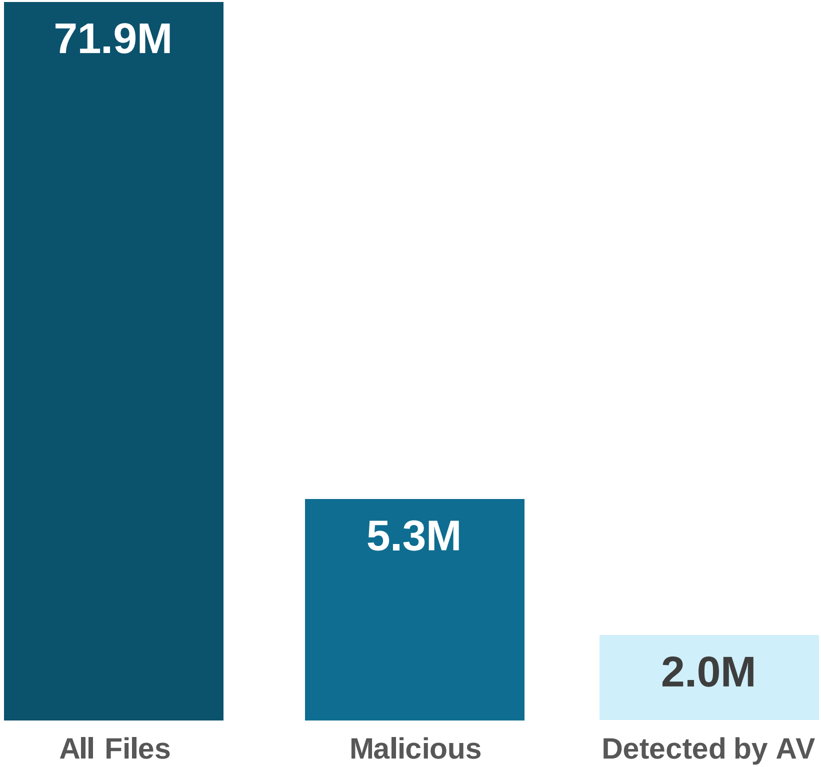
1M+

Unique samples of crypto ransomware collected in Palo Alto Networks WildFire Threat Intelligence Cloud.

30+

Families of crypto ransomware tracked in Palo Alto Networks AutoFocus threat analysis service.

WildFire Demonstrates the Shortcomings of Current Approach



37.5%

Of the malware files seen by WildFire each month are detected by the top 6 enterprise AV vendors*.

*Average monthly values as of January 2016. Source: Palo Alto Networks WildFire and Multi-Scanner

Dealing with Ransomware

Preparation

Prevention

Response

To Prevent Ransomware:

1. Attack Vectors
2. Delivery Methods
3. How to Block

1. Attack Vectors

Exploits

Macros

Exec

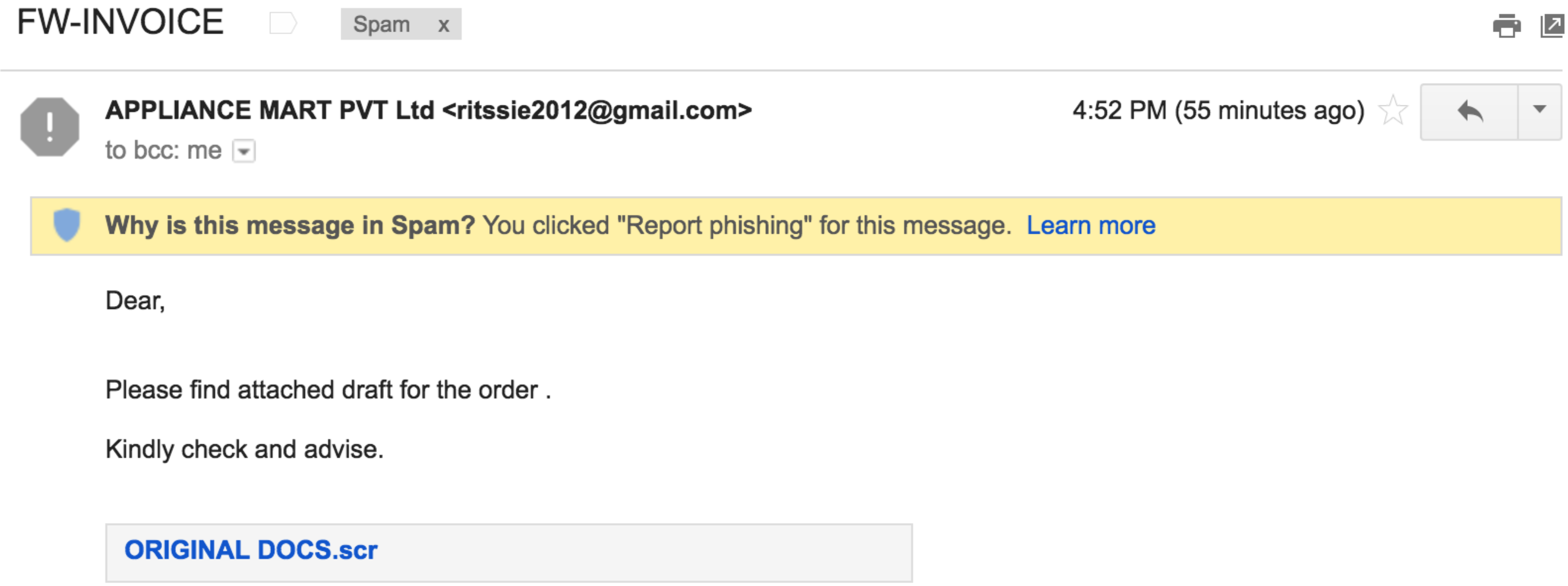
2. Delivery Methods

Exploit Kits

Email Attachments

Drive-by Downloads

A Ransomware Email That I Received on my Personal Email



FW-INVOICE

APPLIANCE MART PVT Ltd <ritssie2012@gmail.com>

to bcc: me

4:52 PM (55 minutes ago)

Why is this message in Spam? You clicked "Report phishing" for this message. Learn more

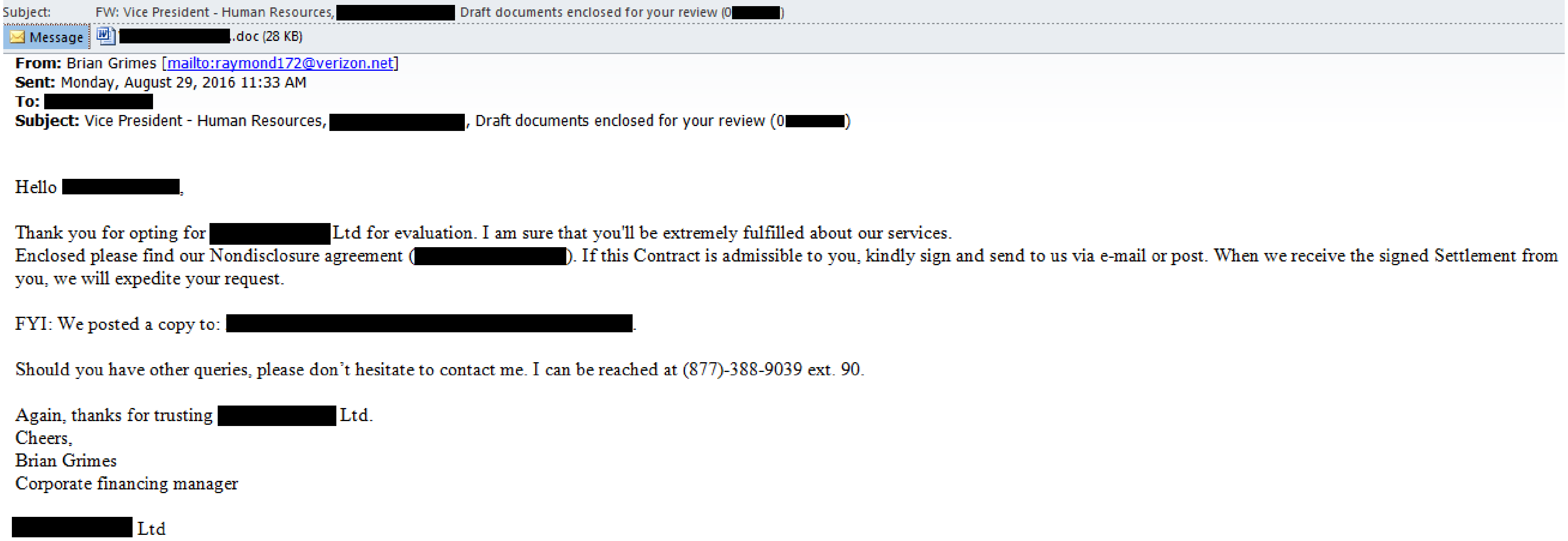
Dear,

Please find attached draft for the order .

Kindly check and advise.

ORIGINAL DOCS.scr

More Sophisticated Ransomware Examples



Subject: FW: Vice President - Human Resources, [redacted] Draft documents enclosed for your review (0[redacted])

[redacted].doc (28 KB)

From: Brian Grimes [mailto:raymond172@verizon.net]
Sent: Monday, August 29, 2016 11:33 AM
To: [redacted]
Subject: Vice President - Human Resources, [redacted], Draft documents enclosed for your review (0[redacted])

Hello [redacted],

Thank you for opting for [redacted] Ltd for evaluation. I am sure that you'll be extremely fulfilled about our services.
Enclosed please find our Nondisclosure agreement ([redacted]). If this Contract is admissible to you, kindly sign and send to us via e-mail or post. When we receive the signed Settlement from you, we will expedite your request.

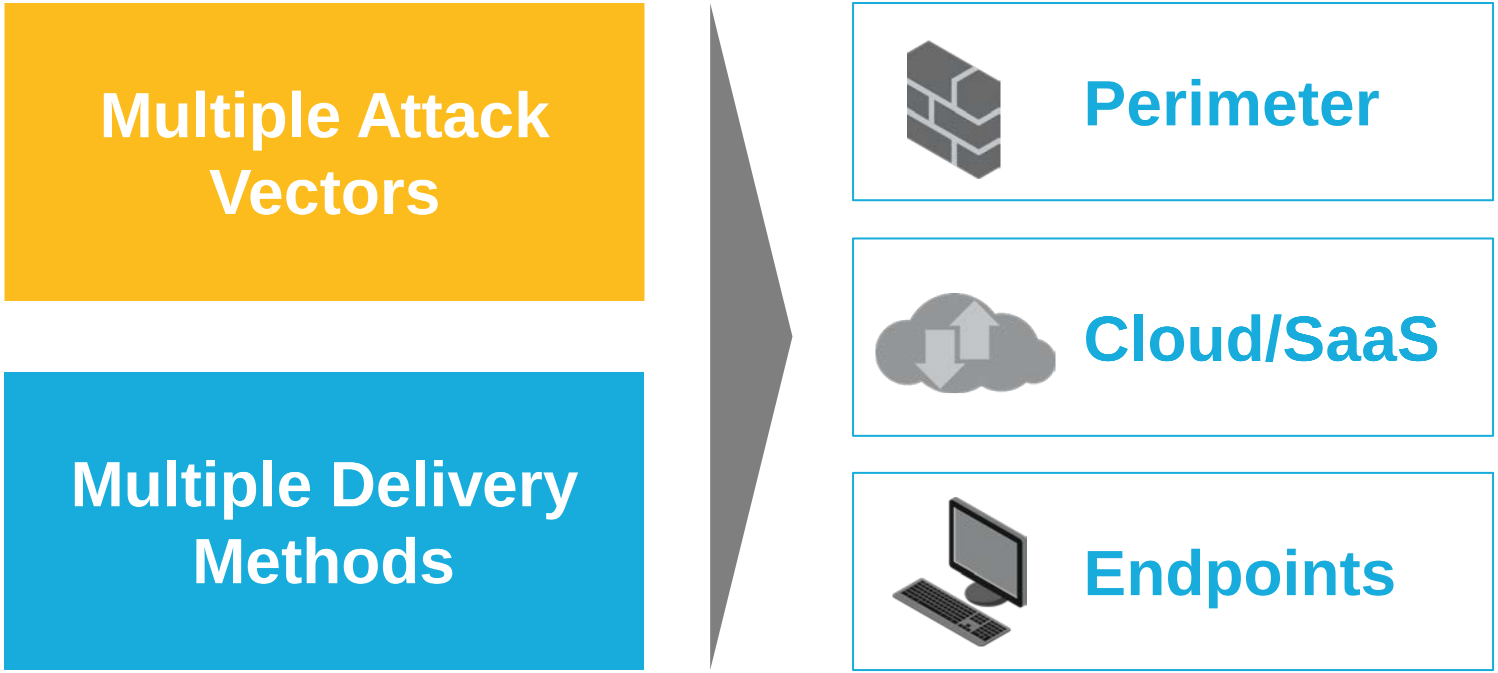
FYI: We posted a copy to: [redacted].

Should you have other queries, please don't hesitate to contact me. I can be reached at (877)-388-9039 ext. 90.

Again, thanks for trusting [redacted] Ltd.
Cheers,
Brian Grimes
Corporate financing manager

[redacted] Ltd

3. How to Block



Multiple Attack Vectors

Multiple Delivery Methods

Perimeter

Cloud/SaaS

Endpoints

3. How to Block

1 Reduce Attack Surface

2 Prevent Known Threats

3 Prevent Unknown Threats

1

Reduce Attack Surface

Disallow non-org access

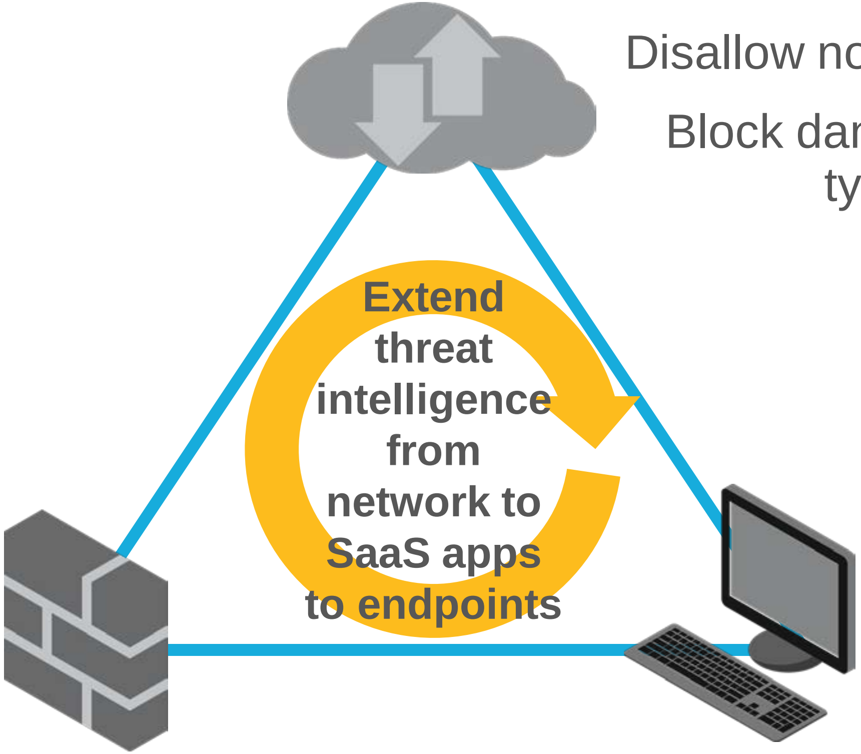
Block dangerous file types

Block unknown traffic

Block malicious URLs

Evaluate encrypted traffic

Stop dangerous file types

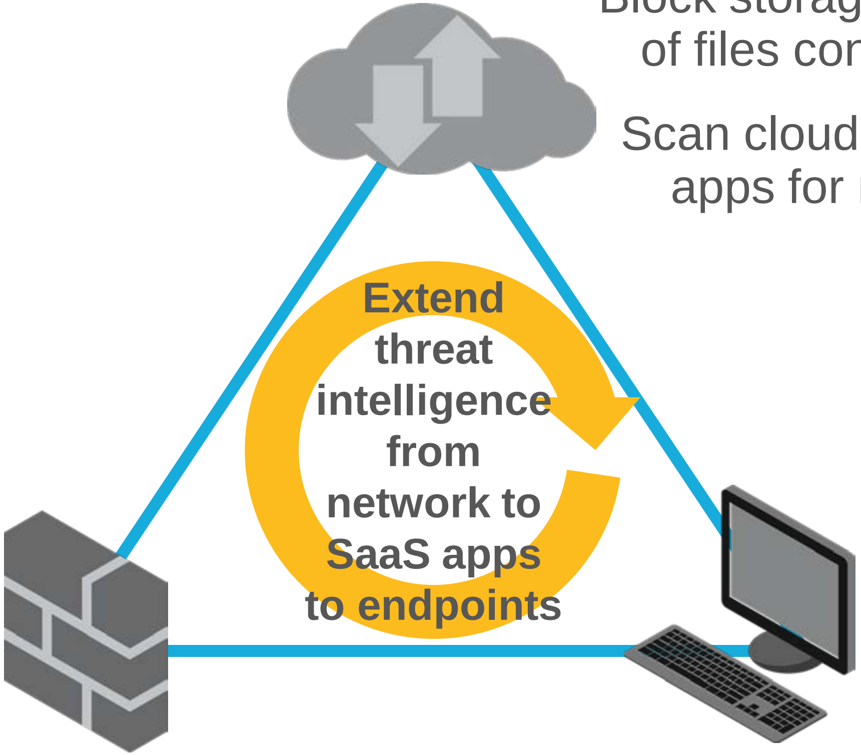


Extend threat intelligence from network to SaaS apps to endpoints

Extend zero-trust policies to endpoints

2

Prevent Known Threats



Extend threat intelligence from network to SaaS apps to endpoints

Block storage or transmission of files containing exploits

Scan cloud storage & SaaS apps for malicious files

Block malicious URLs

Stop known exploits, malware & command-and-control traffic

Block execution of known malware

Block all known exploits

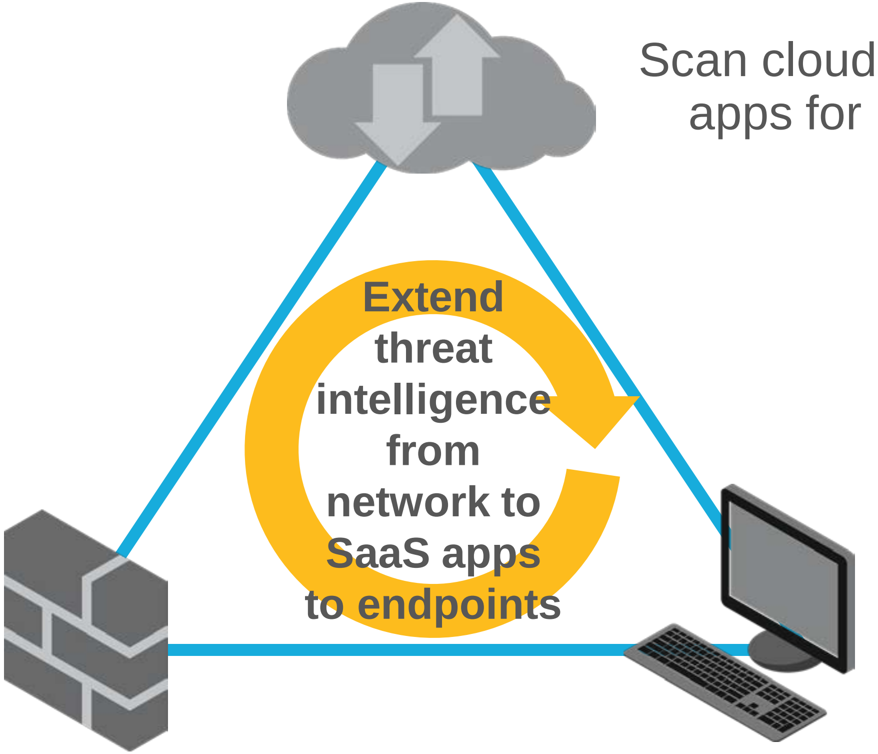
3
Prevent Unknown Threats

Scan cloud storage & SaaS apps for malicious files

Control unknown traffic

Add context to threats and create proactive protections

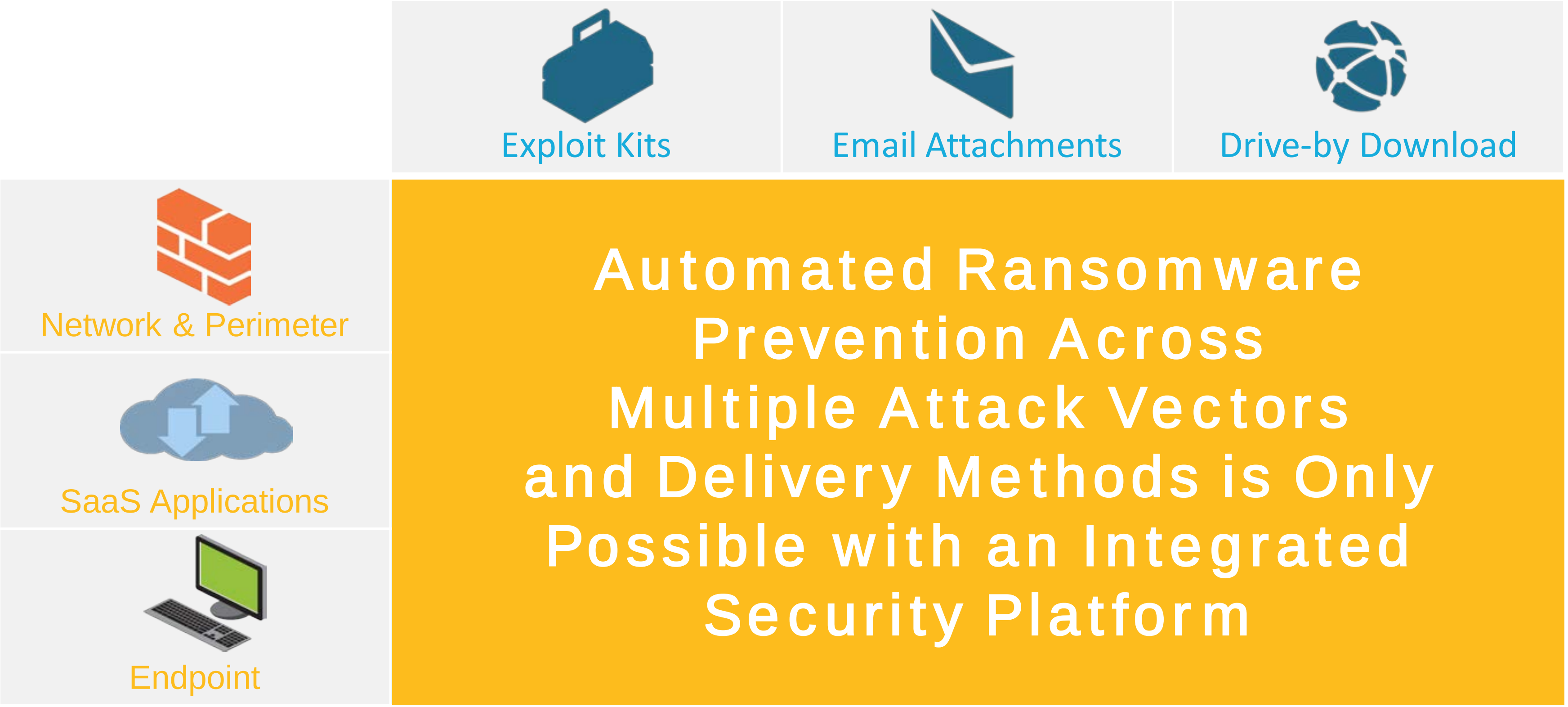
Detect and prevent threats in unknown files and URLs



Extend threat intelligence from network to SaaS apps to endpoints

Block execution of unknown malware

Block all unknown and zero-day exploits



Exploit Kits

Email Attachments

Drive-by Download

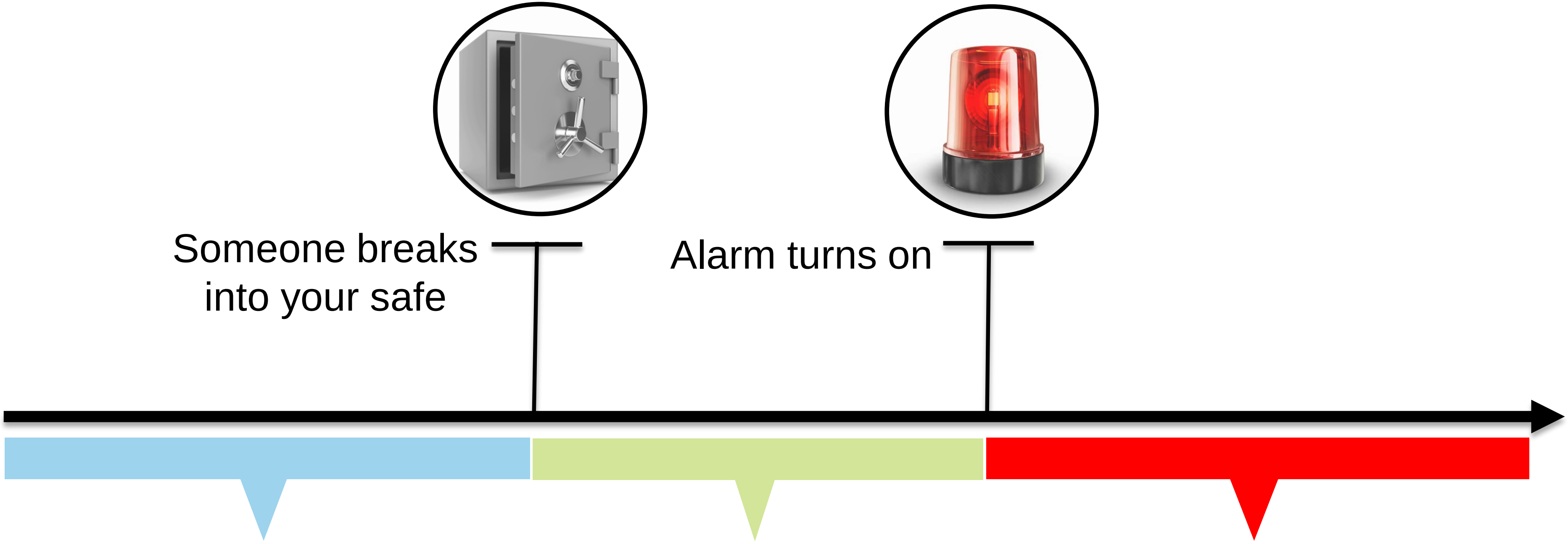
Network & Perimeter

SaaS Applications

Endpoint

Automated Ransomware Prevention Across Multiple Attack Vectors and Delivery Methods is Only Possible with an Integrated Security Platform

Looking at Another Industry Trying to Protect Their Assets



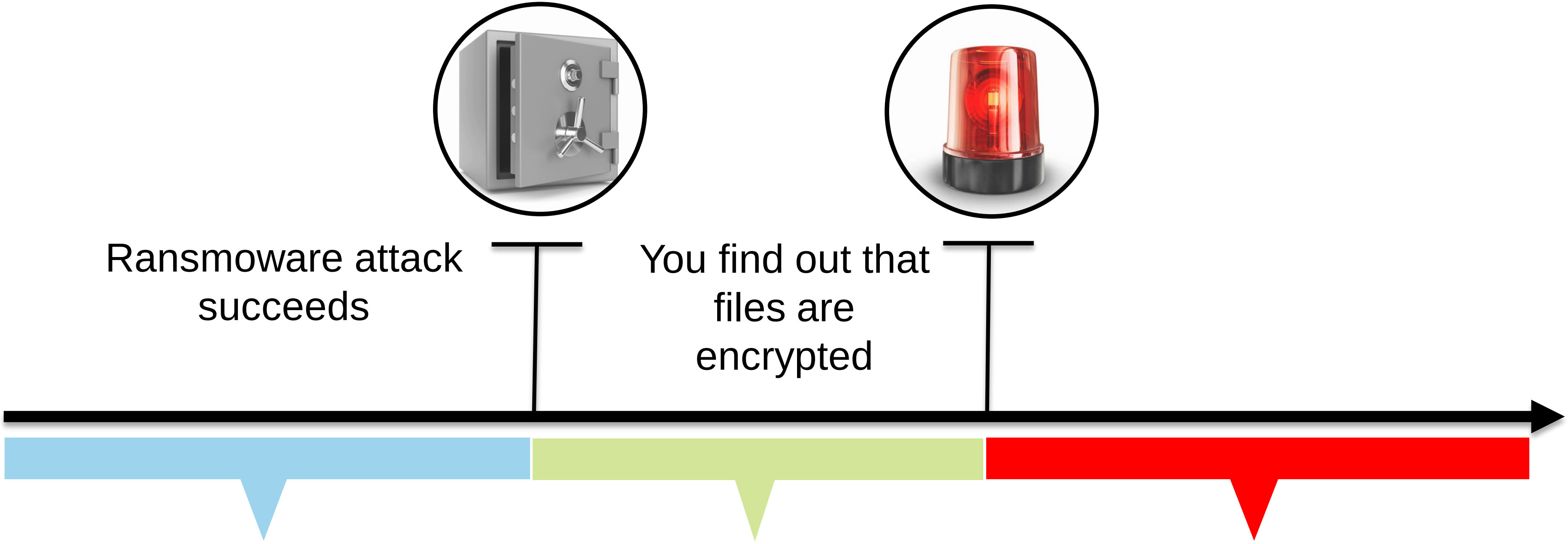
Someone breaks into your safe

Alarm turns on

Stop Thief from entering

Pray you made the right choice

Contain



Ransmoware attack succeeds

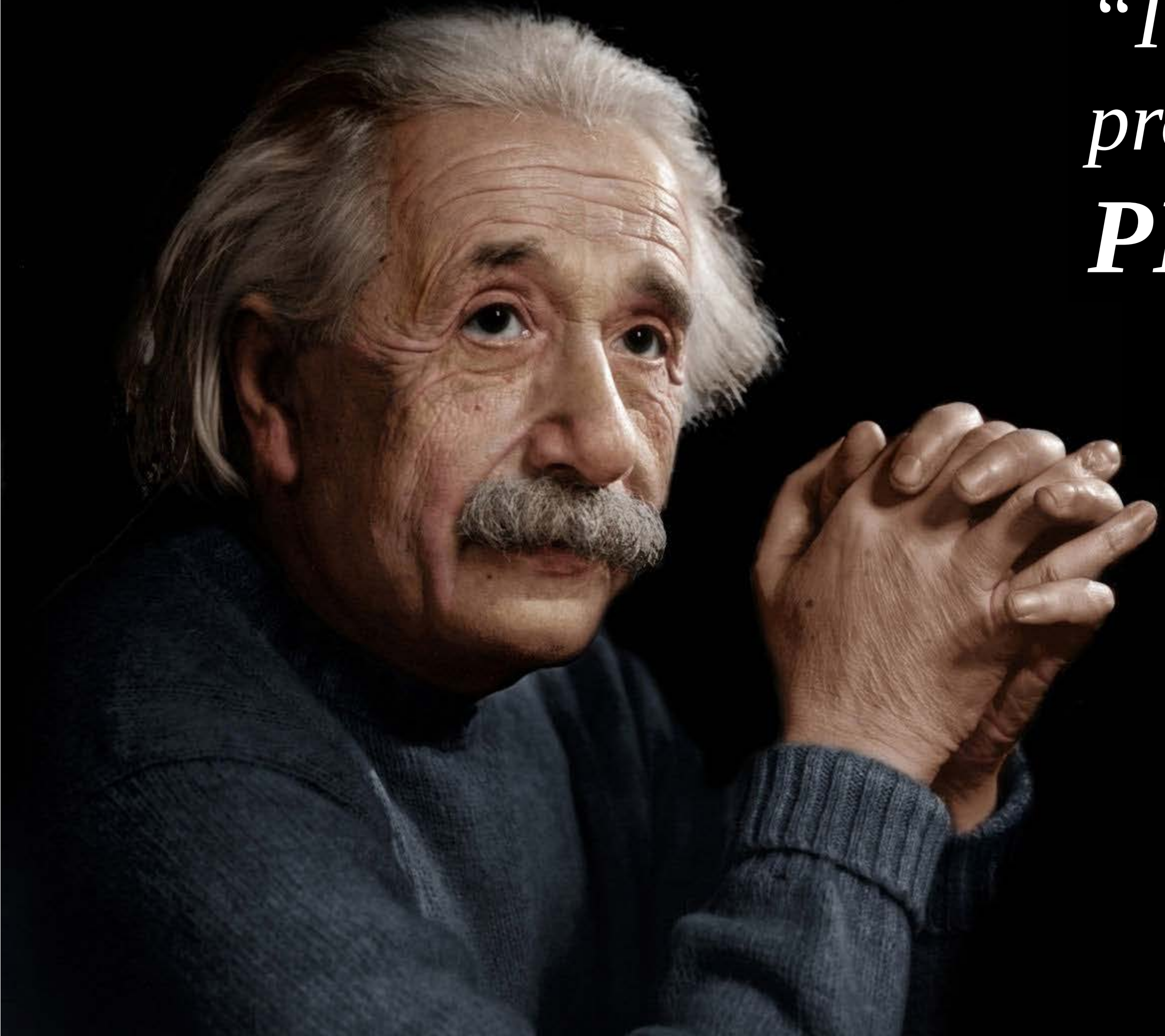
You find out that files are encrypted

Prevention

It’s only a matter of time to find out

Remediation

Where would you prefer to be?



“Intellectuals solve problems. Geniuses ***PREVENT*** *them.”*

-Albert Einstein

THANK YOU

paloalto NETWORKS®