The Rise of Ransomware

Three Critical Steps to Prevent an Outbreak in Your Organization

Pez Zivic

Global Systems Engineer

CISSP, CISA

FBI Says Threat From 'Ransomware' Is Expected to Grow

THE WALL STREET JOURNAL.

Hollywood Hospital Hit By Ransomware Attack, FBI Investigates

InformationWeek DARKReading

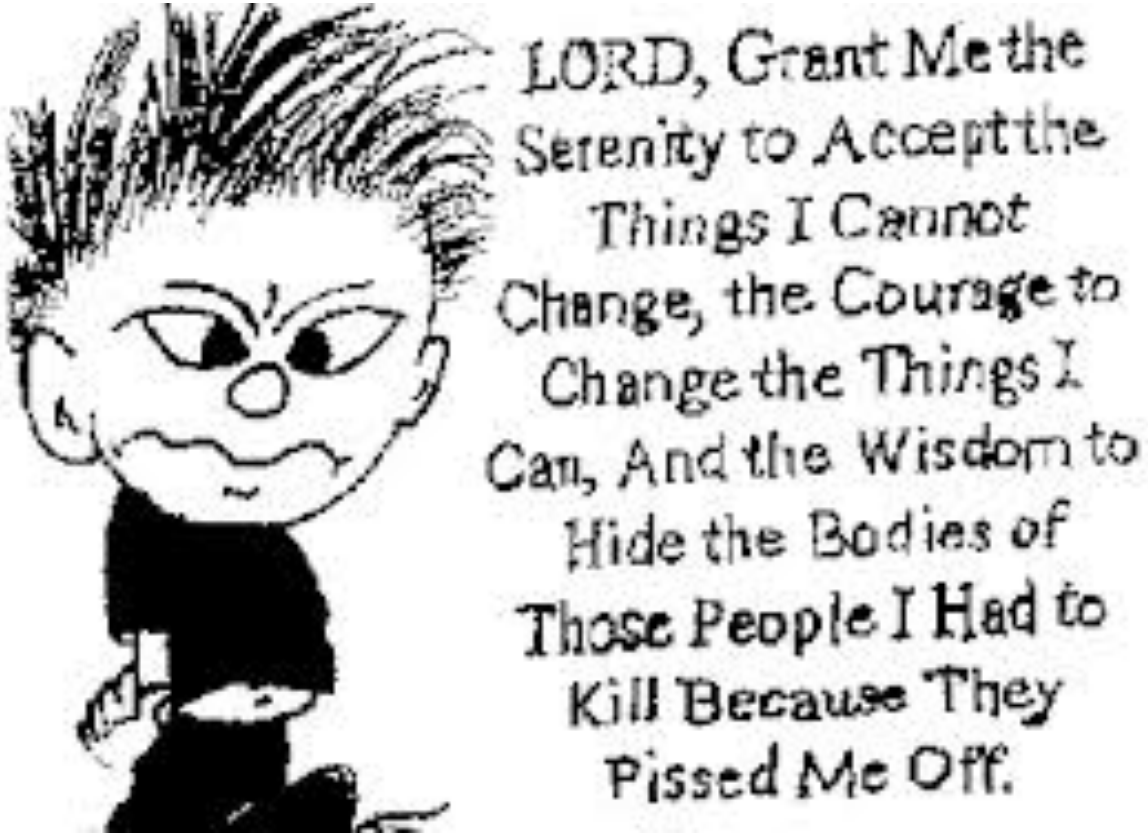
Ransomware Warning Issued After Triad Company's Files Held Hostage

WFMY NEWS 2

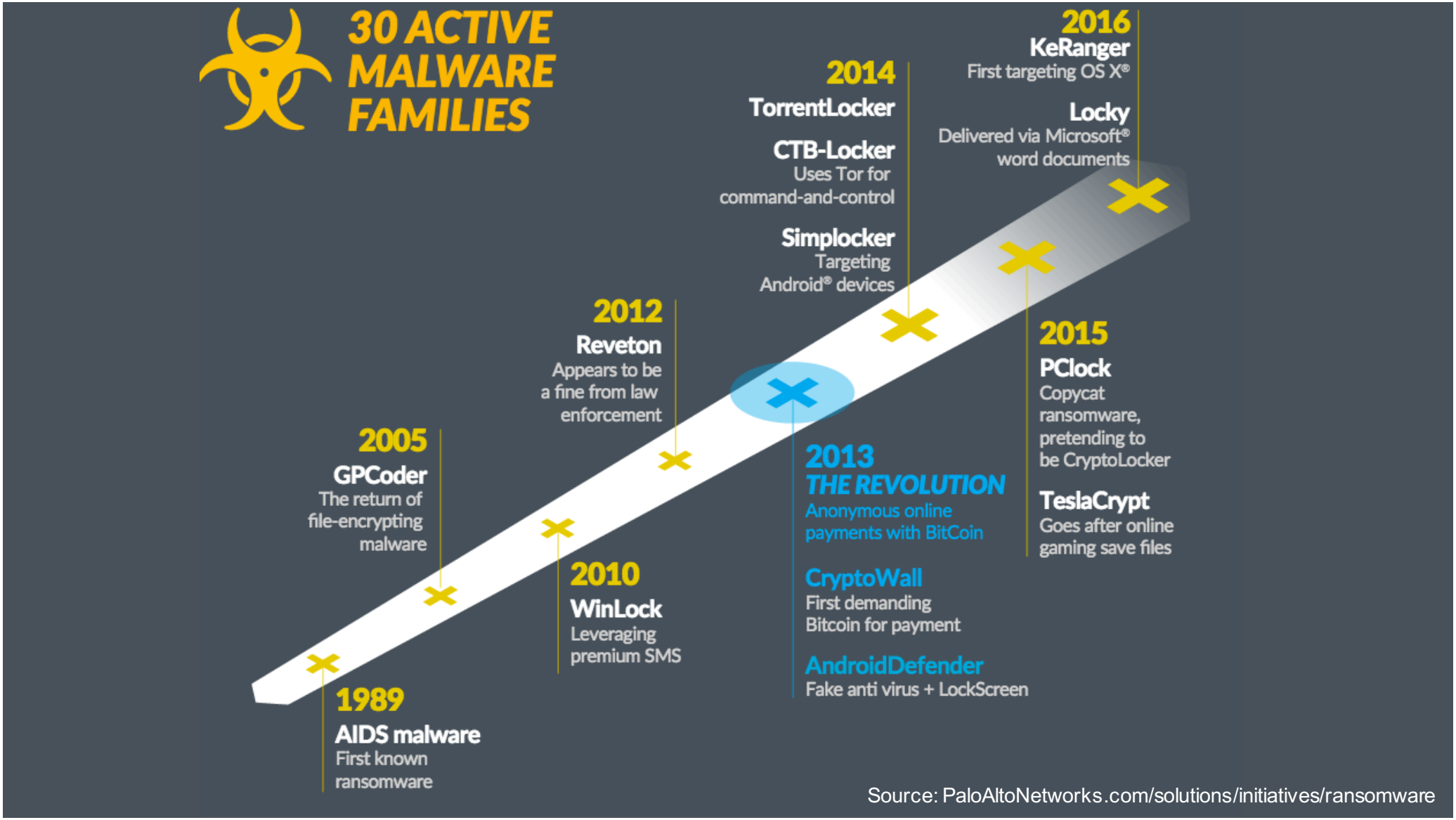
paloalto NETWORKS®


FOX NEWS
FOX BUSINESS
FOX NEWS Latino
FOX NEWS GO
FOX NEWS RADIO
FOX NATION
FOX NEWS INSIDER
LOGIN
TECHNOLOGY FOX NEWS
Search foxnews.com
TECH HOME
COMPUTERS
GOOGLE
VIDEO GAMES
MILITARY TECH
WAR GAMES
SLIDESHOWS
HACKERS
Hospital pays nearly $17G in bitcoins to hackers who disabled computer network
Published February 18, 2016 · FoxNews.com
1284
0
655
AMERICA'S NEWSROOM
CALIFORNIA HOSPITAL HELD HOSTAGE BY HACKERS THAT LOCKED PATIENT RECORDS
NOW PLAYING
Hospital held hostage by hackers pays $17,000 ransom
Never autoplay videos
A Los Angeles hospital paid a ransom of nearly $17,000 in bitcoins to hackers

How do we feel?



Research and Learn!


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

Cooperation and Partnership in Research and Learning

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

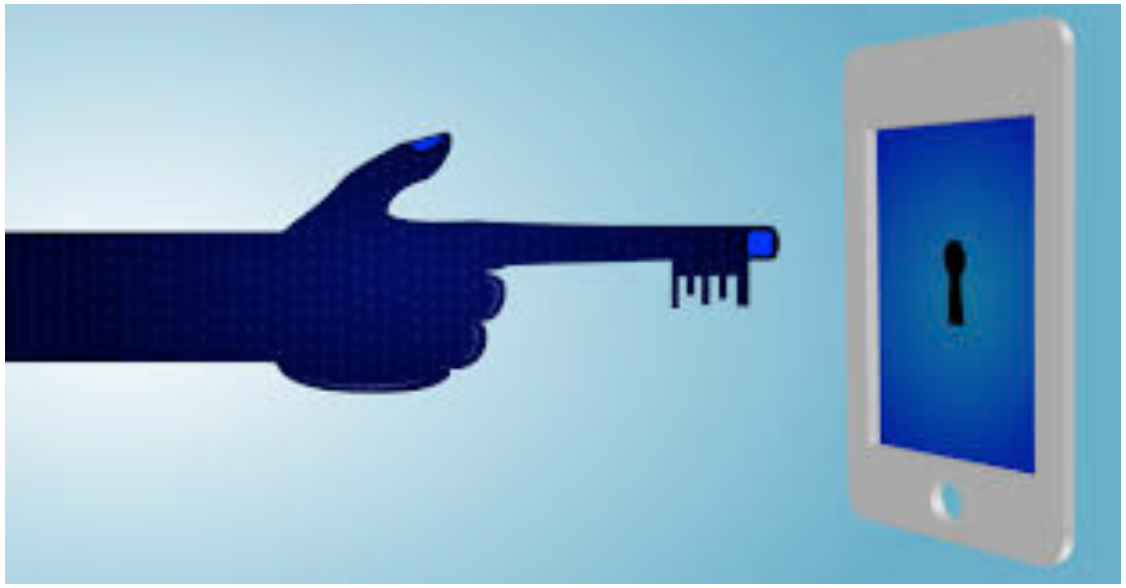
30.7%

Exploit Delivery

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

paloalto NETWORKS

What We Learned?



To Prevent Ransomware:

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

Hidden Attack Vectors!

1. Attack Vectors

1. Attack Vectors

Exploits

1. Attack Vectors

Exploits

Macros

1. Attack Vectors

Exploits

Macros

Exec

Delivery Methods

2. Delivery Methods

2. Delivery Methods

Exploit Kits

2. Delivery Methods

Exploit Kits

User visits a compromised website

Malicious code or ad redirects to exploit kit landing page

Exploit kit page loads; determines best way to compromise user endpoint

Exploit kit compromises user endpoint

Exploit kit delivers ransomware

Ransomware encrypts data and holds it for ransom

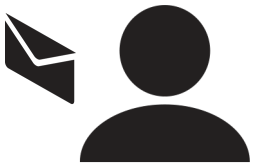
2. Delivery Methods

Exploit Kits

Email Attachments

2. Delivery Methods

Email Attachments



User receives targeted email with infected file

User opens file, thinking it is a legitimate document

Office runs macro, downloads ransomware from URL embedded in doc

Ransomware encrypts data and holds it for ransom

2. Delivery Methods

Exploit Kits

Email Attachments

Drive-by Downloads

2. Delivery Methods

Drive-by Download

User visits a compromised website

Website serves exploit to compromises user endpoint

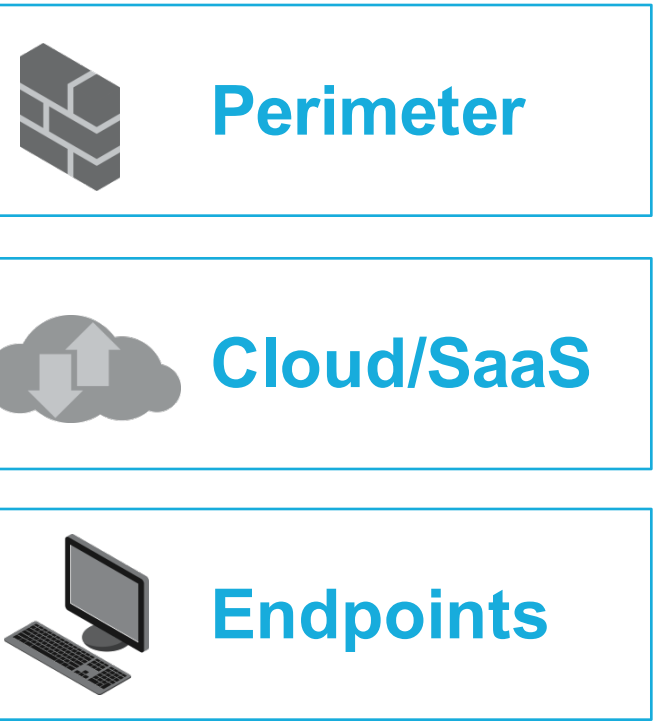
Exploit downloads ransomware

Ransomware encrypts data and holds it for ransom

The Problem – Prevent & Detect Ransomware

Multiple Attack Vectors

Multiple Delivery Methods



How to Block and Detect?

3. How to Block

1

Reduce Attack Surface

2

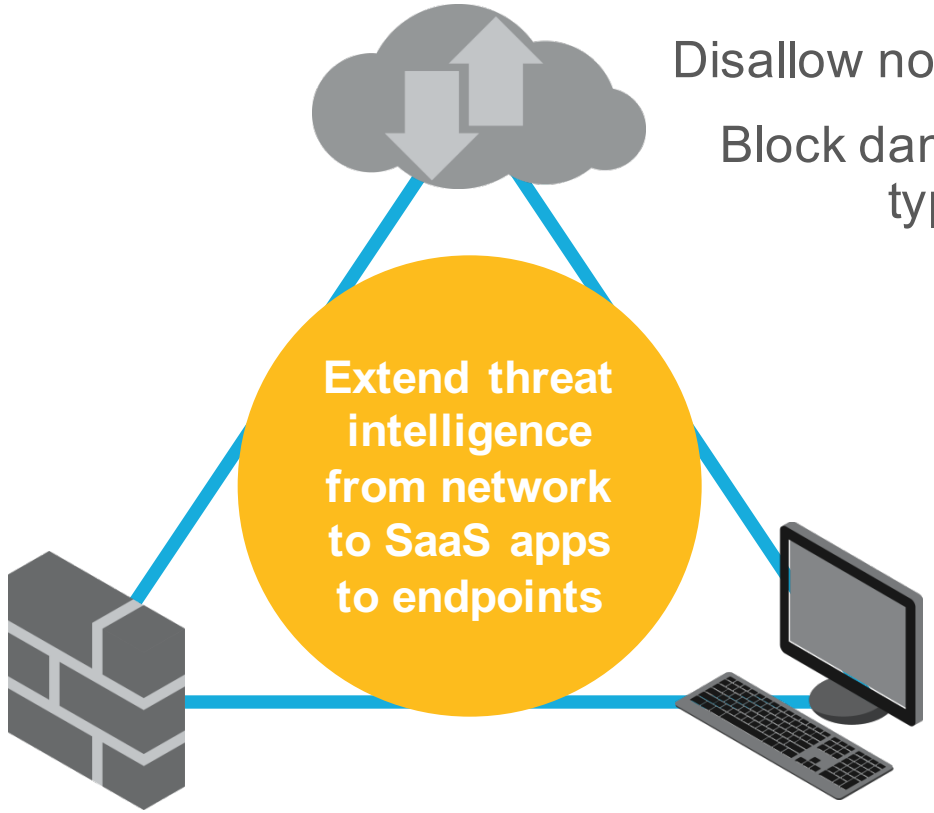
Prevent Known Threats

3

Prevent Unknown Threats

Reduce Attack Surface

1 Reduce Attack Surface



Disallow non-org access

Block dangerous file types

Block unknown traffic

Block malicious URLs

Micro-segmentation N-S & E-W

Stop dangerous file types

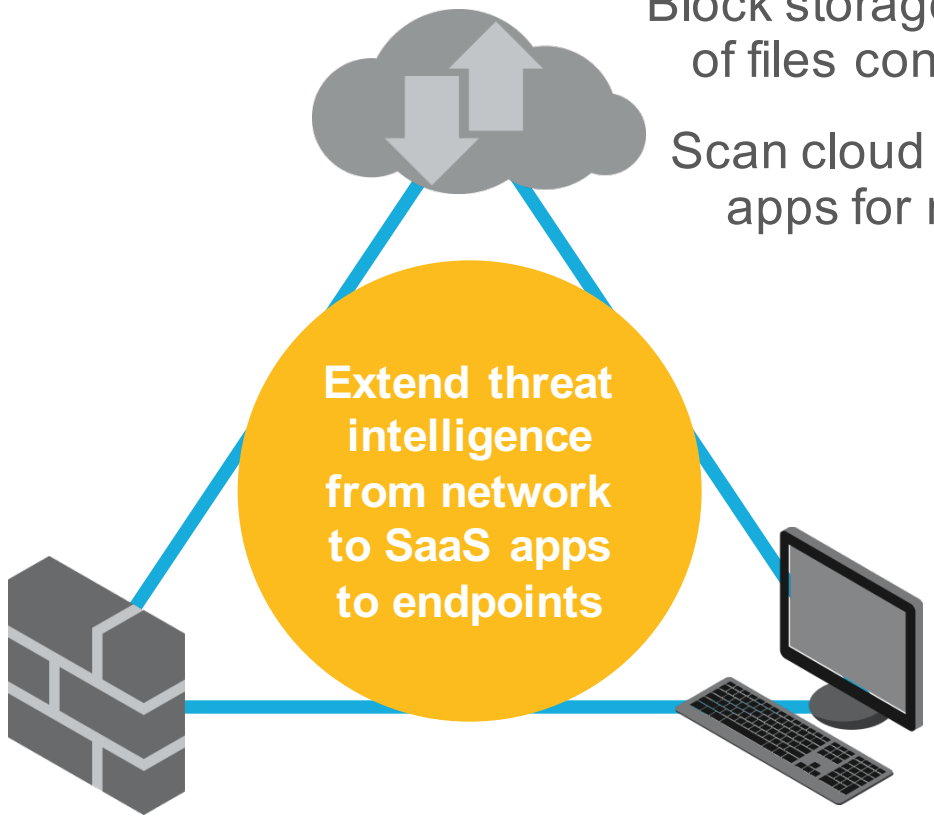
Extend zero-trust policies to endpoints

Prevent Known Threats

2 Prevent Known Threats

Block storage or transmission of files containing exploits

Scan cloud storage & SaaS apps for malicious files



Block malicious URLs

Block Virus & Vulnerabilities

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

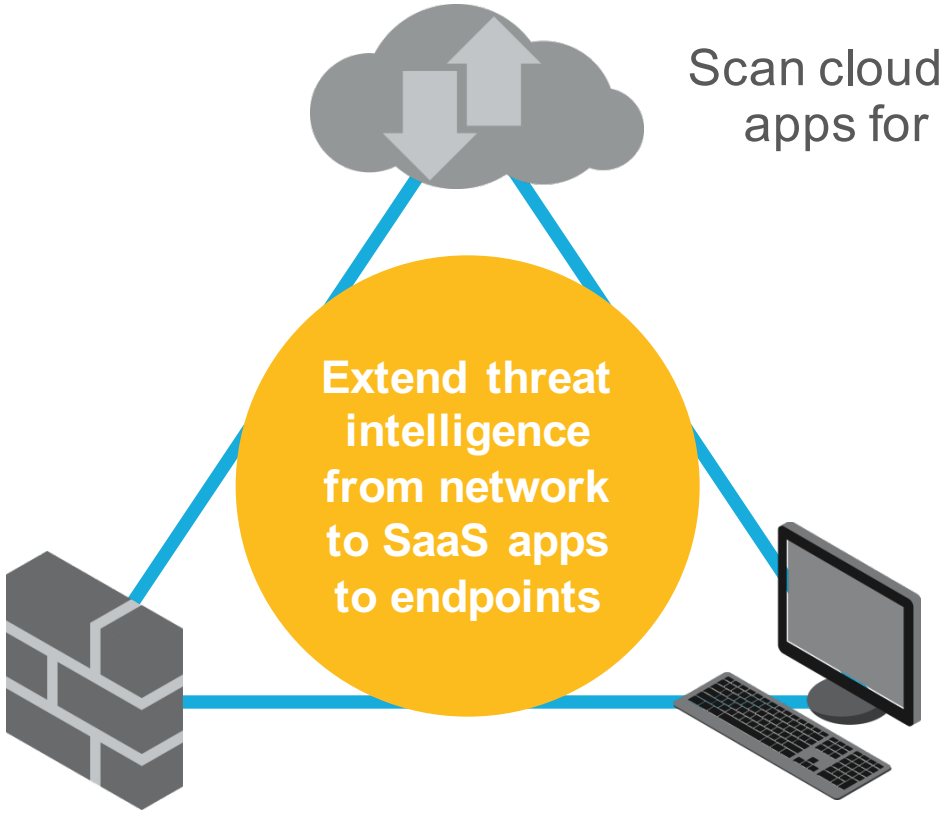
Block execution of known malware

Block all known exploits

Prevent Unknown Threats

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

Block execution of unknown malware

Block all unknown and zero-day exploits

Exploit Kits

Email Attachments

Drive-by Download

Network & Perimeter

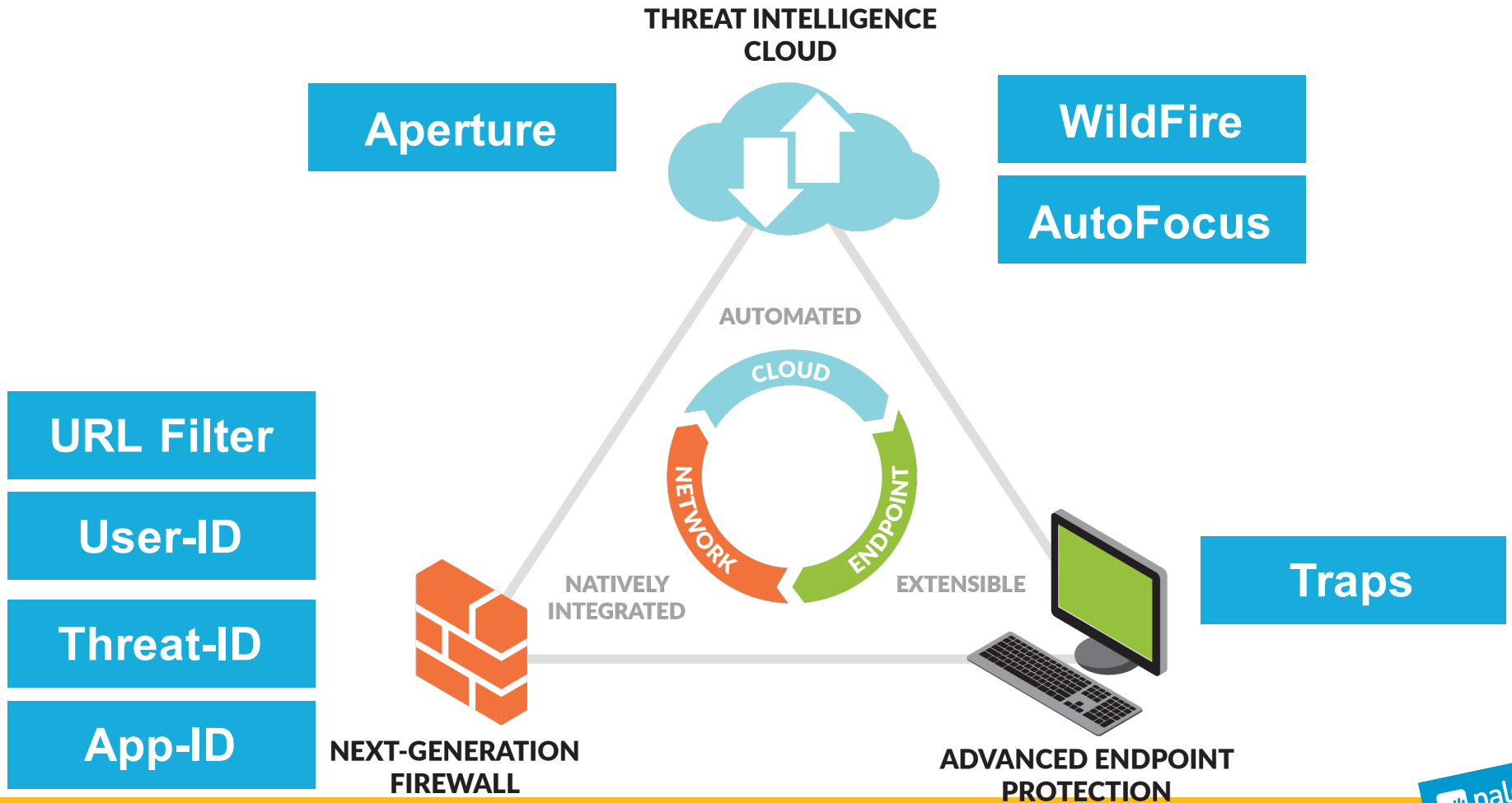
SaaS Applications

Endpoint

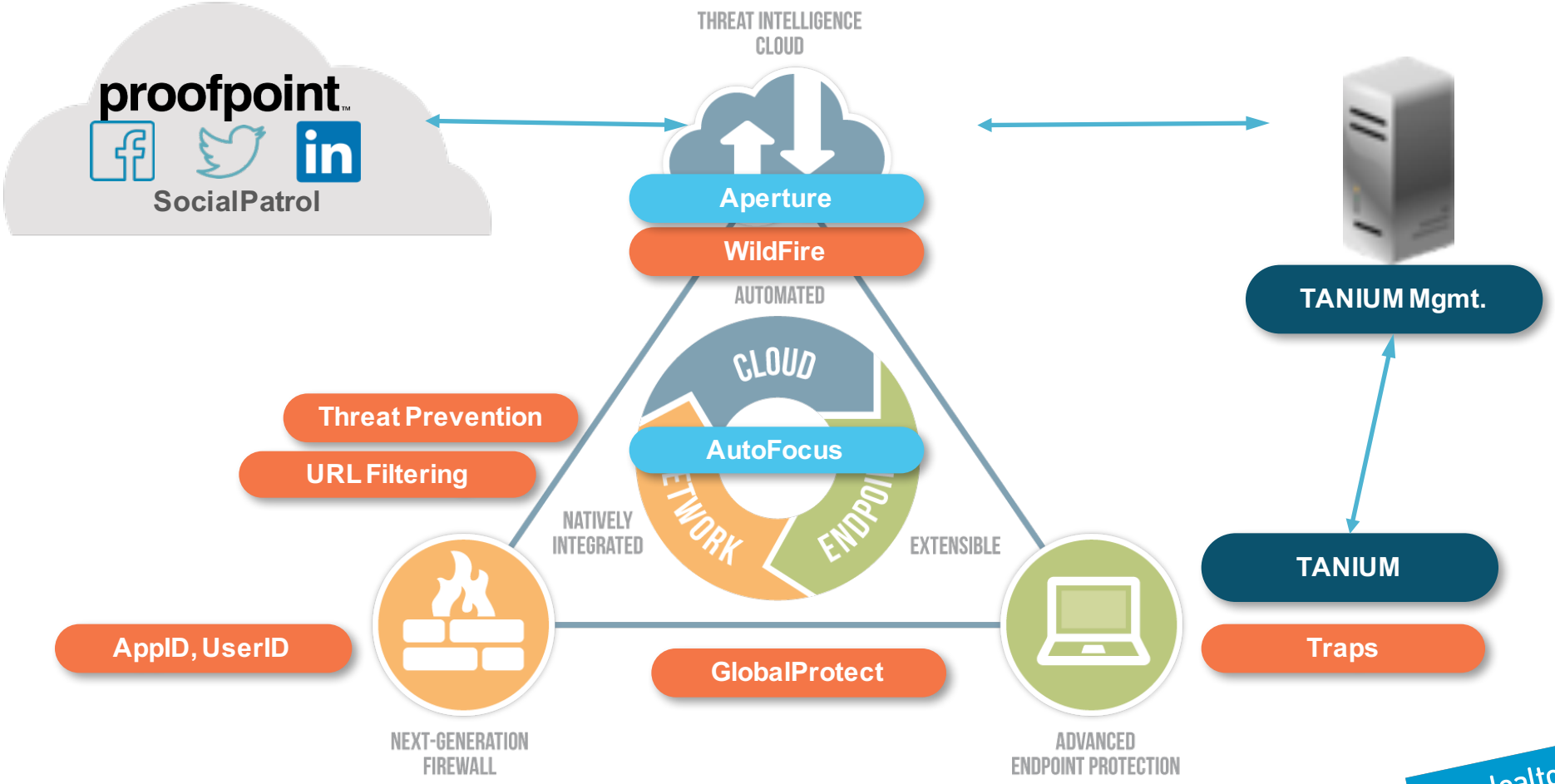
Automated Ransomware Prevention Across Multiple Attack Vectors and Delivery Methods is Only Possible with an Integrated Security Platform

How to Block and Detect?

Implementing Contextual Security



Enhancing Contextual Security with Partners



RESOURCES

Unit 42 Ransomware Report:

http://Go.PaloAltoNetworks.com/ransomware2016

Ultimate Test Drives:

http://Go.PaloAltoNetworks.com/TestDrive