



# How Cryptojacking and other Insider Threats Challenge Digital Economy

Judgment Day

Artur Kane, Technology Evangelist

8<sup>th</sup> November 2018



**Flowmon**

Driving Network Visibility

*“To remain ahead of increasing network complexity,  
network operators must explore and learn new advanced  
automation and analytics tools.”*

Source: NetOps 2.0: Embrace Network Automation and Analytics to Stay Relevant in  
the Digital Business Era, Gartner 2017



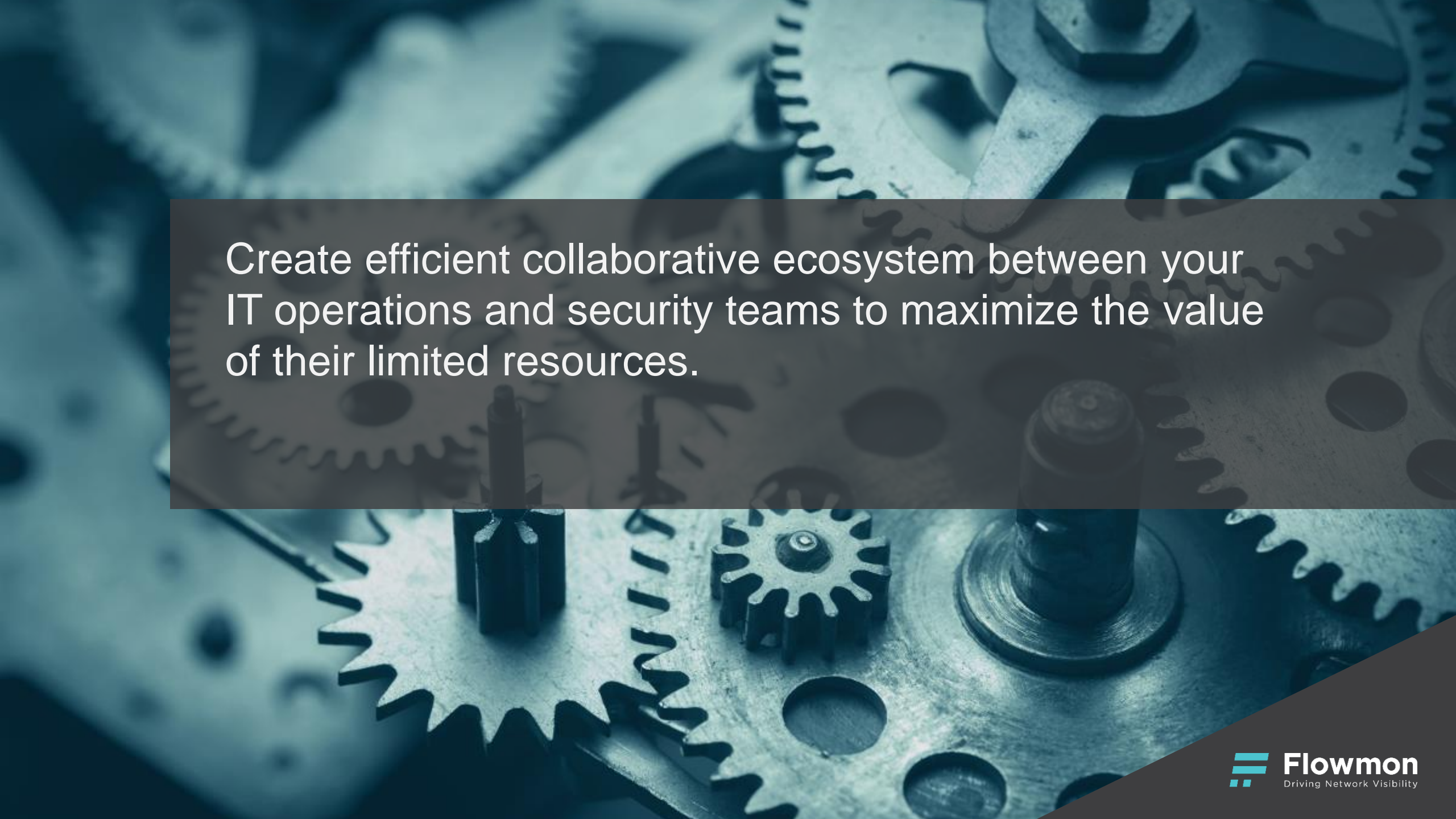
Enterprises are too  
dependent on network



Networks are too  
complicated to operate

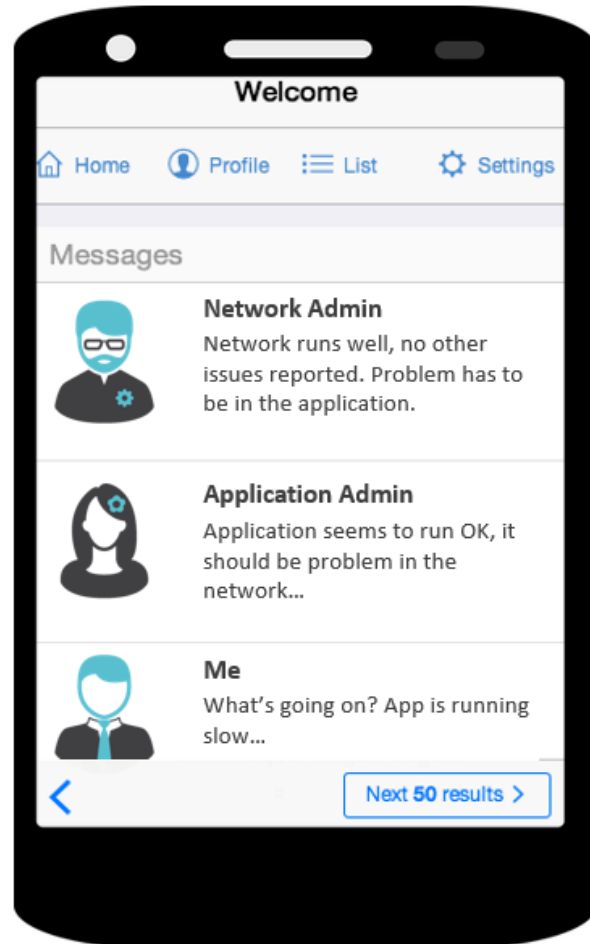


Experienced Experts are  
overwhelmed



Create efficient collaborative ecosystem between your IT operations and security teams to maximize the value of their limited resources.

# Security incidents interrupt business continuity



User reported slow internet connectivity and Mission critical system unreachable



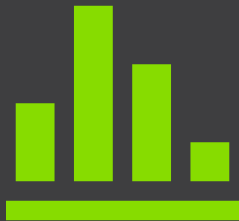
When Mission  
Critical  
Application is  
down, the whole  
business stops



# IMPACTS



Customers sharing experience on social media



Employees are non productive



The company isn't generating a revenue



I am leaving my work to focus on troubleshooting



Management requires explanation and resolution which I cannot offer



# Perimeter vs. Internal security

90% of security budget is spent on perimeter while only 25% target it.



An overhead view of a wooden office desk where several people are working. The desk is cluttered with various items including keyboards, mice, coffee cups, folders, and documents. A central text box is overlaid on the image.

# Insider Threats

one of the most common ways customer data or industrial and trade secrets are leaked





**Once malware get's in,  
perimeter and prevention are useless**



# You Have Been Social Engineered

100 terabytes of data was stolen from Sony Pictures in 2014.

1. Malware gets into a network through a spear-phishing email
2. The malware leverages weak passwords, different vulnerabilities, escalates privileges and takes over the control of accesses
3. The attacker can now operate freely

## **Countermeasures:**

Filter mails and educate employees!



# Attackers Among Us

A Korea Credit Bureau's employee sold details of their 104 million customers to a marketing firm.

1. An angry worker who wants to get some cash?
2. Has access to company data
3. Takes data out the old way – on a USB stick

## Countermeasures:

Get DLP and restrict accesses!



# Policies Do Not Apply To Some

40 million credit card details were lost because Target company engineers did not pay attention to their security system alerts.

1. All technologies and processes are in place
2. More restrictions to users only brings trouble
3. Person under pressure, being arrogant or just lazy can go rouge


## Countermeasures:

Inevitable. 90% of all Insider Threats are caused by “Goofs”.  
Fast detection and response minimizes business impact.



# Early detection and response

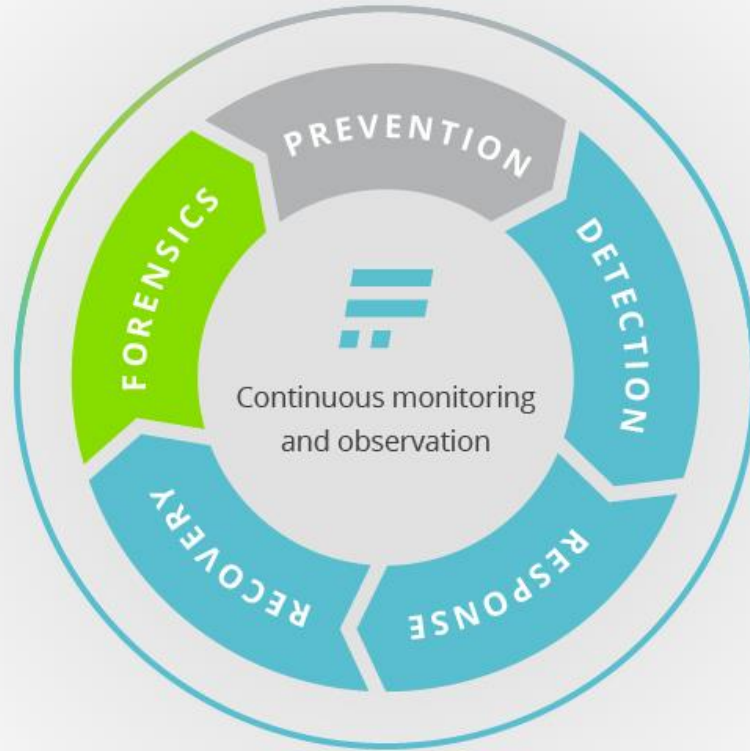
## Behavior Analysis & Anomaly Detection



Signature based detection is like border control –  
you aren't on the blacklist, you may pass



Using data from airport surveillance, Anomaly Detection is a brain with capability to detect suspicious behavior of an unknown attacker anywhere, anytime, real-time.





Secure perimeter

---



Educated users

---



Access control and activity logging

---



Early detection and response





# Trending now

## Cryptomining malware

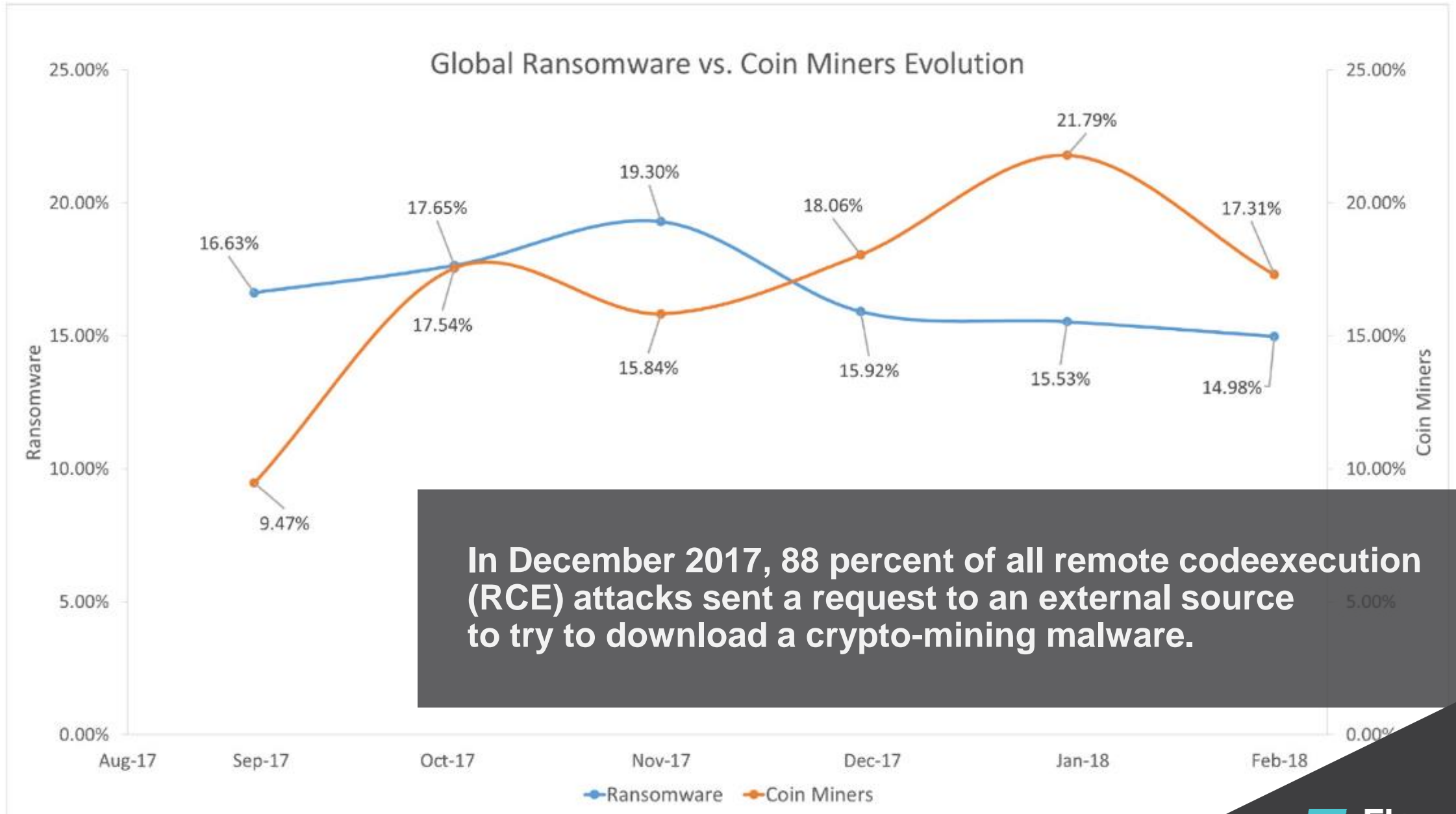
The Rise of Cryptomining  
Malware

Defenders' Hope for  
Vaccination


Evasive Techniques

## 3 Malware Trends to Watch Out for in 2018

by Minerva Labs





A Bitcoin coin is placed on a wooden block. A wire snare trap is set up on the block, with the wire loop positioned over the coin. The background is a gradient of orange and red.

***“Hackers see cryptojacking as a cheaper,  
more profitable alternative to ransomware,”***  
Comodo Cybersecurity Threat Research Labs’ Q1 Global Malware Report

## **CSO**

IT time spent on detection and investigation

## **CIO**

help desk and IT time spent tracking down performance issues

## **CFO**

cost of higher electricity consumption

## **CEO**

reputation impact



**Cryptojacking malware is relatively simple but can go undetected for a long time and cause extensive impacts.**





Prevent by patching

---



Educate users on phishing

---



Use web filters and browser extension blockers

---



Monitor network anomalies

## Quarantine

Select all threats

Restore

Delete

# Undetected for almost 3 months

My colleagues' experience – time between detection and first online mentions of this malware.



JS:Miner-C [Trj]

f\_003803

Users > roman > Libran > Caches > Googl > Chron > Defaul > Cache > f\_003803

10: > 8 Jan 2018 at 06:27

10: > 7 Jan 2018 at 10:47

10: > 6 Jan 2018 at 11:38

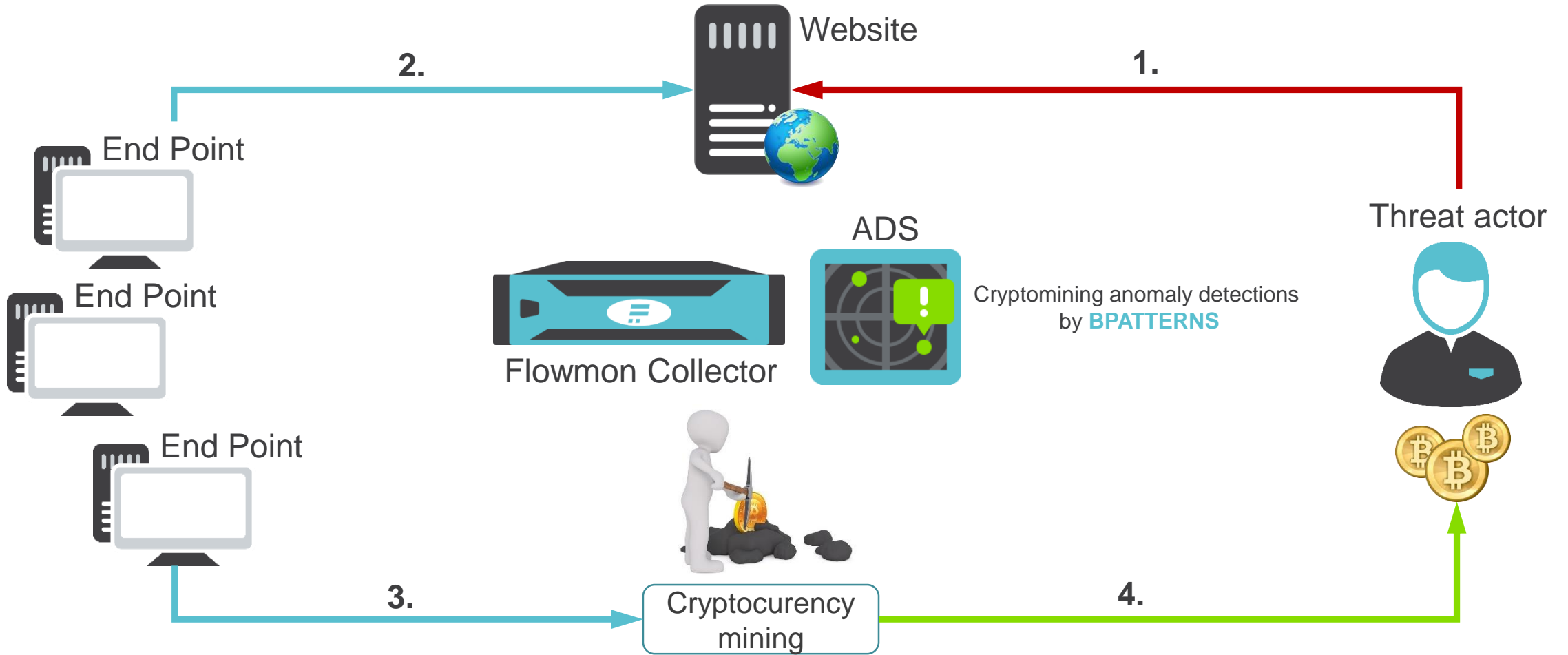
You have 3 items in (

We stopped all threats from spreading and put them in Quarantine.

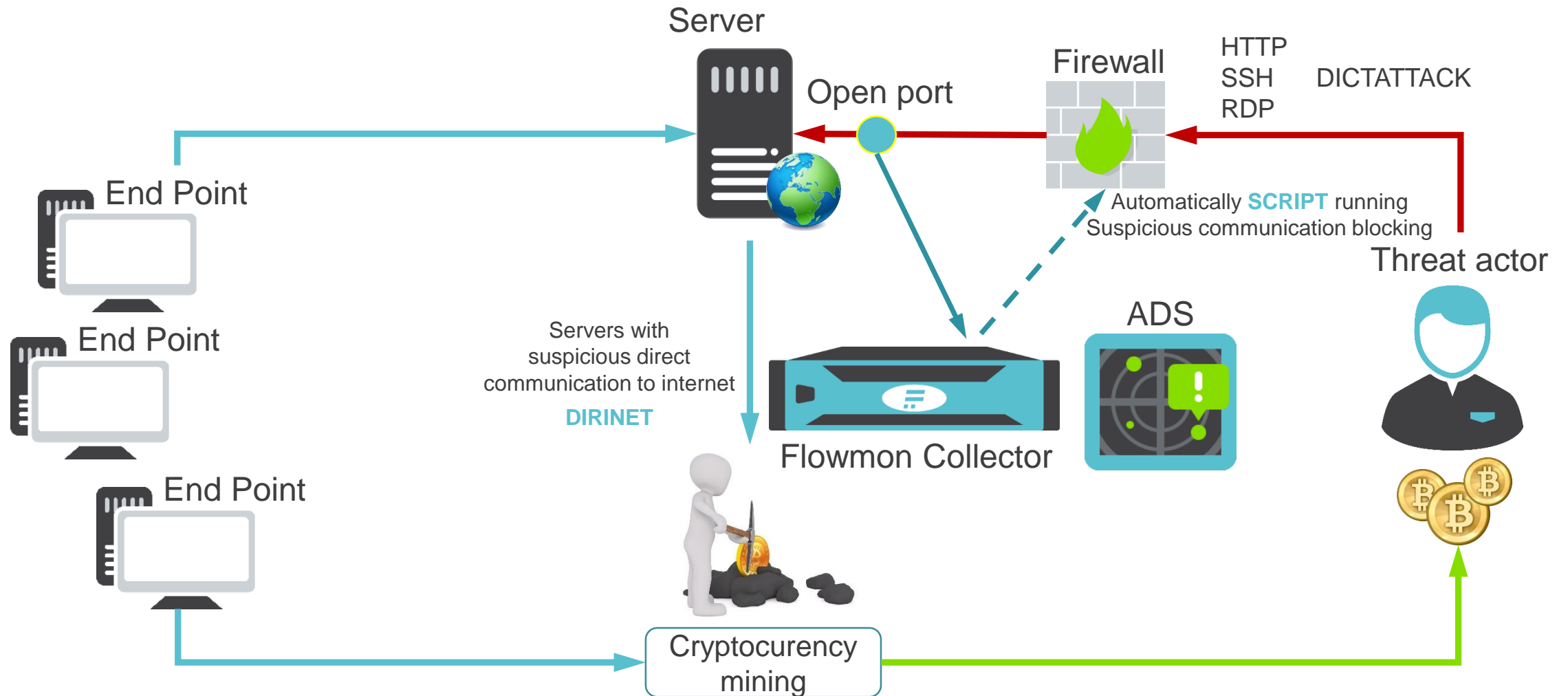


Close





<https://www.flowmon.com/en/blog/crypto-jacking-crypto-mining>



<https://www.flowmon.com/en/blog/crypto-jacking-crypto-mining>

