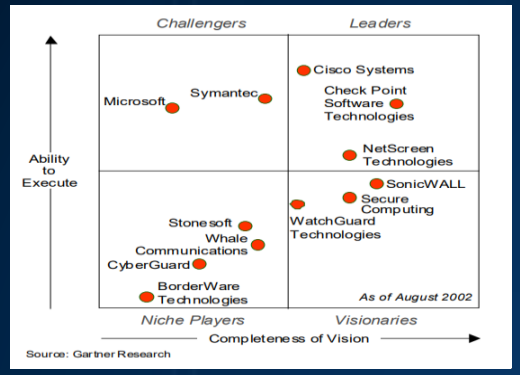
Sophos XG Firewall Evolved

sicurezza network & endpoint: Sophos synchronized security

Emilio Tonelli
Senior Sales Engineer

SOPHOS DISCOVER 2019
EVOLVE



Firewall

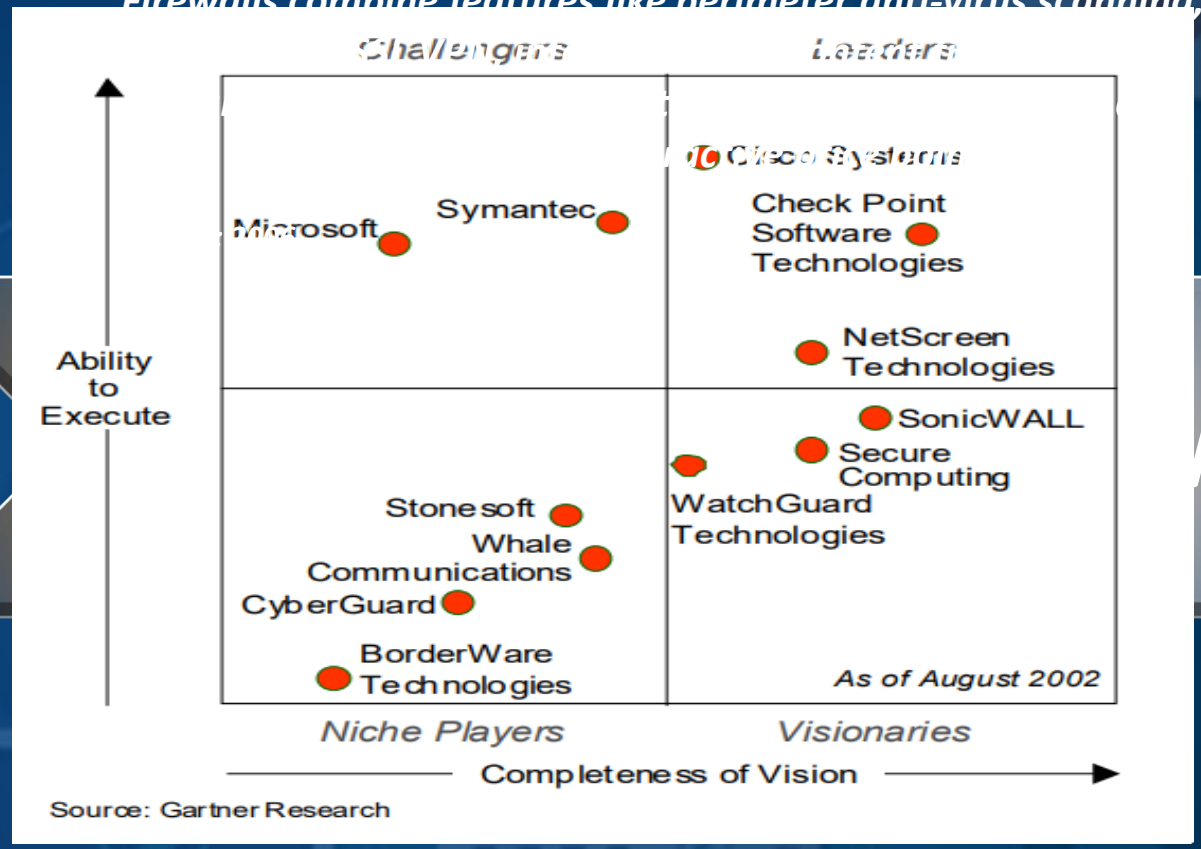
The Role of Firewall

Once a firewall is configured, it filters network traffic, examining packet headings which packets should be forwarded or allowed to enter and which should be stopped.

Gartner: 2002

UTM / NGFW

Firewalls combine features like perimeter anti-virus scanning,




CHALLENGERS
LEADERS
Fortinet
Check Point Software Technologies
Cisco
Sophos
SonicWall
Huawei
Juniper Networks
WatchGuard
Barracuda Networks
Stormshield
Venustech
Hillstone Networks
Untangle
Rohde & Schwarz Cybersecurity
NICHE PLAYERS
VISIONARIES
ABILITY TO EXECUTE
COMPLETENESS OF VISION
As of July 2018
© Gartner, Inc
Source: Gartner (September 2018)

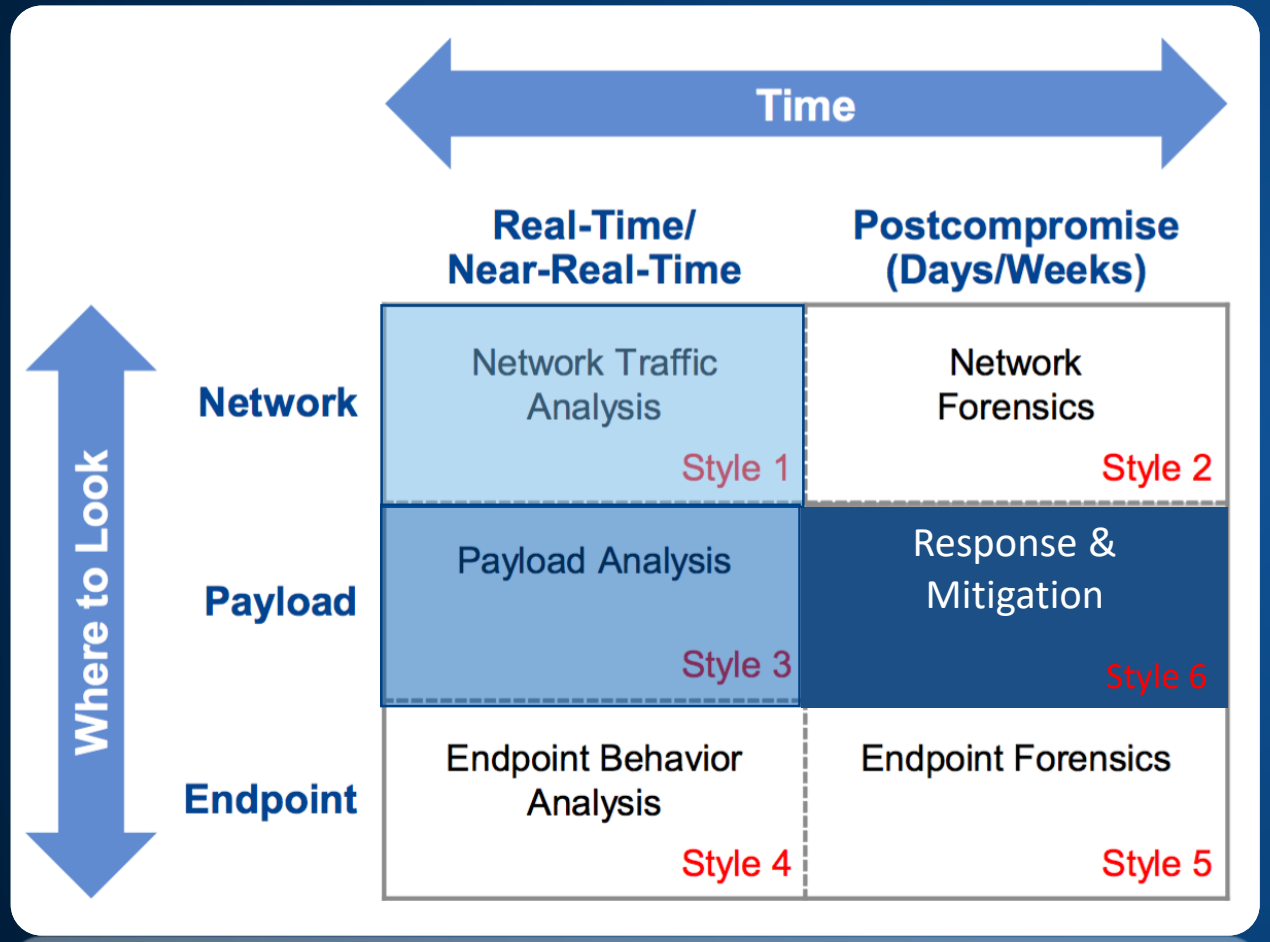

CHALLENGERS
LEADERS
Palo Alto Networks
Cisco
Fortinet
Check Point Software Technologies
Huawei
Sophos
Juniper Networks
Barracuda
Forcepoint
Sangfor
Hillstone
WatchGuard
AhnLab
SonicWall
Stormshield
New H3C Group
NICHE PLAYERS
VISIONARIES
ABILITY TO EXECUTE
COMPLETENESS OF VISION
As of September 2018
© Gartner, Inc
Source: Gartner (October 2018)

UTM

NGFW

Essential Firewall Protection

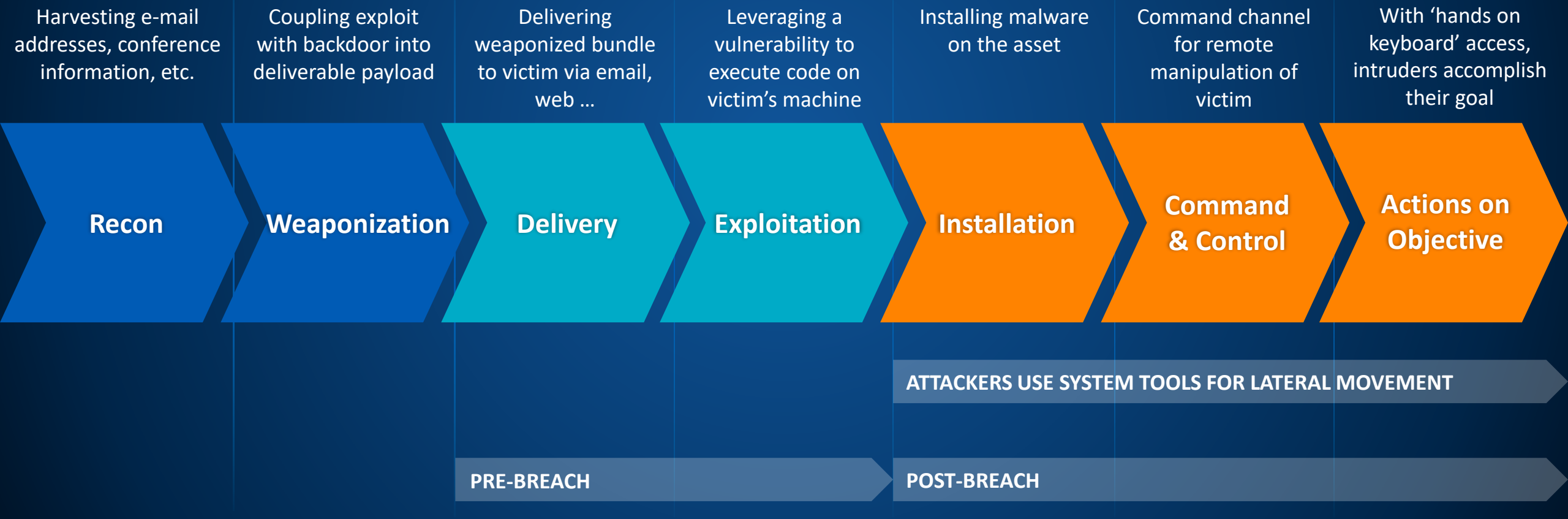
Gartner, Sophos and other experts agree…



- Intrusion Prevention System
- Application Control
- Web Protection & SSL Inspection
- Advanced Threat Protection
- Deep Learning Sandboxing
- Lateral Movement Protection

Threat Lifecycle

Attack Kill Chain



Threat Lifecycle

Attack Kill Chain: what about the firewall?

Recon	Weaponization	Delivery	Exploitation	Installation	Command & Control	Actions on Objective
Harvesting e-mail addresses, conference information, etc.	Coupling exploit with backdoor into deliverable payload	Delivering weaponized bundle to victim via email, web …	Leveraging a vulnerability to execute code on victim's machine	Installing malware on the asset	Command channel for remote manipulation of victim	With 'hands on keyboard' access, intruders accomplish their goal

ATTACKERS USE SYSTEM TOOLS FOR LATERAL MOVEMENT

PRE-BREACH

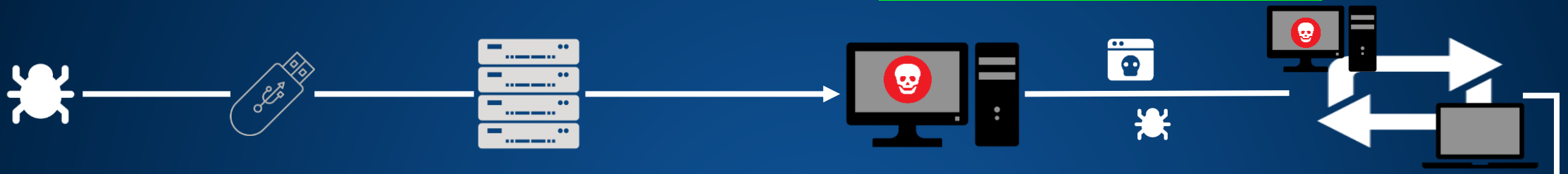
POST-BREACH

SOPHOS DISCOVER 2019

EVOLVE

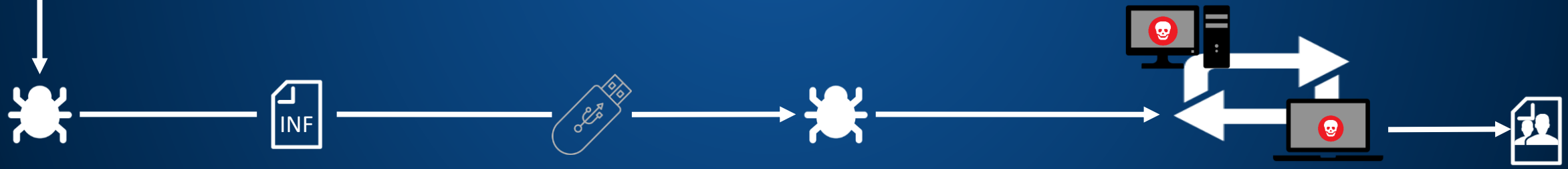
Historical Attacks..

How the Attack Has Evolved.. Conficker Worm in 2008-09..



WORM_DOWNAD.AD arrives via removable drives, network shares or other malware

It sends exploit packets for CVE MS08-067 to machines on the network and random targets on the internet



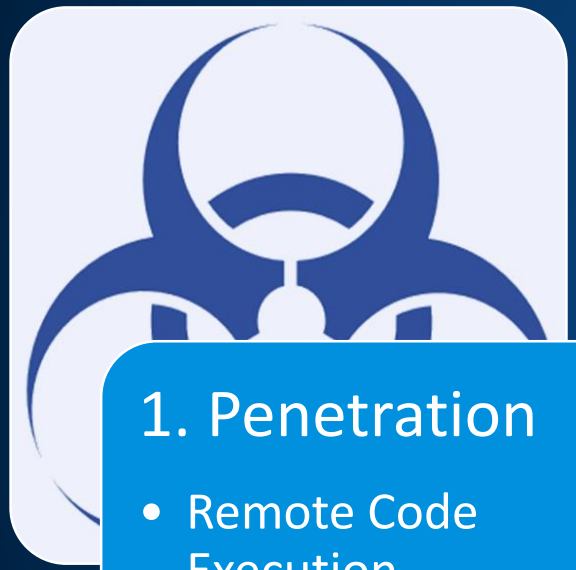
It drops a copy of itself and an obfuscated autorun.inf file into the Recycle Bin of all available removable and network drives

It enumerates and tries to log into the available servers on the network via a dictionary attack and uses it to gather a list of user accounts ; if successful, it drops a copy of itself

https://en.wikipedia.org/wiki/Conficker


10 Years Later

WannaCry Attack Stages



1. Penetration

- Remote Code Execution
- Ring 0
- Propagation

2. Deployment

- Unpacking
- Environment Preparation
- Payload Execution

3. Encryption

- Encrypt Documents
- Delete Shadow Copies and Backups
- Display Ransom Notes

Stuxnet

"The NSA and Israel wrote Stuxnet together"

Edward Snowden, 2010

WannaCry

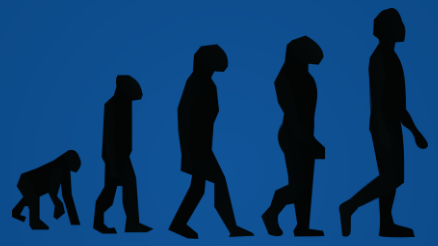
"Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service"

WannaCry ransomware message, 2017

EMOTET

"Amongst the most costly and destructive threats to U.S. businesses right now"

U.S. Department for Homeland Security, 2018

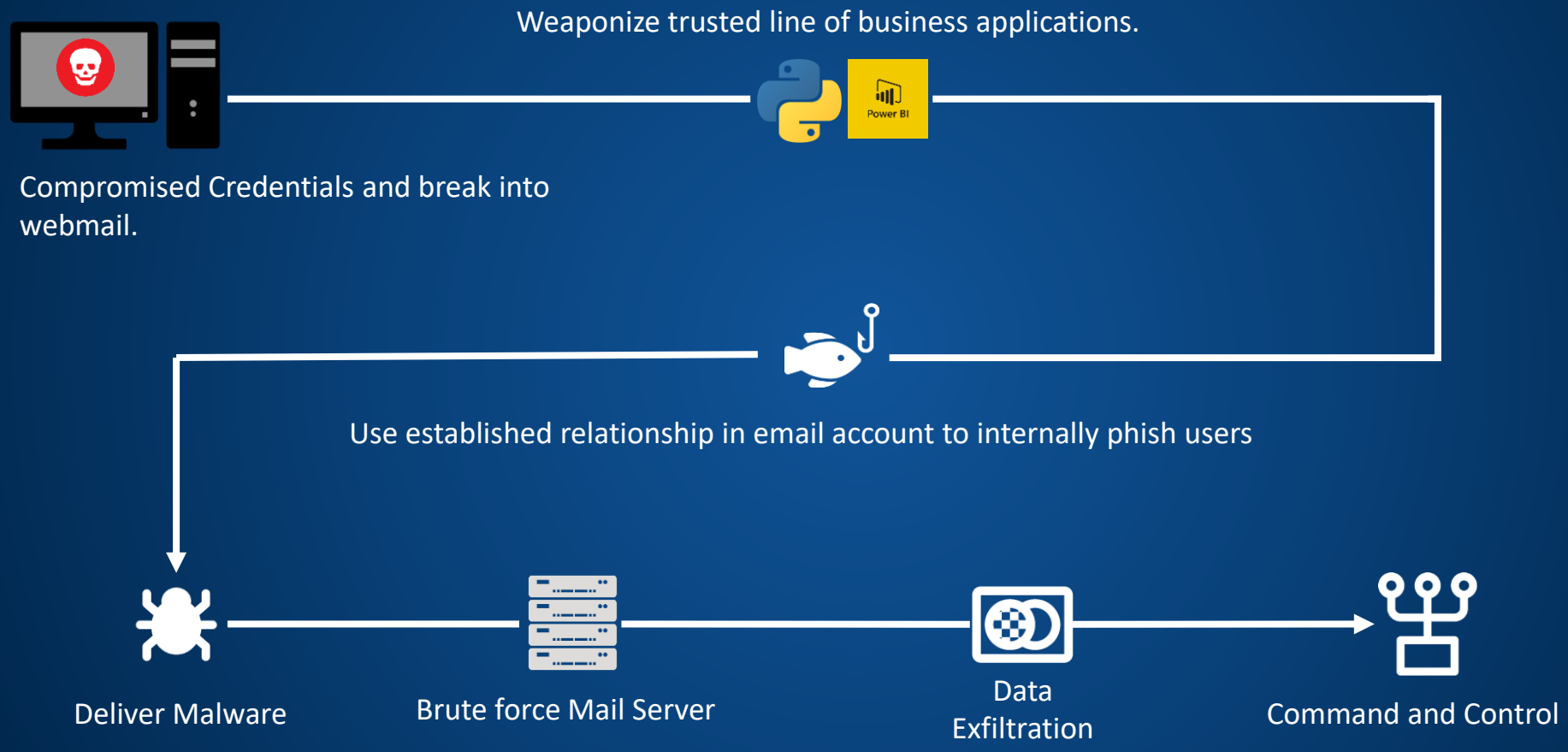


Fast spreading worm targeting known vulnerability

State sponsored sophisticated attacks, supply chain compromises, organized crimes

Protection Capabilities Now (DEMO)

Multi-Staged Attack



SOPHOS DISCOVER 2019

EVOLVE

The Attacker

Multi-Stage Attacks

1. *Delivery and Instruction*

Adversary Options

Phishing

Malicious URL

Command & Control

Code Cave

Weaponized Doc

Layered Defenses

Phishing Training

ATP

URL Filtering

PUA Detection

IPS

Sandboxing

Infection of the host

Multi-Stage Attacks

2. *Exploit and Execution*

Adversary Options

Credential Theft

Privilege Escalation

Malicious Executable

Application Exploit

Layered Defenses

WAF / 2 FA

VPN / RED

IPS

SyncApps

Heartbeat

Lateral Movement Prevention

Responding with Synchronised Security

Multi-Stage Attacks

3. *Exfiltration*

Adversary Options

Data Exfiltration

Ransomware

Credential Dump

Further Attacks

Layered Defenses

ATP

CASB

Custom IPS

Heartbeat

Lateral Movement Prevention

Layered Approach

1. *Delivery and Instruction*


Phishing

Malicious URL


Command & Control


Code Cave

Weaponized Doc

- PUA Detection
- URL Filtering
- ATP
- Sandboxing
- Phishing Training
- IPS

2. *Exploit and Execution*


Credential Theft


Privilege Escalation

Malicious Executable

Application Exploit

- WAF
- IPS
- Heartbeat
- VPN / RED
- SyncApps
- Lateral Movement Prevention

3. *Exfil*


Data Exfiltration


Ransomware


Credential Dump


Further Attacks

- ATP
- Custom IPS
- Heartbeat
- CASB
- Lateral Movement Prevention

Sophos Central Management of XG Firewall

A single pane of glass for managing all your IT security

Management

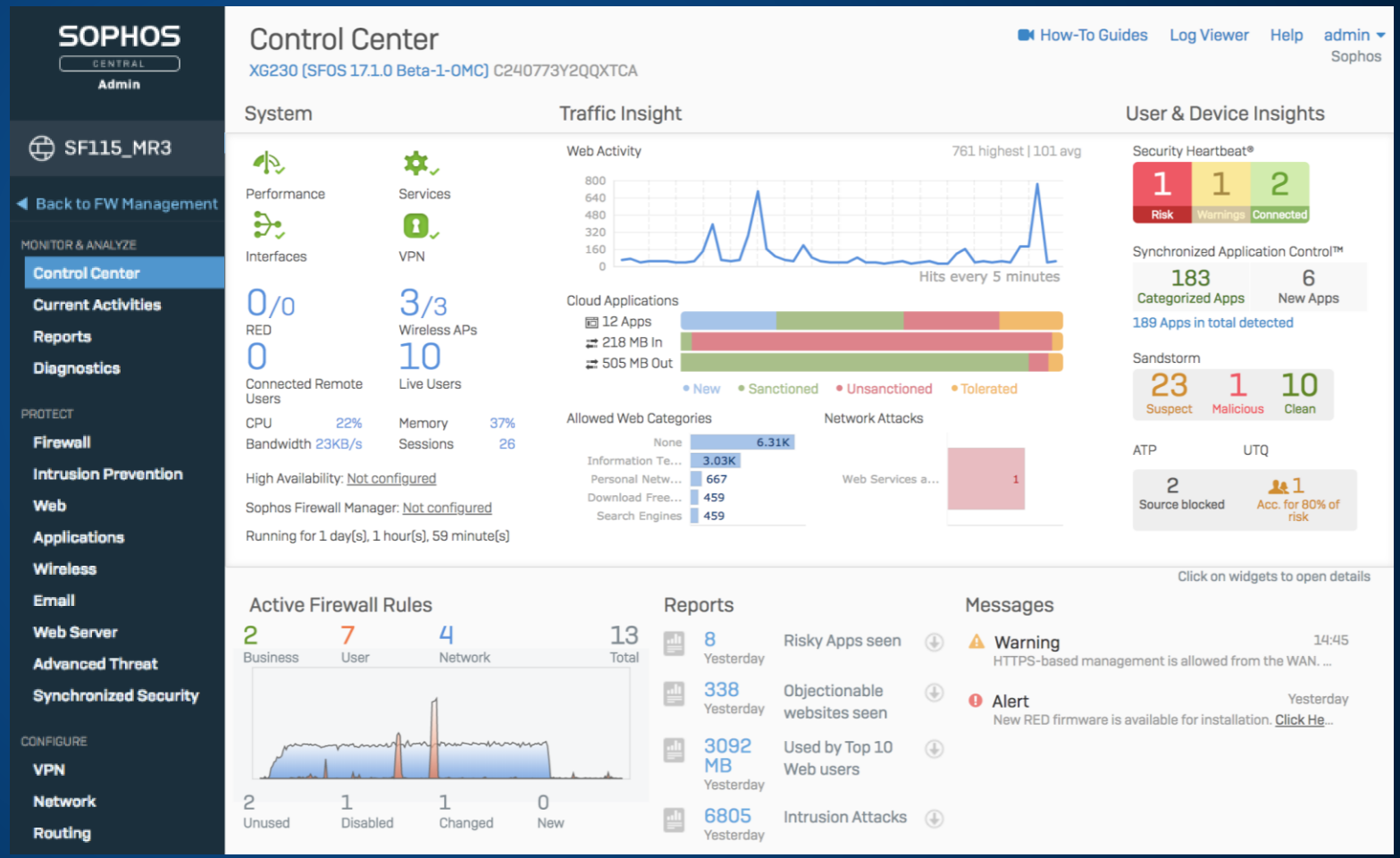
Zero-touch setup of new firewalls, full SSO device management, store/maintain backups, multi-device firmware updates

Visibility

Complete visibility of network security across your enterprise

Dashboard

Alerting and status for availability, licensing, performance, and security



SOPHOS

Cybersecurity made simple.