



# A new Security Architecture : from protection to integrated and automated detection and response

Patrick Commers

Business Development Manager Belux - MESH & SASE

Fortinet

# Cybersecurity Challenges

## Work From Anywhere

The shift to remote work is expected to persist even after the pandemic. **52%** of CIOs expect work from home to increase in 2021.

Gartner – Top Priorities for IT Leadership 2021

## Network Edge Explosion

By 2025, **70%** of digital business initiatives will require I&O leaders to report on the business metrics from digital experience, up from less than **15% today**.

Gartner Market Guide for Digital Experience Monitoring, August 2020 ID G00724605

## Application Journey

By year-end 2023, **50%** of large enterprises will have a documented edge computing strategy, compared to less than **5%** in 2020.

Building an Edge Computing Strategy Gartner, published 3, September 2021

## Sophisticated Attacks

**36%** of organizations state the growing sophistication of the threat landscape is the top challenge in preventing ransomware attacks.

Fortinet – Ransomware survey 2021

## Operational Technology Connectivity

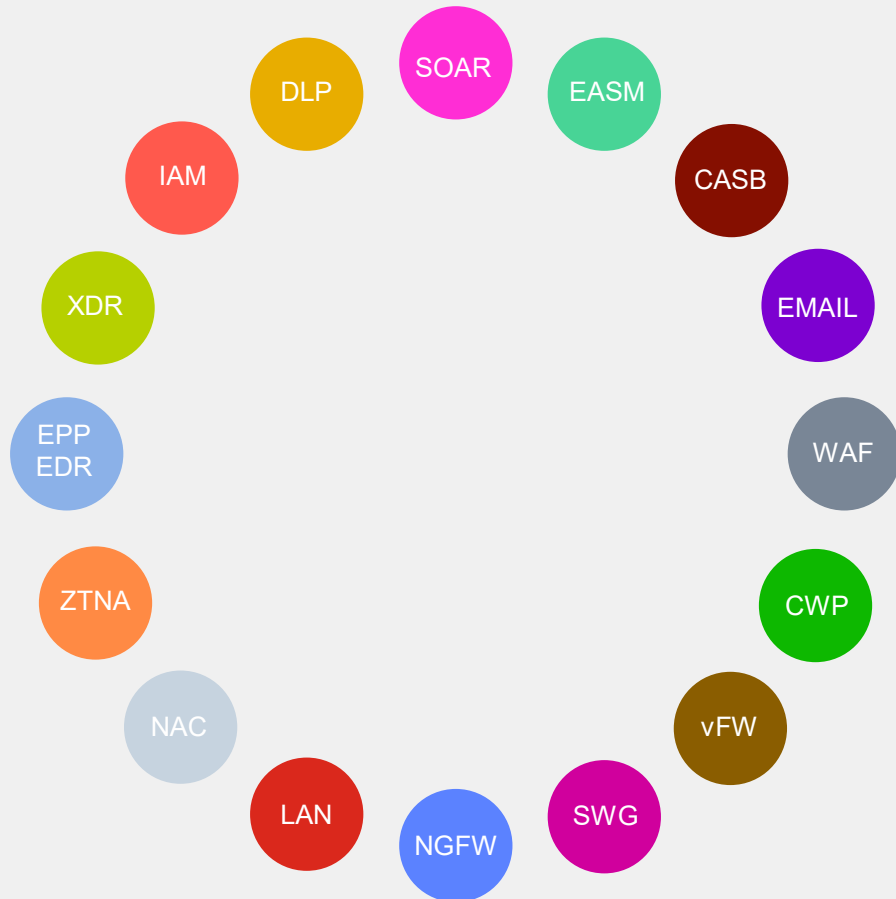
**42%** indicate that their control systems had direct connectivity to the internet up from **12%** in 2019.

SANS 2021 Survey: OT/ICS Cybersecurity, published August 2021



# Consolidation of Security Point Product Vendors

## Cybersecurity Point Products

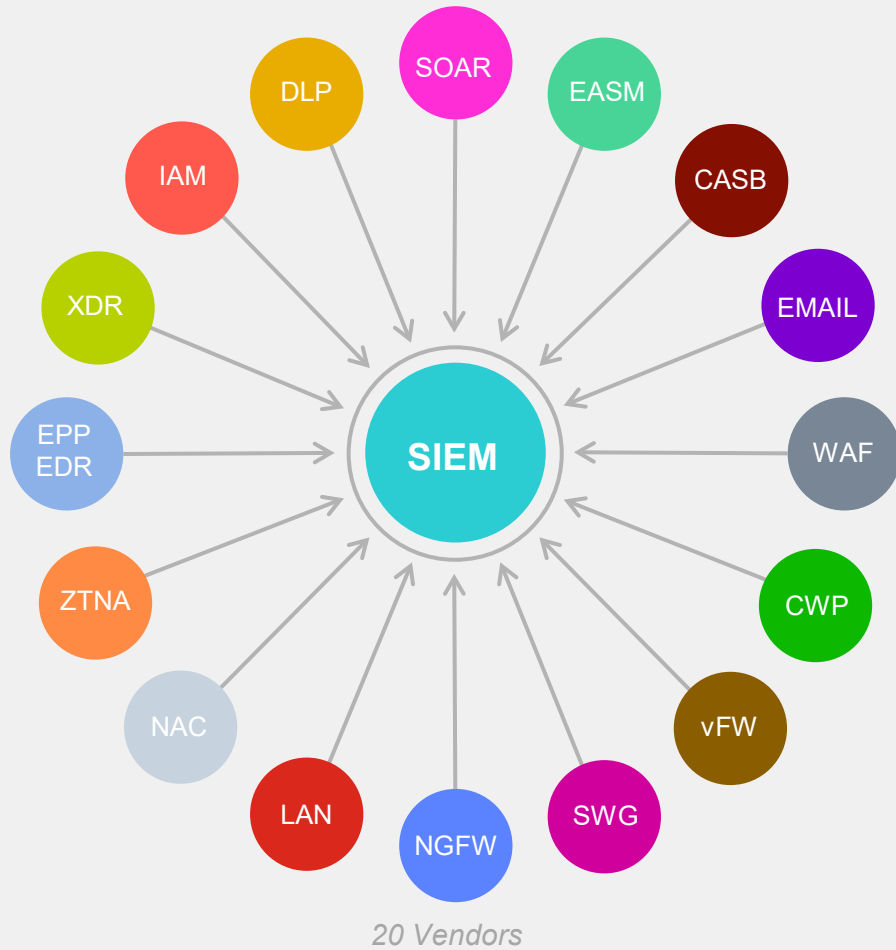


20 Vendors



# Consolidation of Security Point Product Vendors

## Cybersecurity Point Products



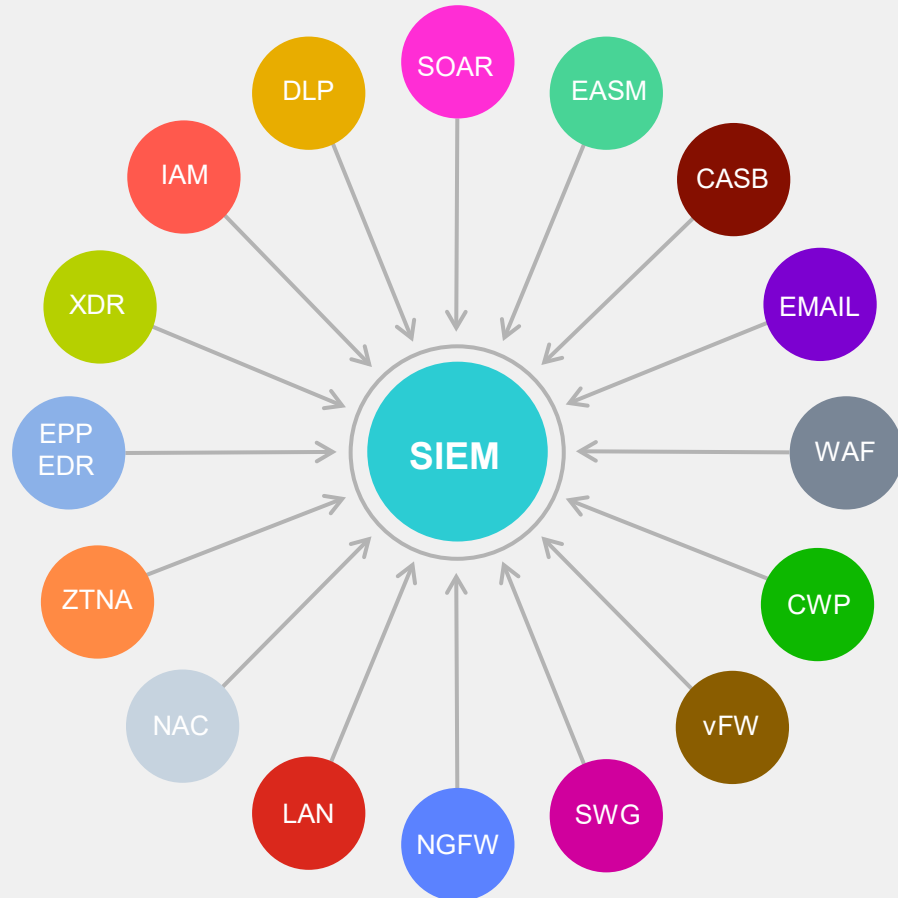
20 Vendors



# Consolidation of Security Point Product Vendors

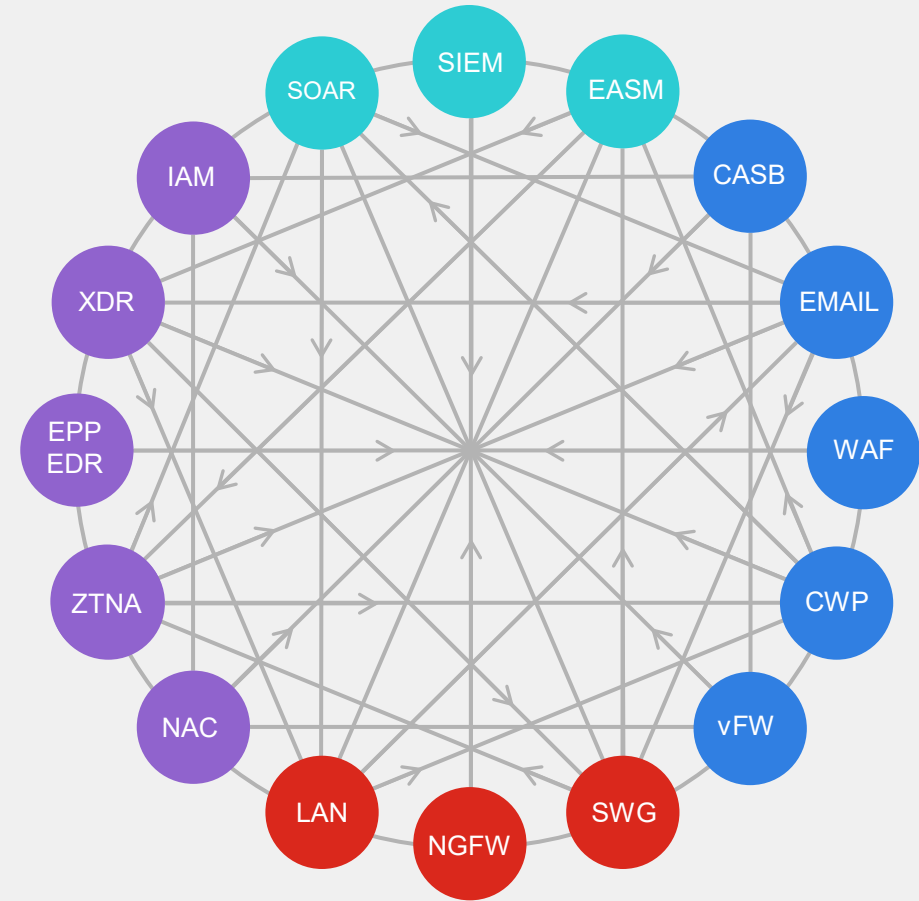
Gartner Cybersecurity MESH Architecture (CMSA)

Cybersecurity Point Products



20 Vendors

Cybersecurity Platform Approach



4-6 Platforms



# Security Is NOT Straightforward

Security is Technology *Plus* Psychology

Where is the Attacker Along The Cyber Kill Chain? And How Do We Stop Him?

PRE-ATT&CK

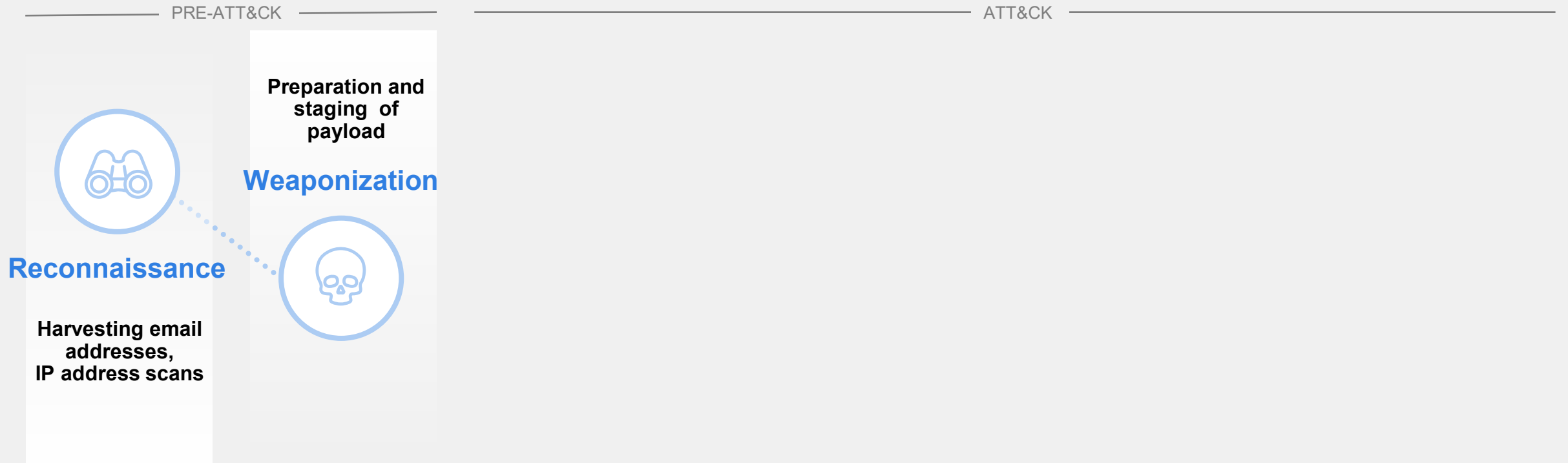
ATT&CK



# But Security Is NOT Straightforward

Security is Technology *Plus* Psychology

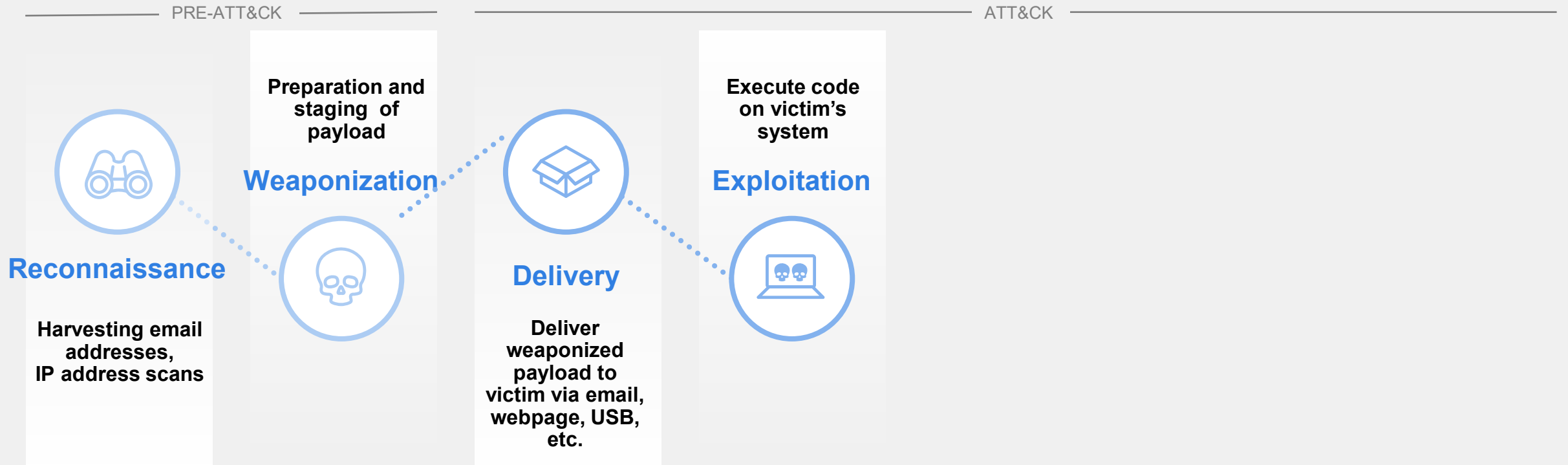
Where is the Attacker Along The Cyber Kill Chain? And How Do We Stop Him?



# But Security Is NOT Straightforward

Security is Technology *Plus* Psychology

Where is the Attacker Along The Cyber Kill Chain? And How Do We Stop Him?

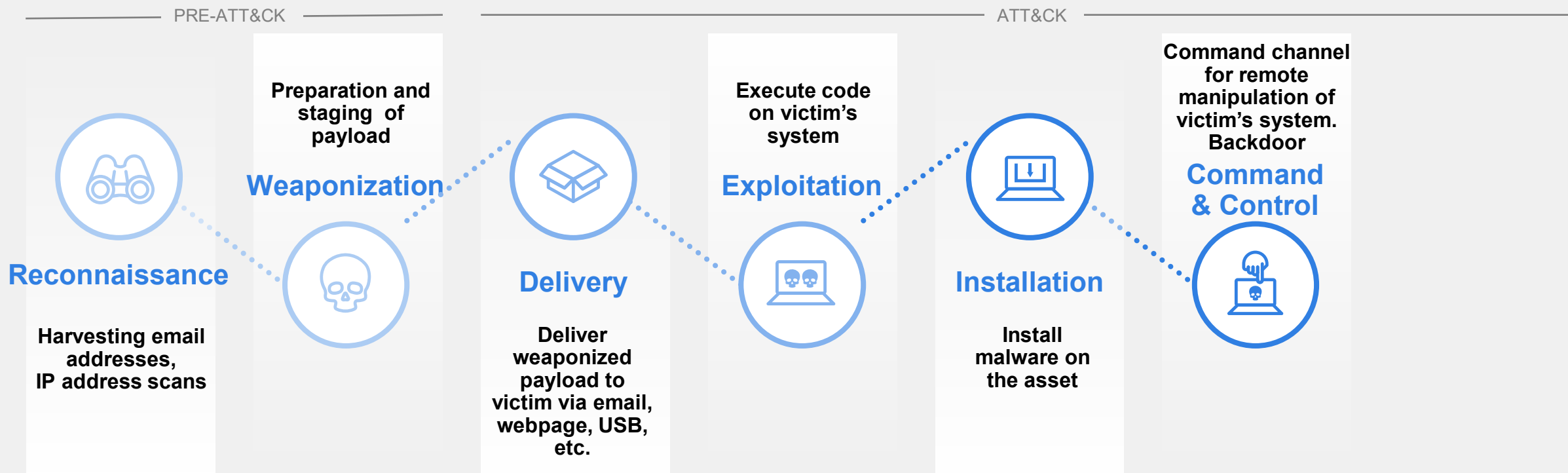




# But Security Is NOT Straightforward

Security is Technology *Plus* Psychology

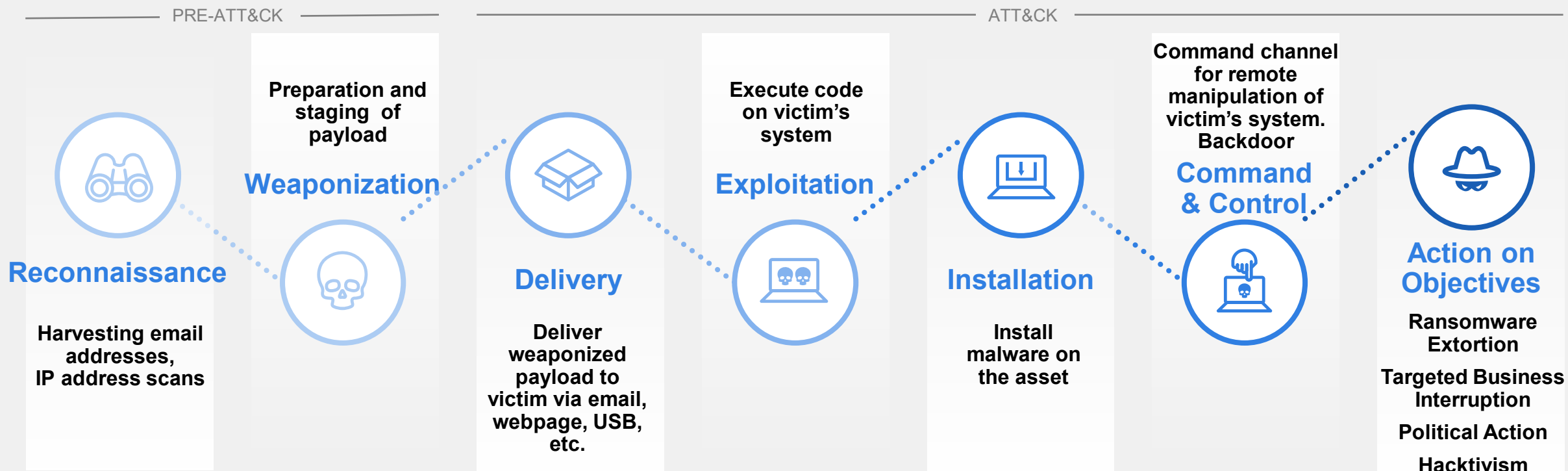
Where is the Attacker Along The Cyber Kill Chain? And How Do We Stop Him?



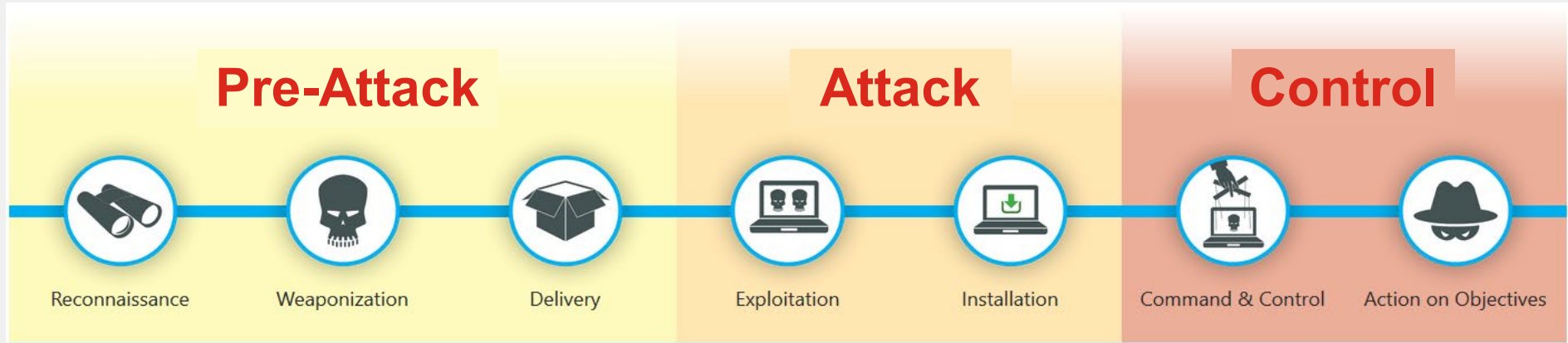
# But Security Is NOT Straightforward

Security is Technology *Plus* Psychology

Where is the Attacker Along The Cyber Kill Chain? And How Do We Stop Him?



# Tools For Every Stage. LOTS of Tools. . .



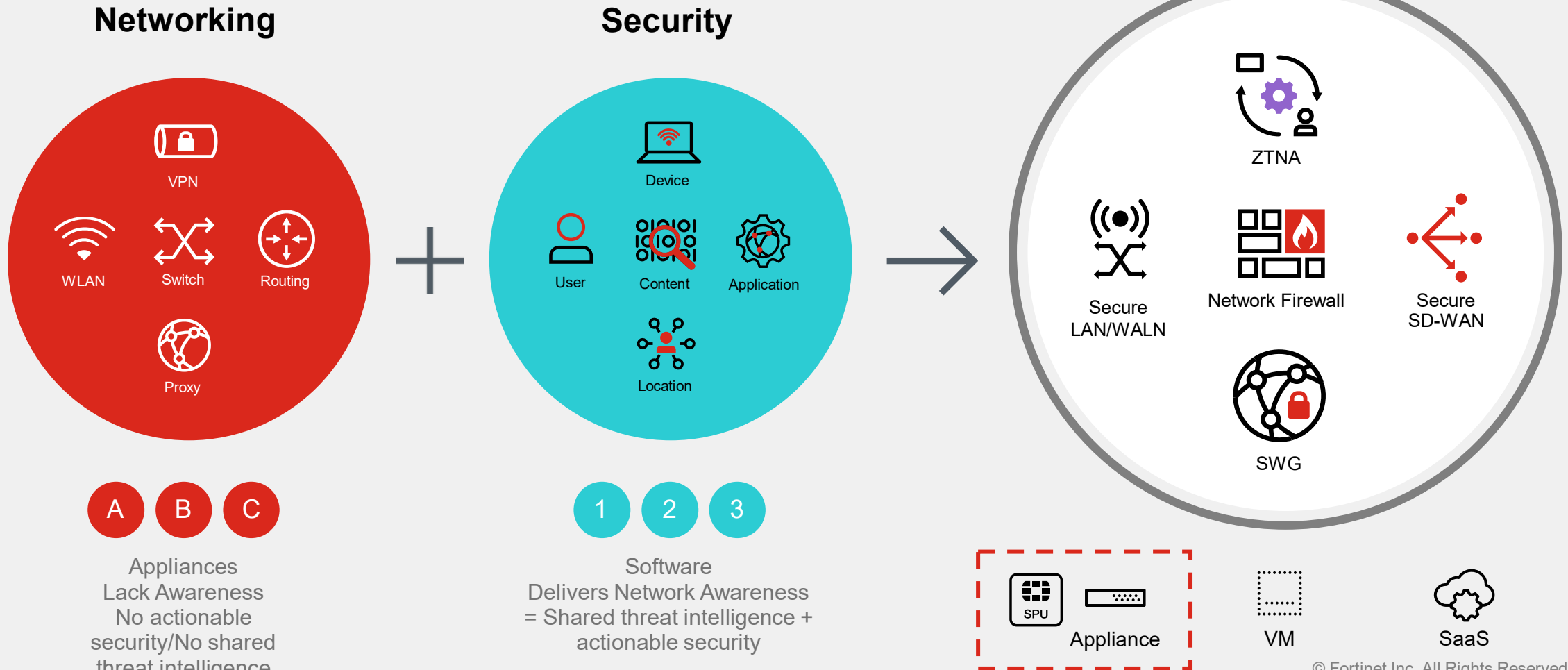
Intrusion Prevention	Green	Light Blue	Green	Green	Light Blue	Light Blue	Light Blue
Anti-Virus	Light Blue	Light Blue	Green	Green	Green	Light Blue	Light Blue
Anti-Botnet	Light Blue	Light Blue	Green	Light Blue	Green	Green	Green
Email Analysis / Anti-Spam	Light Blue	Light Blue	Green	Light Blue	Light Blue	Light Blue	Light Blue
Web Filtering	Light Blue	Light Blue	Green	Light Blue	Light Blue	Green	Light Blue
Web Security	Green	Light Blue	Light Blue	Green	Light Blue	Light Blue	Light Blue
EDR	Light Blue	Light Blue	Light Blue	Green	Light Blue	Light Blue	Light Blue
Sandboxing	Light Blue	Light Blue	Green	Light Blue	Green	Green	Light Blue
Threat Analysis w/or w/out AI	Light Blue	Light Blue	Green	Green	Light Blue	Light Blue	Green
Honey Pot / Deception tools	Green	Light Blue	Light Blue	Green	Light Blue	Light Blue	Green
Access Control	Green	Light Blue	Light Blue	Green	Light Blue	Light Blue	Light Blue



# Convergence of Networking and Security

## Security-Driven Networking

## Security-Driven Networking



# Fortinet Security Fabric

A Mesh Architecture with AI Threat Intelligence

## Broad

visibility and protection of the entire digital attack surface to better manage risk

## Integrated

solution that reduces management complexity and shares threat intelligence

## Automated

self-healing networks with AI-driven security for fast and efficient operations



# Three Take-Aways

## Attacks Follow a Structure



AI-Driven Security Operations  
provide a reliable Framework  
from Detection to Response



# Three Take-Aways

## Attacks Follow a Structure



AI-Driven Security Operations provide a reliable Framework from Detection to Response

## A Holistic Security Platform Mesh is Needed



Point solutions cannot address the complexity and sophistication of new threats



# Three Take-Aways

## Attacks Follow a Structure



AI-Driven Security Operations provide a reliable Framework from Detection to Response

## A Holistic Security Platform Mesh is Needed



Point solutions cannot address the complexity and sophistication of new threats

## Holistic does not mean Monopolistic



Your security and infrastructure tools need to coordinate regardless of vendor



**F****RTINET**®