Sophos Evolve

Walter Narisoni
Sales Engineer Manager

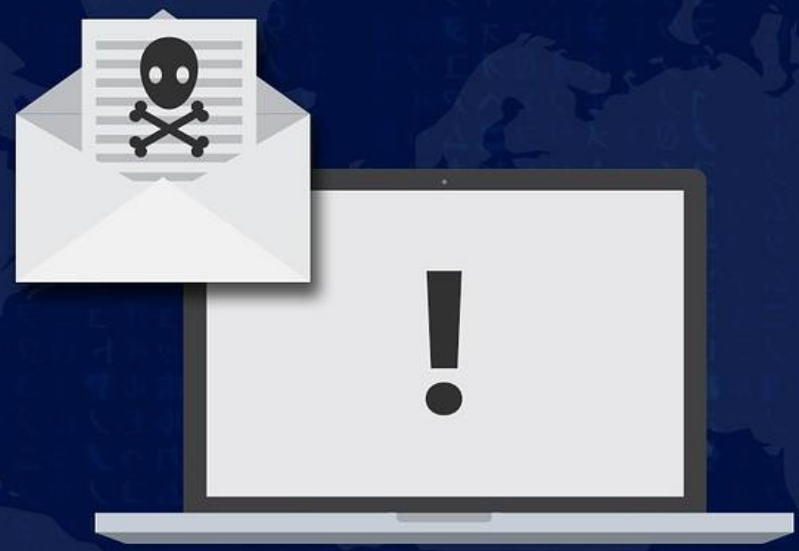
SOPHOS DISCOVER 2019
EVOLVE

500,000

new malware per day

75%

only seen once



SOPHOS labs

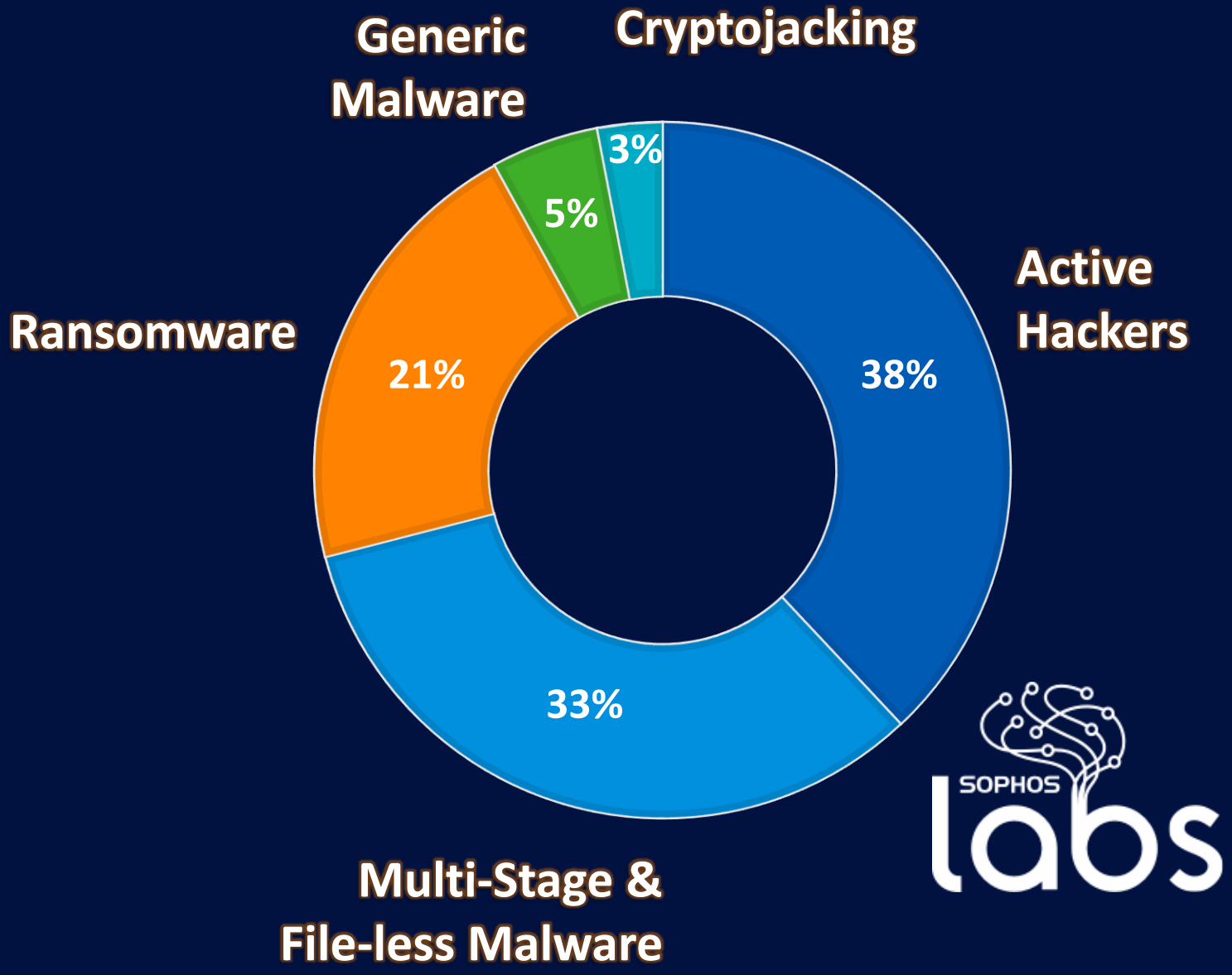
53%

orgs hit by ransomware

*Source: State of Endpoint Protection Study 2018

1/3

paid the ransom



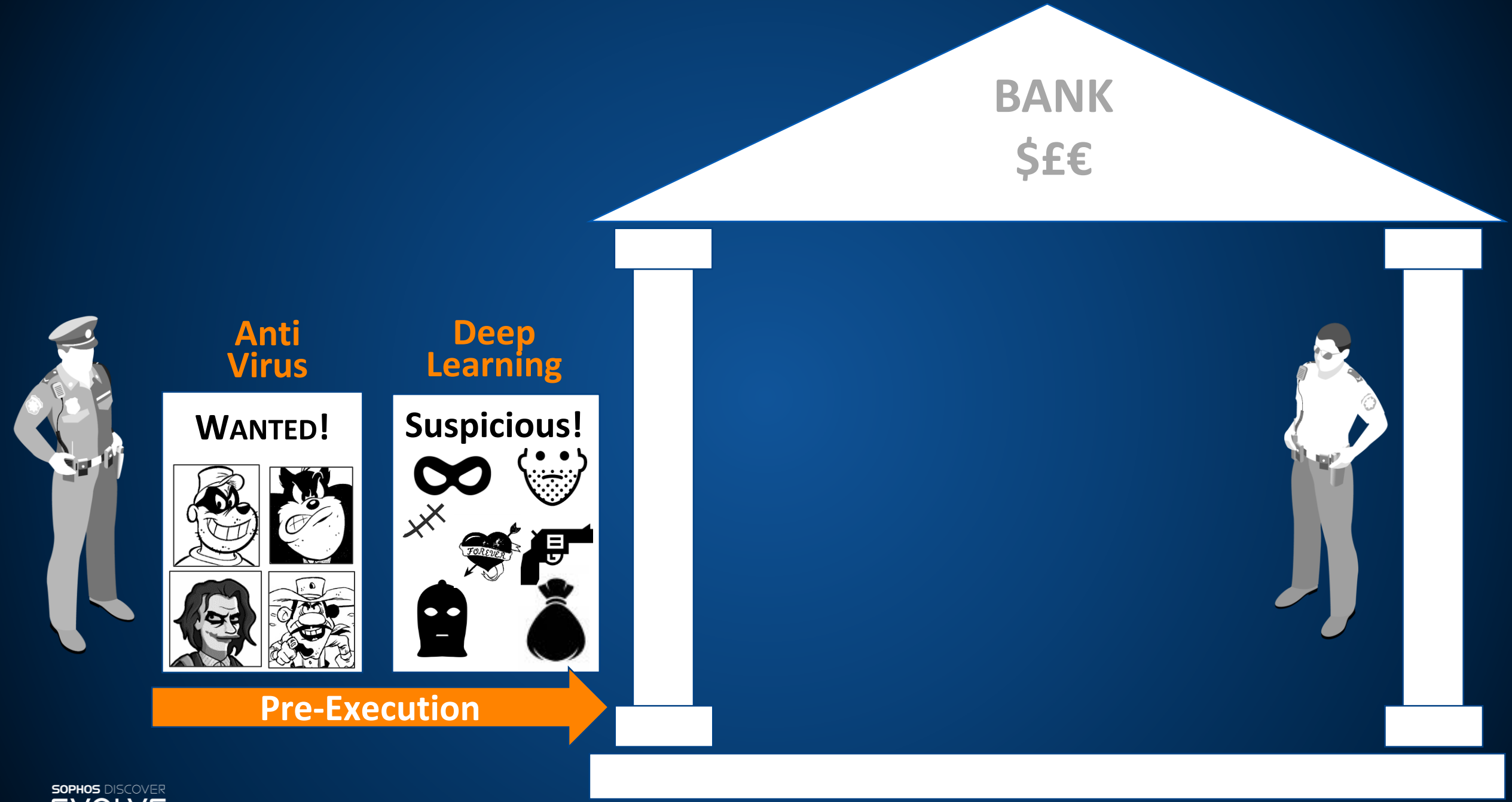
SOPHOS labs

Vulnerabilities Waiting to Be Exploited

Software Vulnerabilities Reported by Year

SOPHOS DISCOVER EVOLVE

Source information NIST National Vulnerability Database as of Feb 14 2019
https://nvd.nist.gov/vuln-metrics/visualizations/cvss-severity-distribution-over-time


BANK
$£€
Anti Virus
Deep Learning
WANTED!
Suspicious!
FOREVER
Pre-Execution

BANK

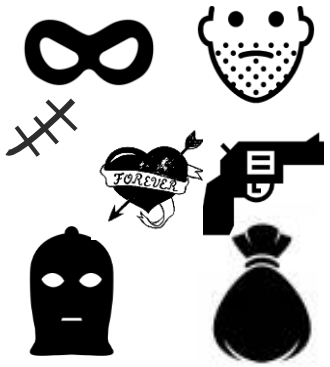
$£€

Anti Virus

WANTED!

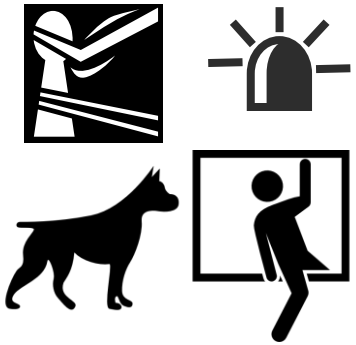
Deep Learning

Suspicious!



Exploit Prevention

Techniques!



Behavior Monitoring

Actions!

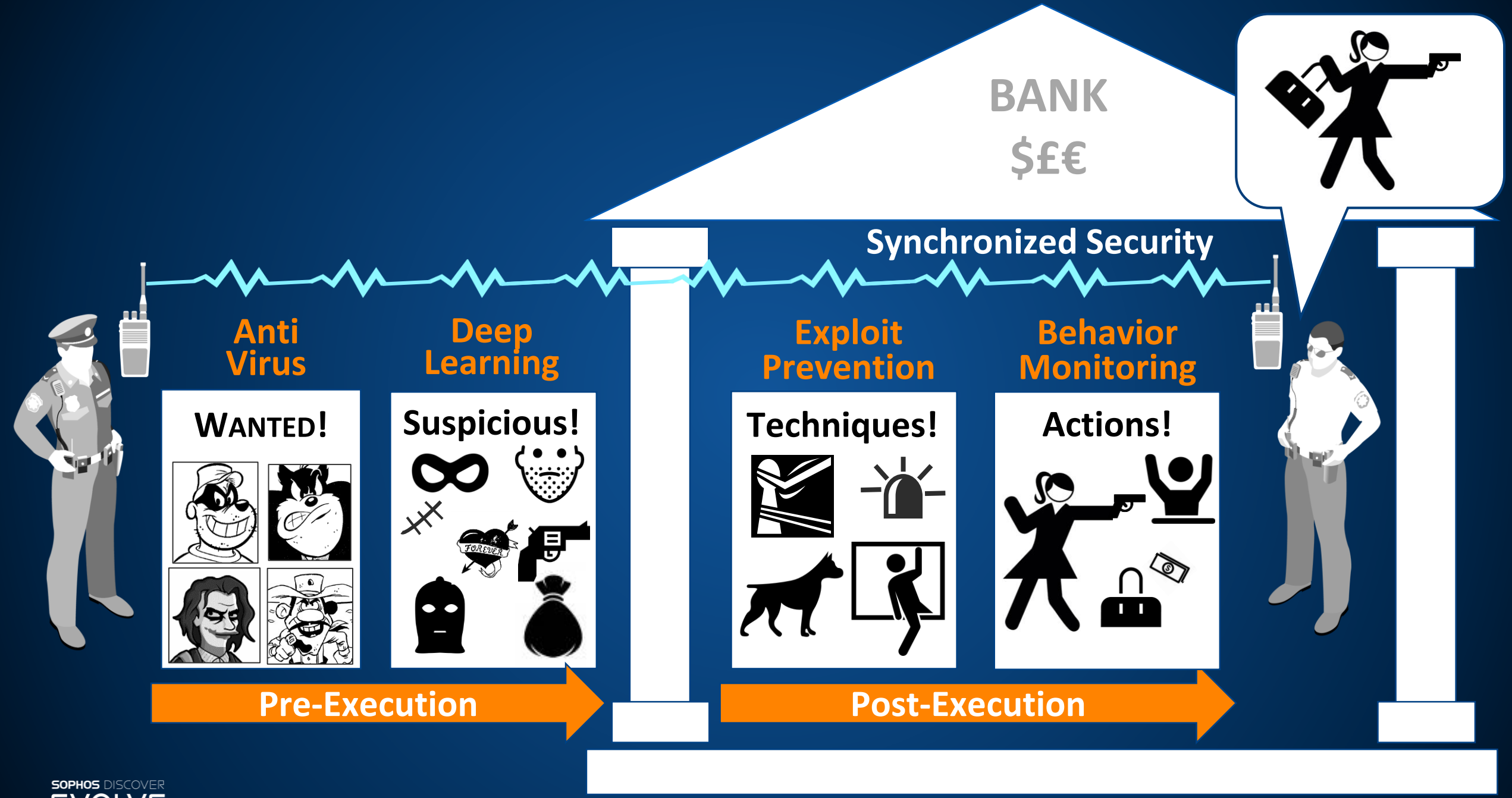
Pre-Execution

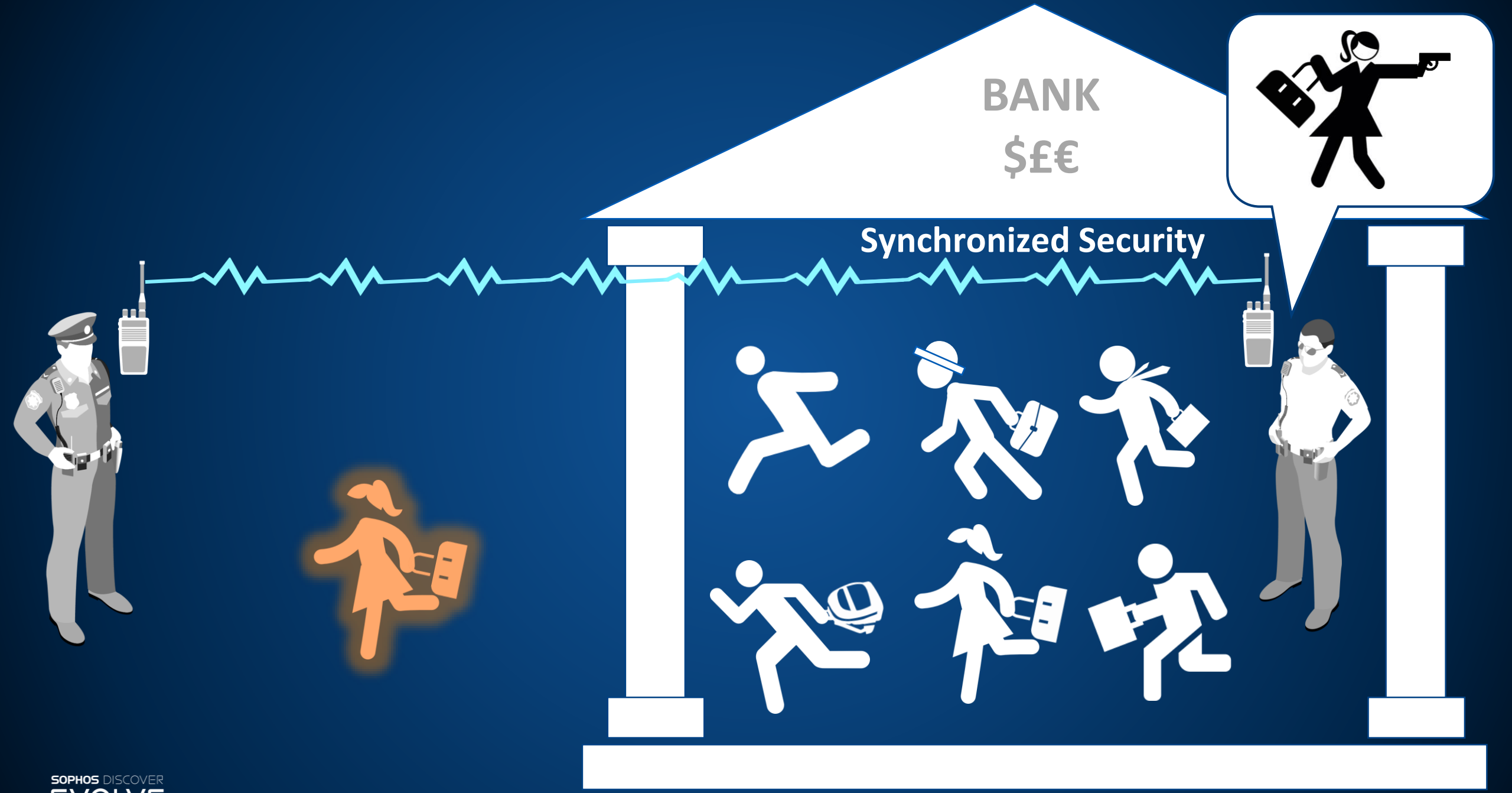
Post-Execution

THERE IS ALWAYS SOMEONE

WILLING TO DO IT CHEAPER

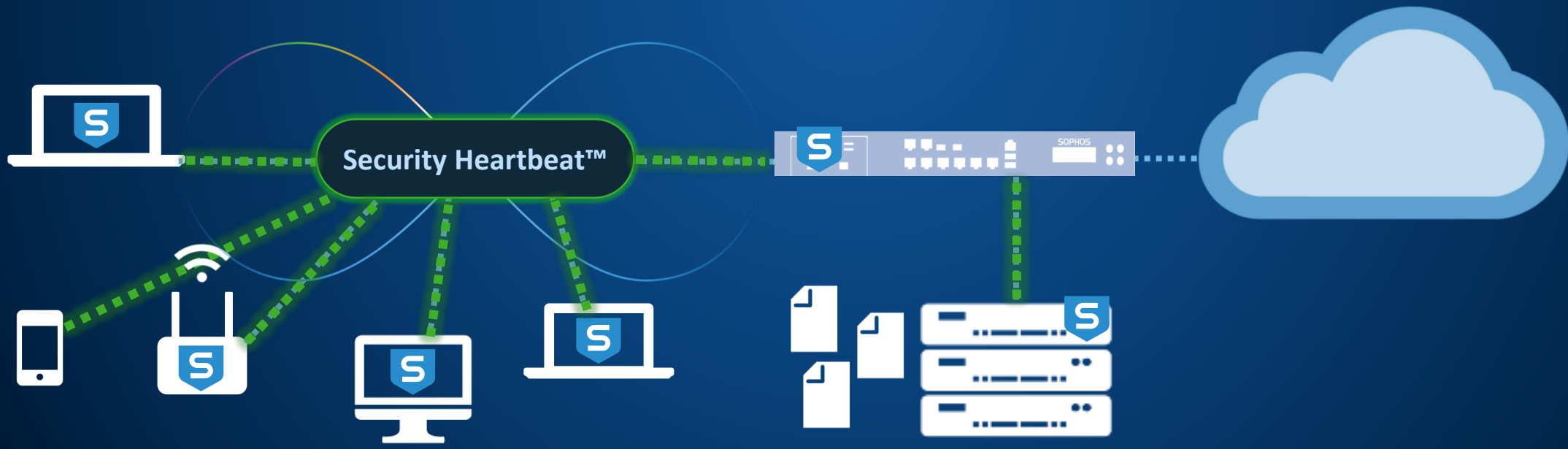
Best protection and lowest TCO in the industry


BANK
$£€
Synchronized Security
Anti Virus
Deep Learning
Exploit Prevention
Behavior Monitoring
WANTED!
Suspicious!
Techniques!
Actions!
FOREVER
Pre-Execution
Post-Execution


BANK
$£€
Synchronized Security

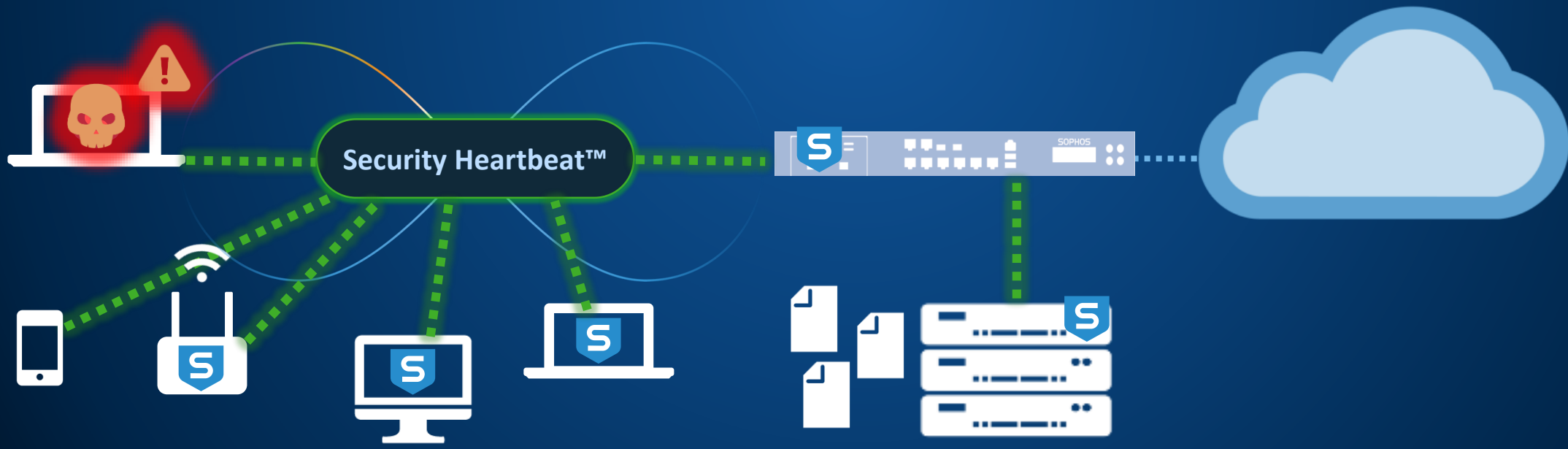
Reacting to threats with Synchronized Security

Clients, Servers, Mobile Devices, Access Points and Firewall communicate with each other using the Security Heartbeat



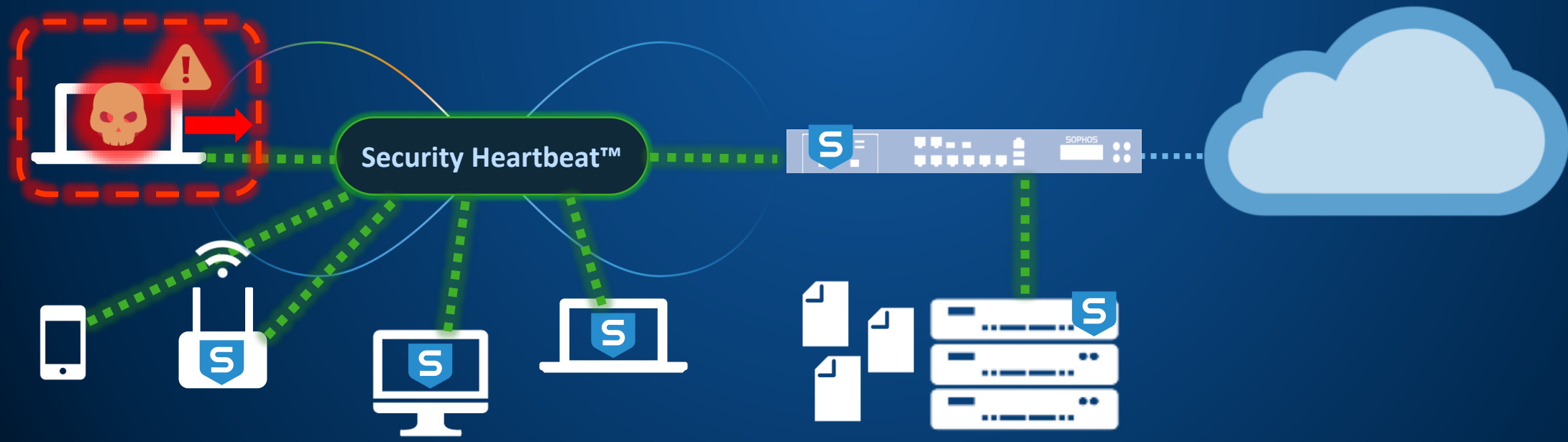
Reacting to threats with Synchronized Security

In case of a threat all components are informed and react automatically



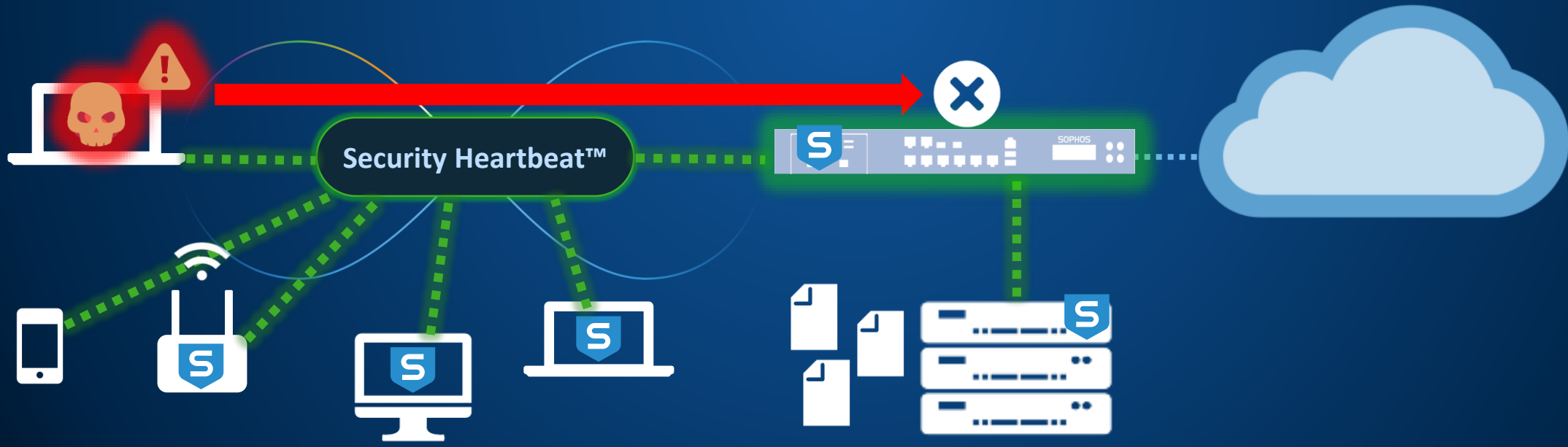
Reacting to threats with Synchronized Security

The client isolates himself..



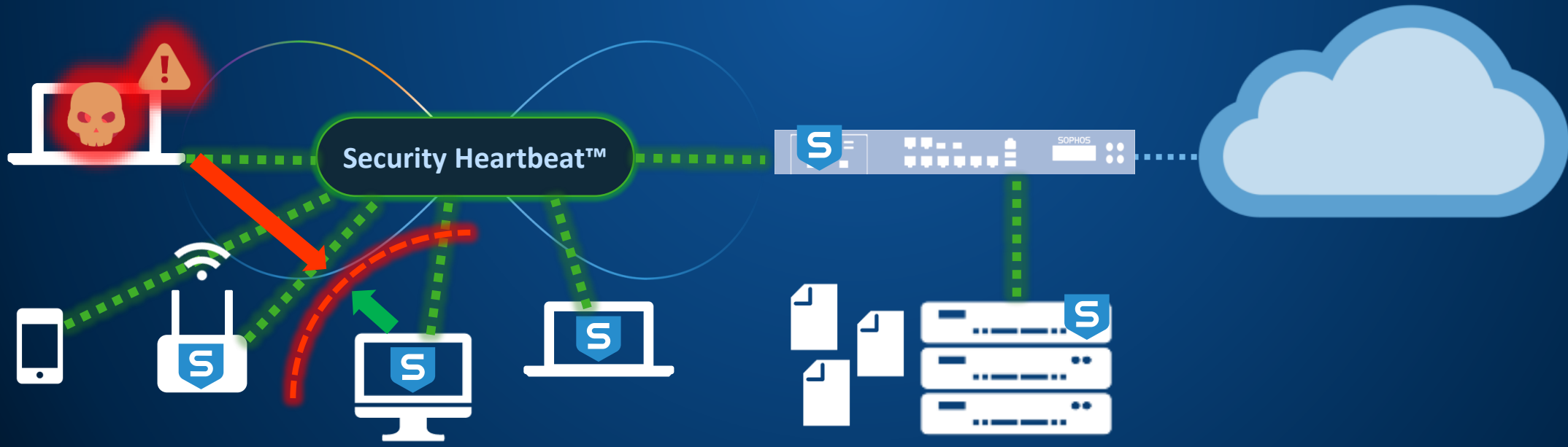
Reacting to threats with Synchronized Security

The Firewall quarantines the client and prevents communication to other network segments and the Internet



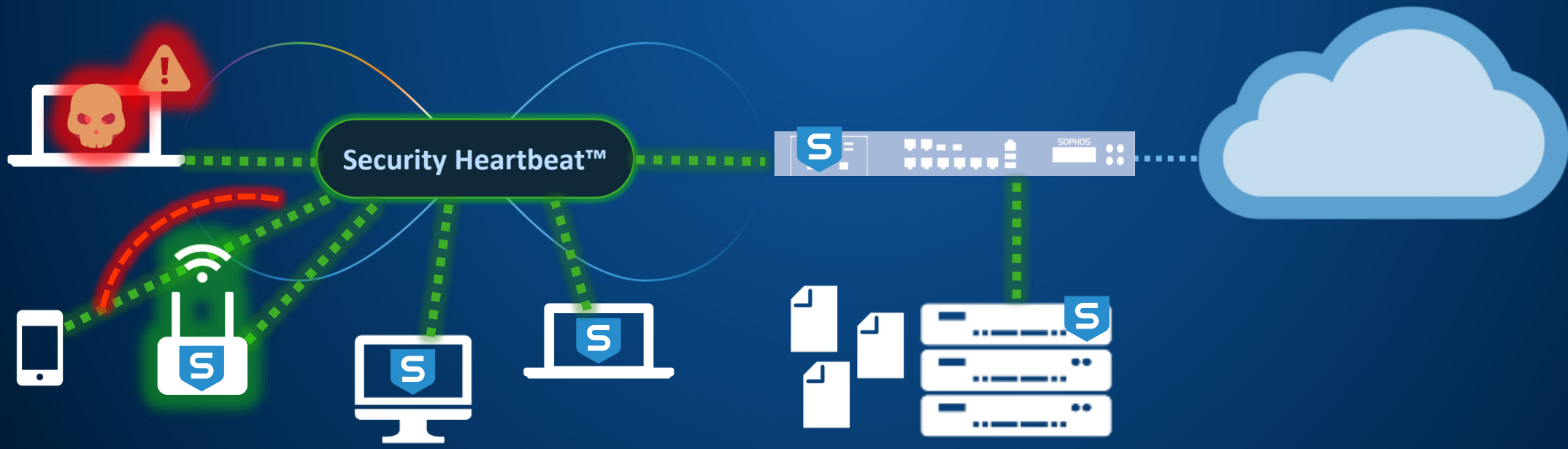
Reacting to threats with Synchronized Security

Clients in the same network segment do not communicate anymore with the infected client



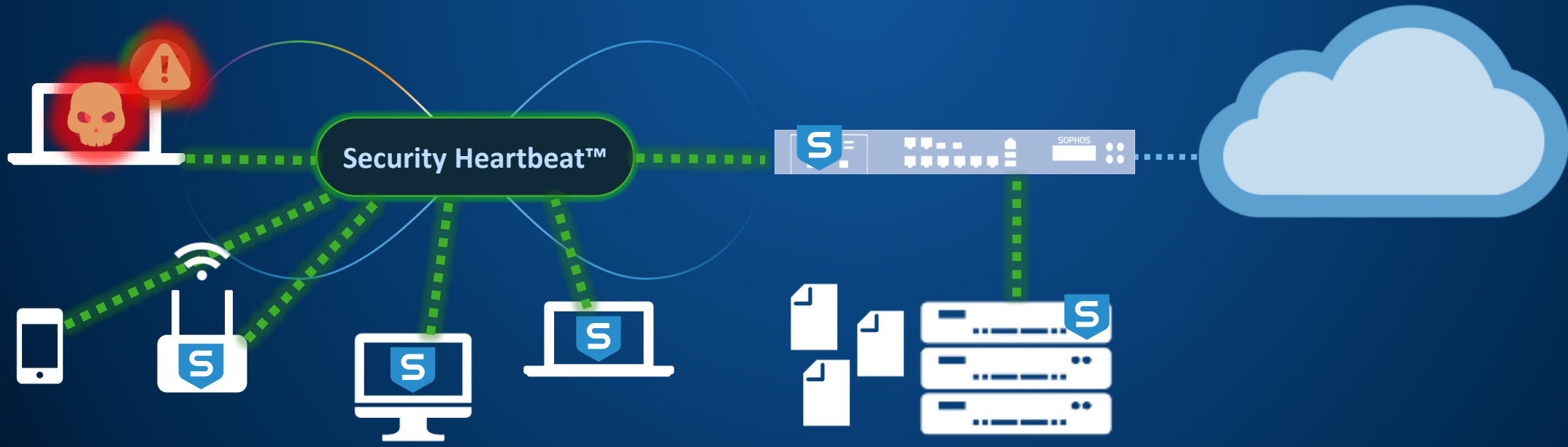
Reacting to threats with Synchronized Security

The WIFI Access Point does not allow the infected client to connect to the wireless network



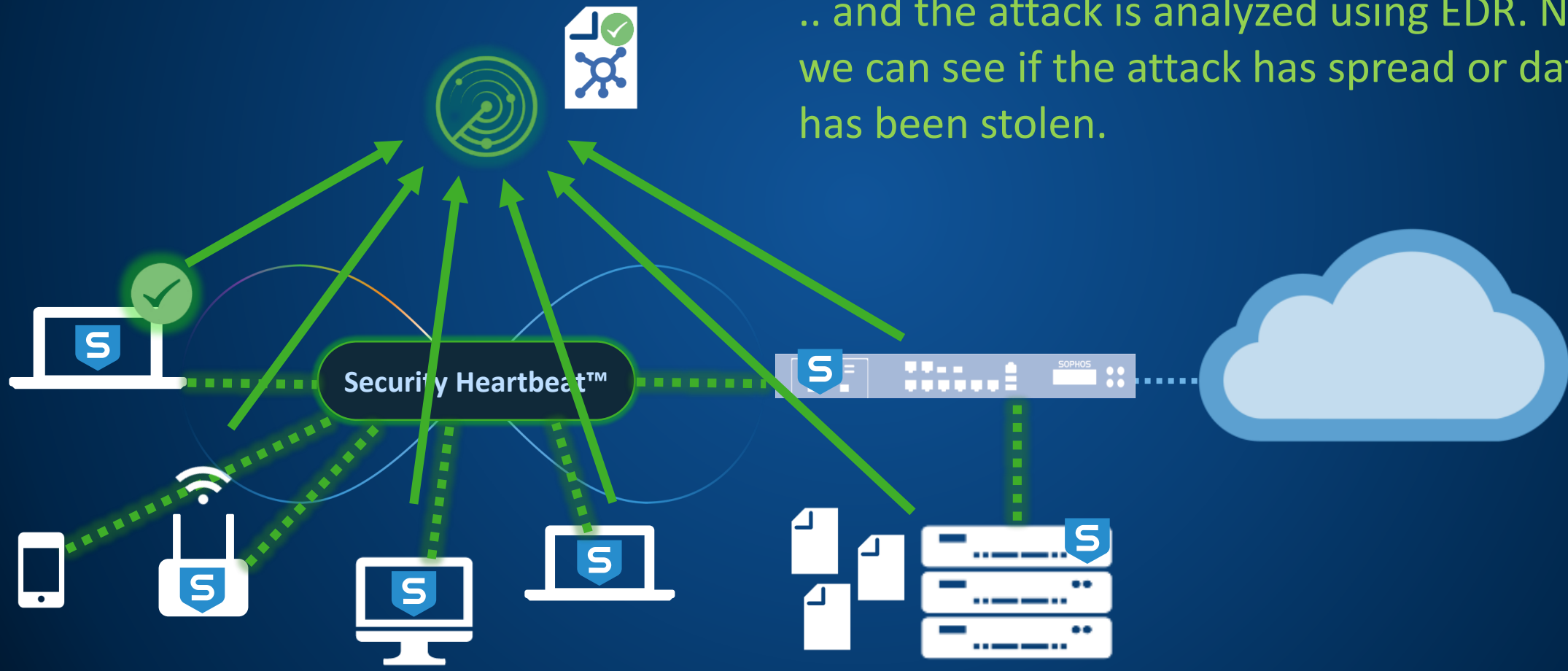
Reacting to threats with Synchronized Security

..the threat is being cleaned up..

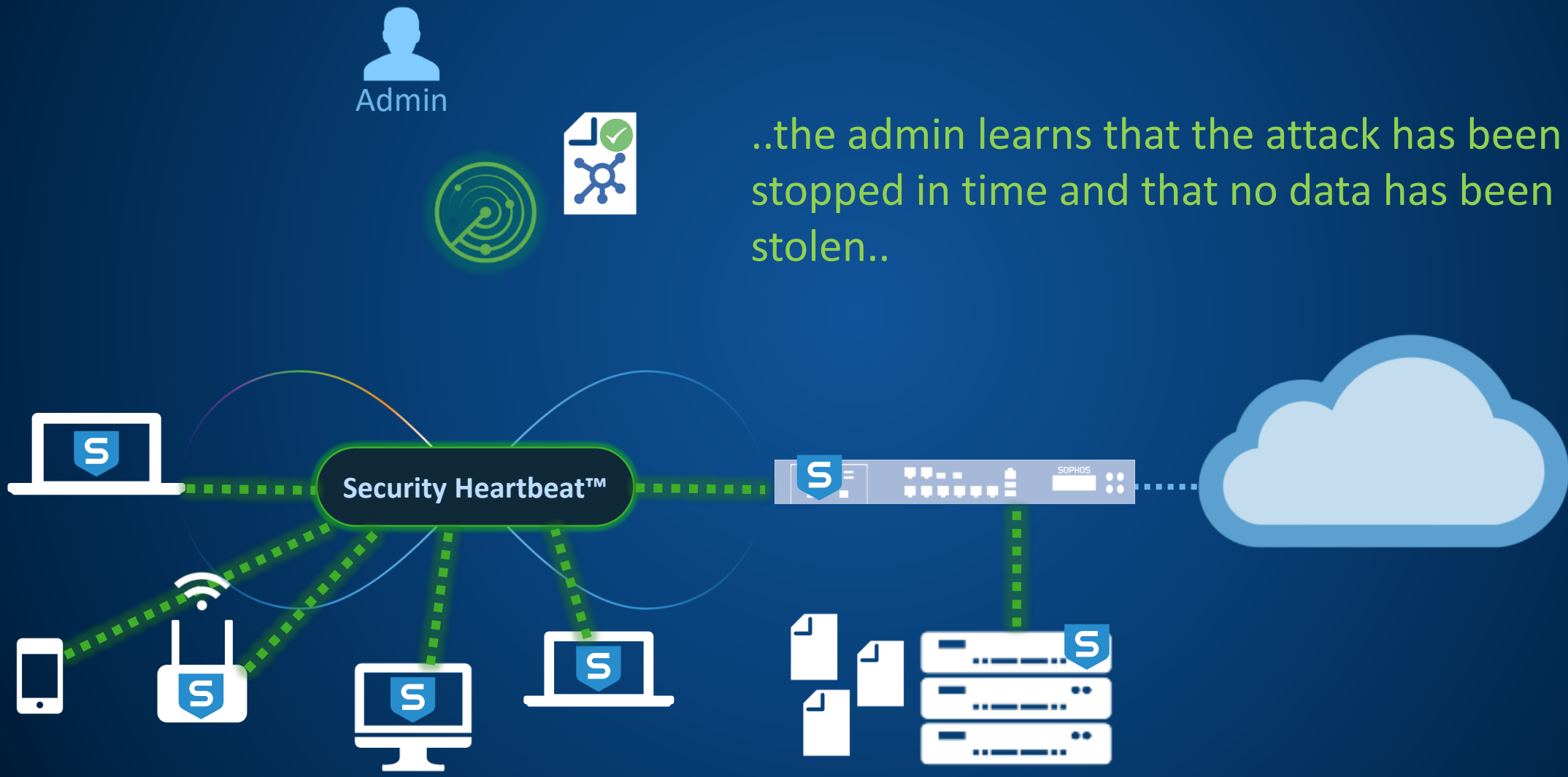


Reacting to threats with Synchronized Security

.. and the attack is analyzed using EDR. Now we can see if the attack has spread or data has been stolen.



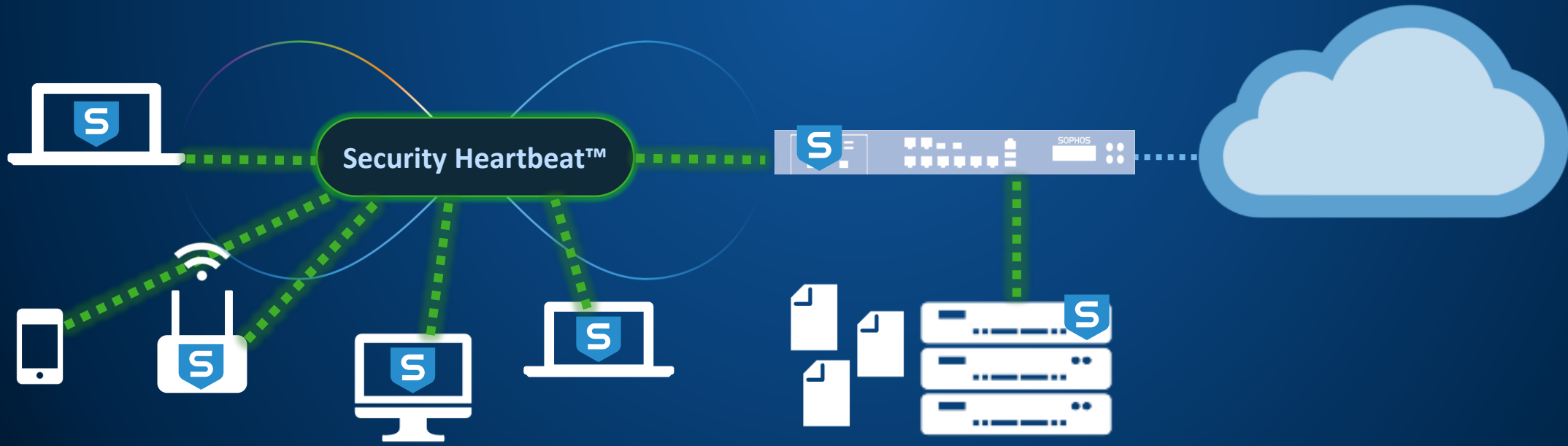
Reacting to threats with Synchronized Security



..the admin learns that the attack has been stopped in time and that no data has been stolen..

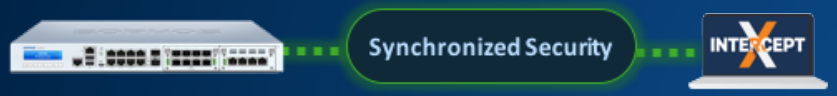
Reacting to threats with Synchronized Security

..and the CEO is happy that the IT works so perfectly.



Three Winning XG Sales Plays

1. Aggressive Firewall Replacement



Who to target… and how…

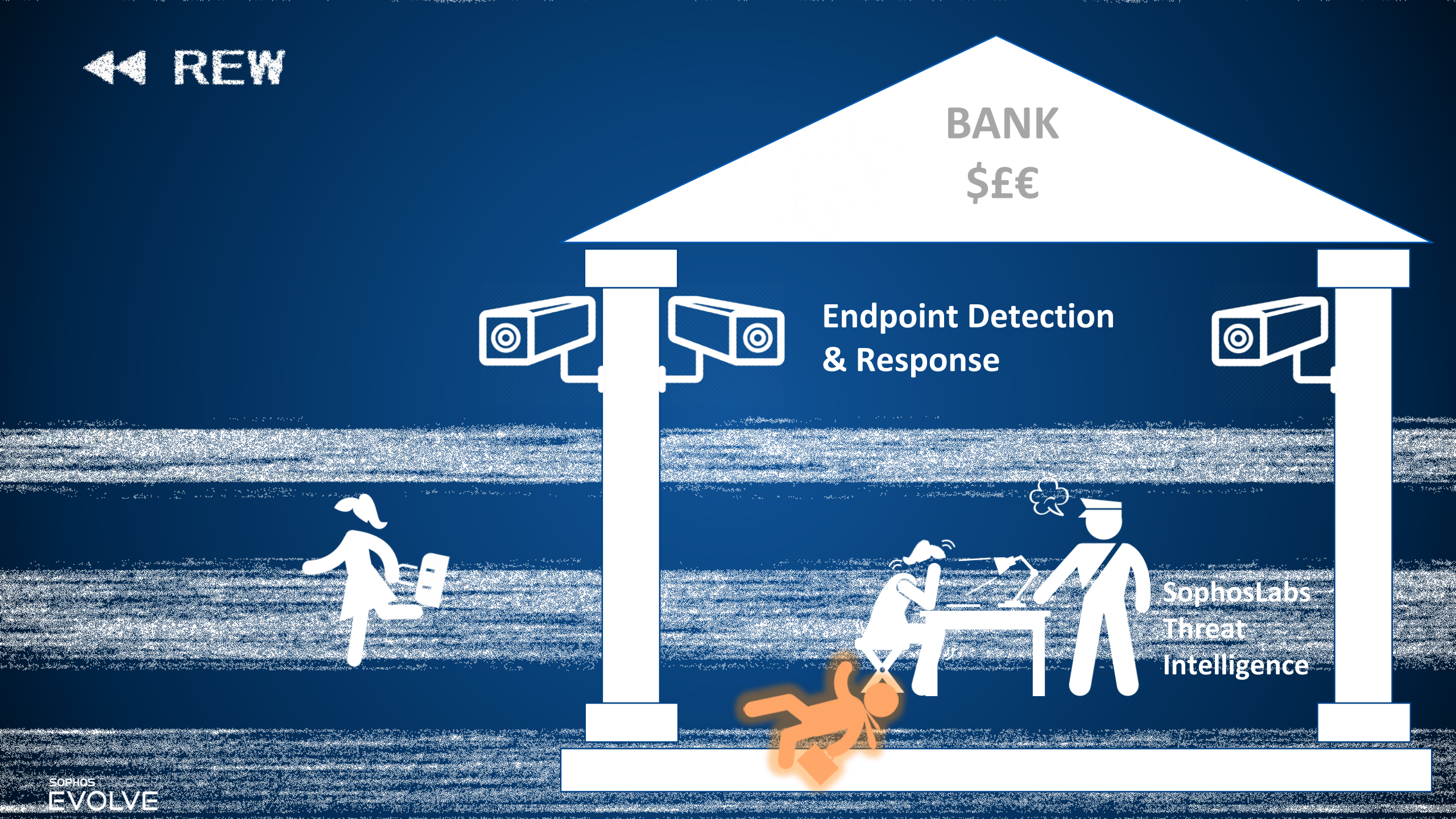
- ✓ Replace SonicWALL, WatchGuard, and Legacy UTM
- ✓ Primary <100 Users , Secondary <500 Users,
- ✓ UTM Deployments, Lite Campus Edge (NGFW)
- ✓ Lead with Industry Accolades, Key Differentiators, Sync Security

2. Opportunistically pursue Pragmatic Enterprise

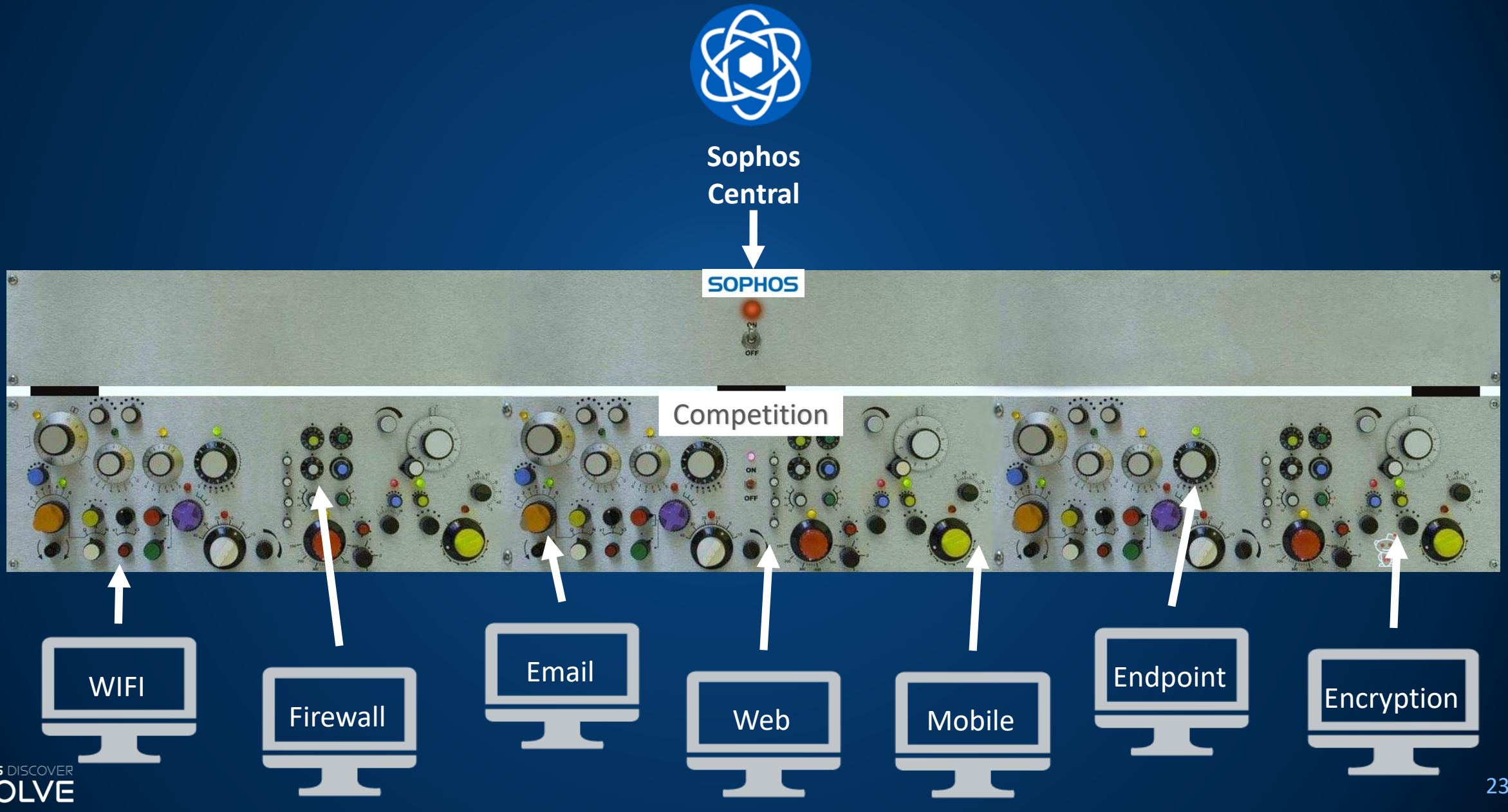
- ✓ Inline Deployment (for Synchronized Security)
- ✓ Opportunistically pursue Pragmatic Enterprise, SE validation needed
- ✓ Cisco/PAN/Checkpoint/Fortinet
- ✓ Lead with enabling Synchronized Security
- ✓ Be prepared to pivot between firewall replacement and inline deployment

3. Cross-Sell to Intercept X Install Base

- ✓ Discover Mode (off to the side) deployment, no impact or risk to network
- ✓ Enables Synchronized Security reporting and visibility only
- ✓ Piggyback off of huge Intercept X demand/growth (Central EP Install base)
- ✓ Get into the rack


REW
BANK
$£€
Endpoint Detection
& Response
SophosLabs
Threat
Intelligence

The most comprehensive cloud platform



Evolution of Synchronized Security with Cloud

Our vision to provide the best protection and visibility, wherever your data resides

DISCOVERY

Assets in AWS, Azure, Google Cloud

COMPLIANCE

Reporting and adherence based on behaviors and best practices

RESPONSE

Instant remediation and incident response

Sophos Synchronized Security

SOPHOS DISCOVER 2019

EVOLVE