Symantec Complete Endpoint Defense

Abhishek Srivastava
Sr. Director, Product Management
Endpoint and Hybrid Cloud Security

May 2019

Symantec Endpoint Security

The Most Complete Endpoint Security Solution

DEEPEST PROTECTION

ANTIMALWARE

PREVENT DETECT RESPOND

HARDENING

ISOLATE CONTROL DECEIVE

DEFEND AGAINST ALL ATTACK VECTORS AND METHODS

BROADEST COVERAGE

TRADITIONAL PLATFORMS

MODERN PLATFORMS

iOS

COMPUTE AND STORAGE

Windows Server, redhat, Google Cloud Platform, docker, Microsoft Azure, aws, SharePoint, amazon S3, EMC²

EXTENSIVE COVERAGE TO PROTECT ALL ENDPOINTS

MODERN MANAGEMENT

AUTO-MANAGE

AUTO EVALUATE → AUTO RECOMMEND → AUTO APPLY→ AUTOLEARN

MODERN MANAGEMENT & MODERN APP

arm, airwatch by vmware, Intune

EXTEND SECURITY WITH MODERN MANAGEMENT

INTEGRATED ARCHITECTURE

SIMPLIFIED ARCHITECTURE

SINGLE AGENT SINGLE CONSOLE

FLEXIBLE MANAGEMENT

ON-PREM HYBRID CLOUD

OPEN PLATFORM

ICDX, OpenC2, MS Graph API

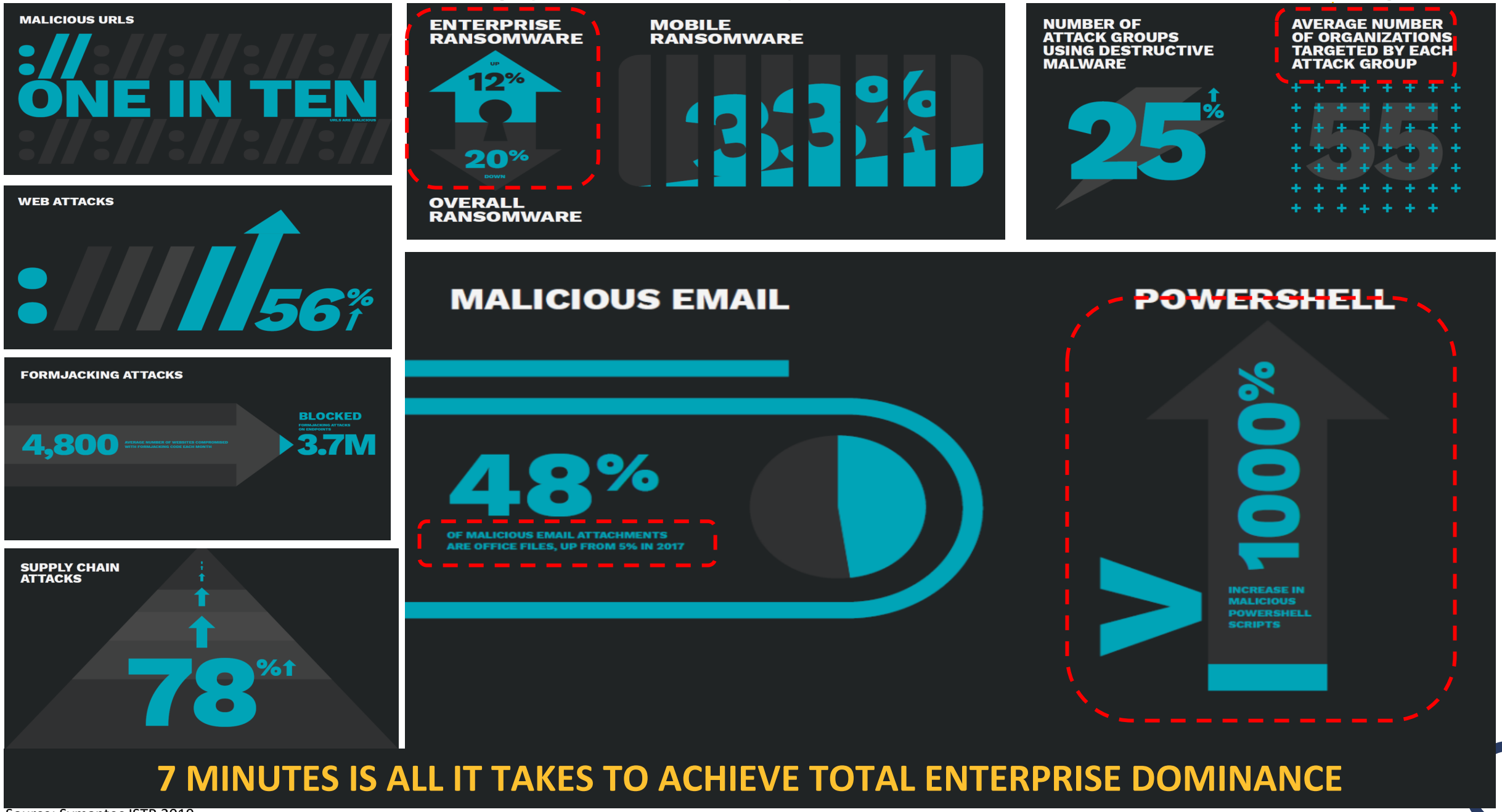
ACHIEVE SUPERIOR OPERATIONAL EFFICIENCIES

HOMOGENOUS ENDPOINT SECURITY AND MANAGEMENT FOR A HETEROGENOUS WORLD

Deepest Protection

Symantec™

Modern Threats increasingly Fileless/Script/Content/Web based and Targeted



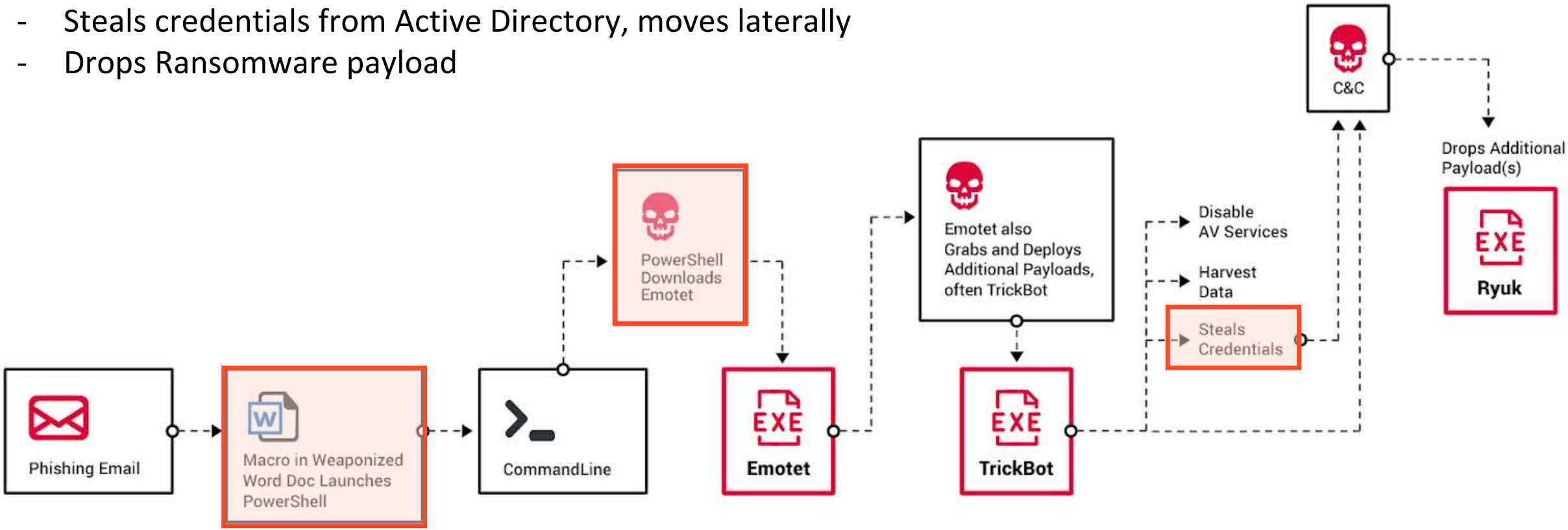
7 MINUTES IS ALL IT TAKES TO ACHIEVE TOTAL ENTERPRISE DOMINANCE

Source: Symantec ISTR 2019

Advanced Persistent Threat Example

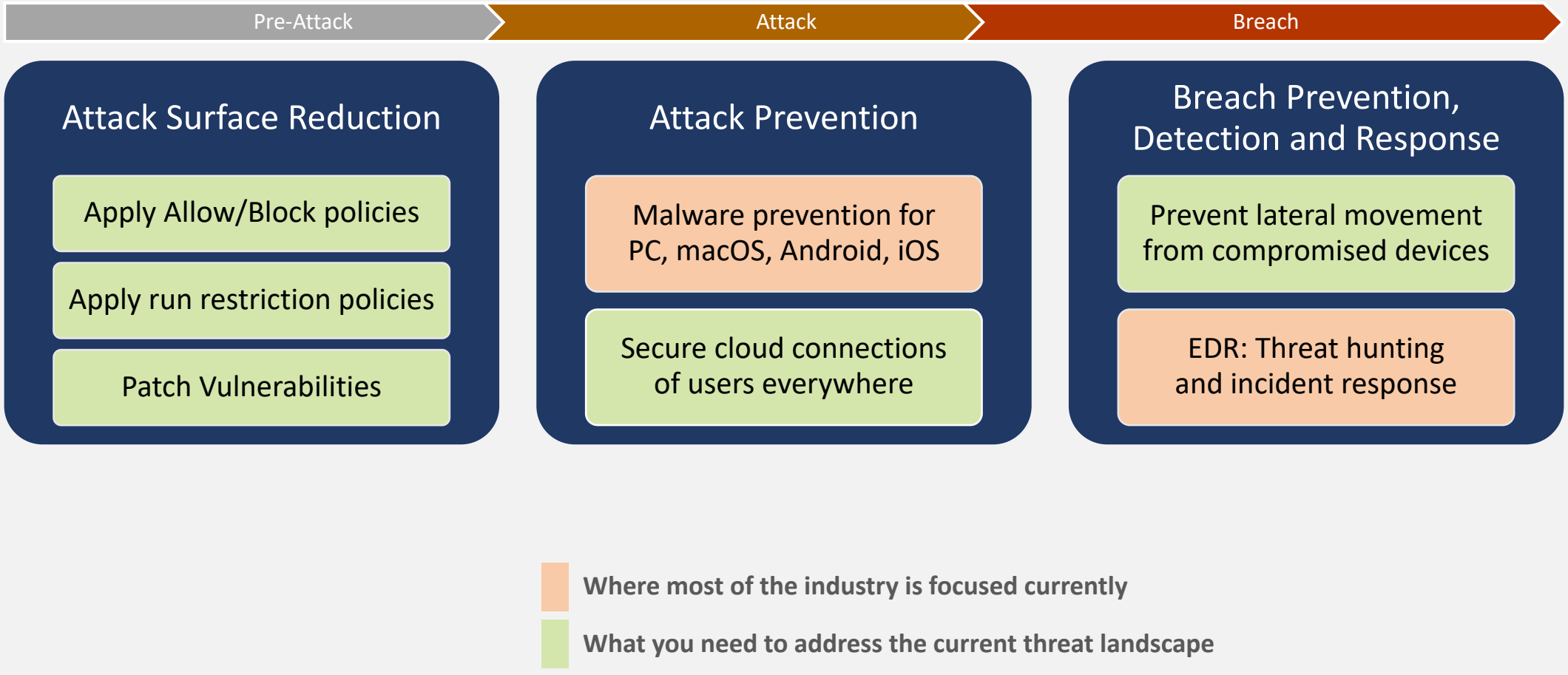
Emotet continues to evolve

- Uses weaponized Word Doc to launch Powershell
- Downloads Tricbot, Connects to C&C
- Steals credentials from Active Directory, moves laterally
- Drops Ransomware payload



Securing Endpoints from Advanced Threats

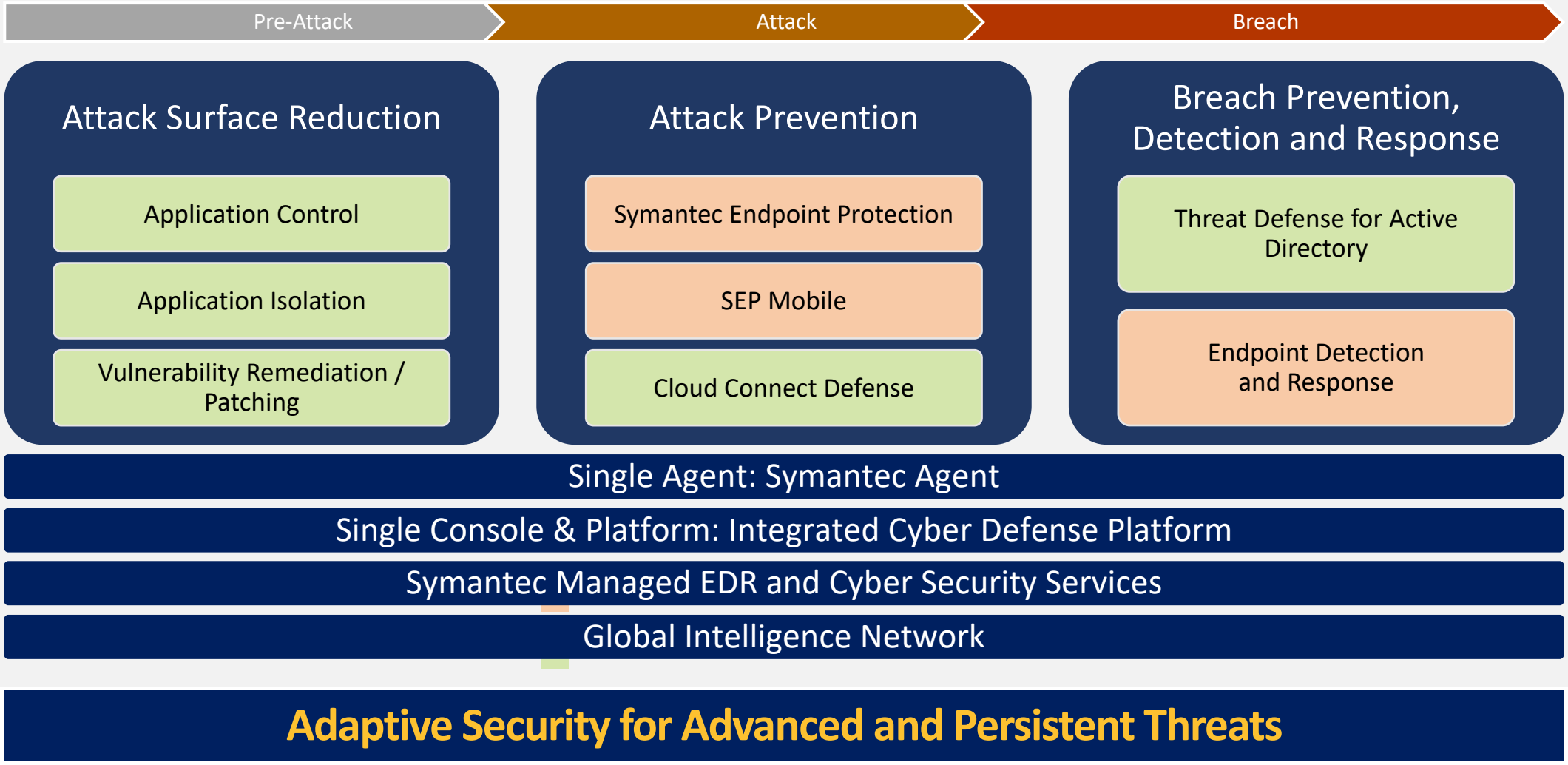
The Need for Proactive and Continuous Protection



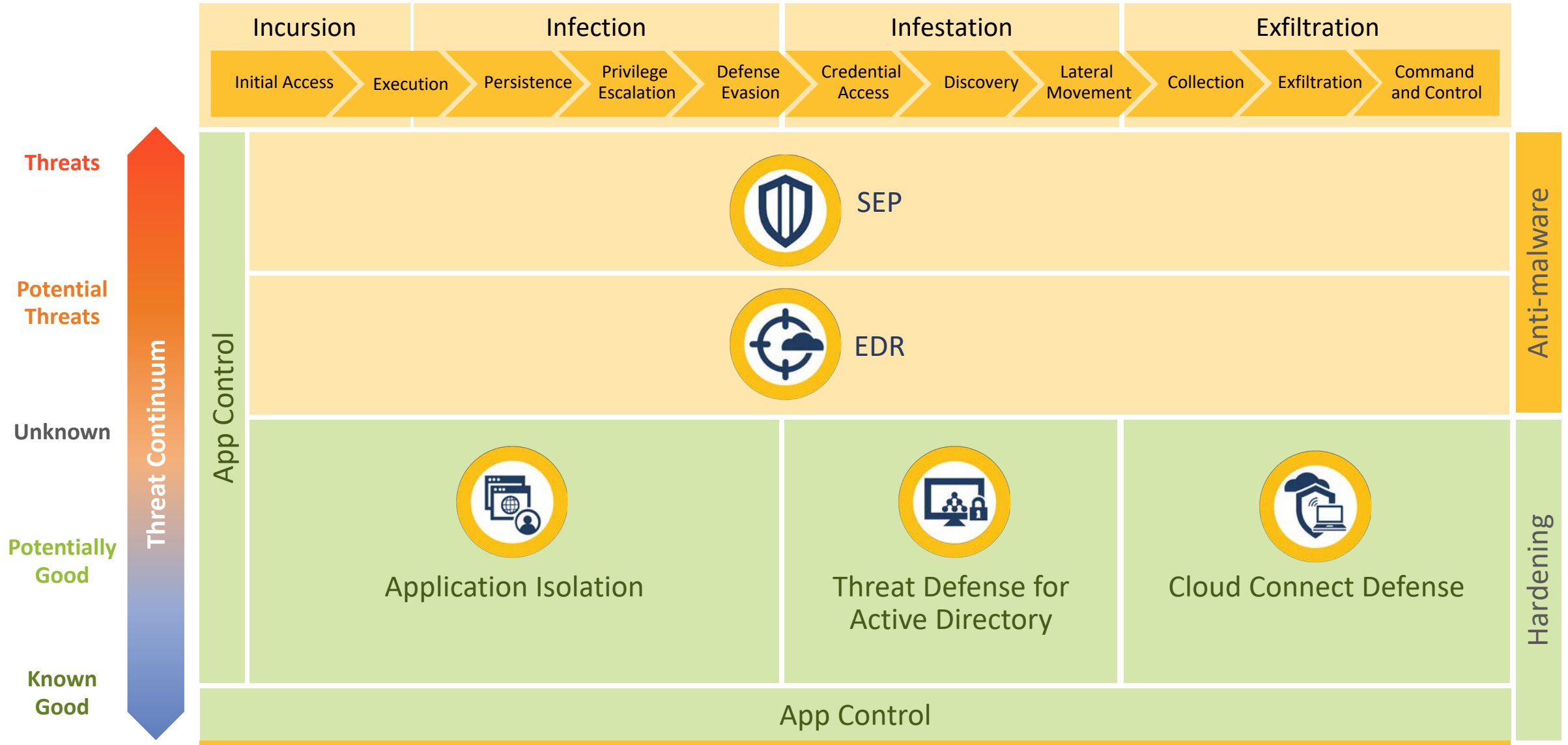
Adaptive Security for Advanced and Persistent Threats

Securing Endpoints from Advanced Threats

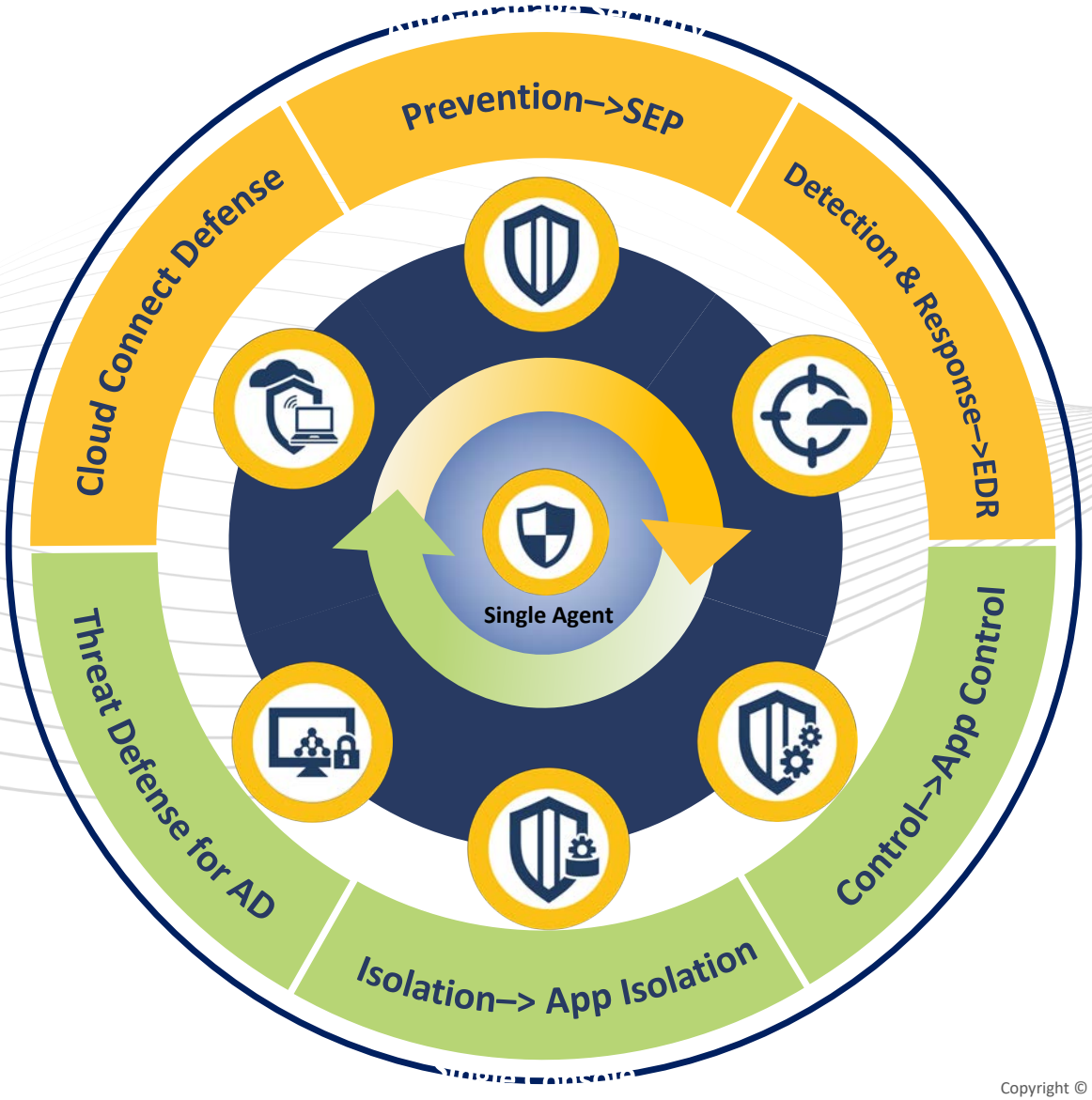
Symantec Complete Endpoint Defense



…Covering the entire MITRE ATT&CK Framework



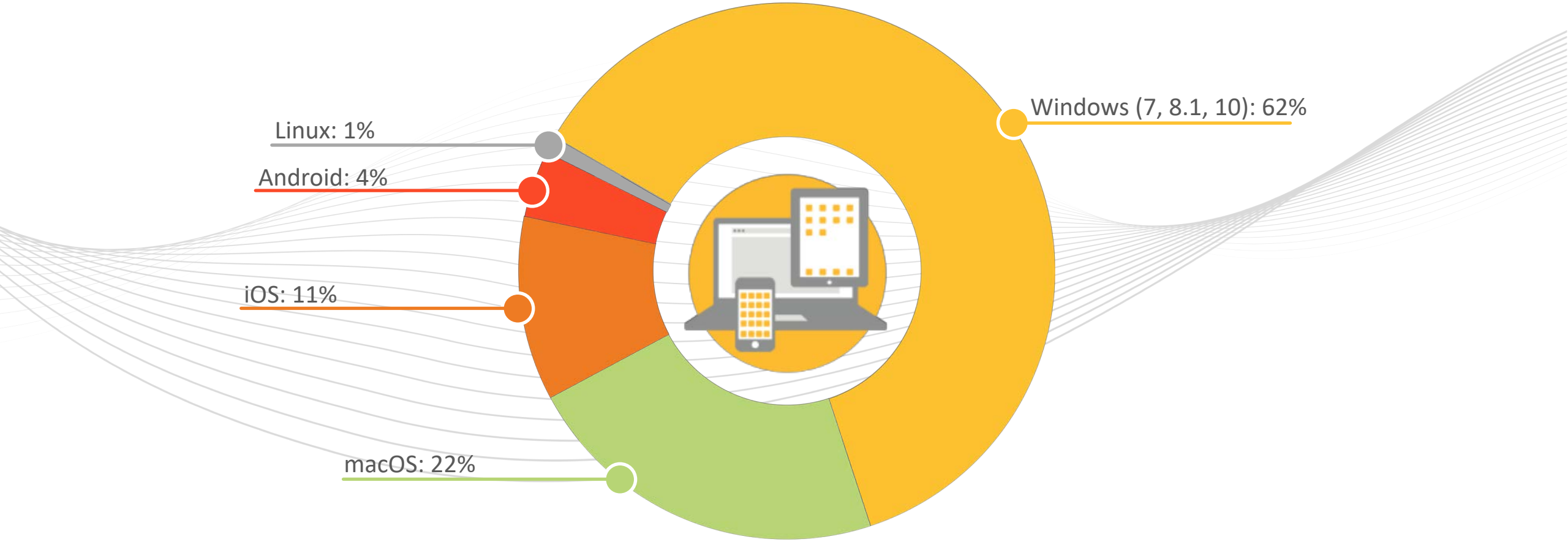
…Delivered Through a Single Agent and Console



Broadest Coverage

Symantec™

Protection Across Multiple Operating Systems



DELIVERING BROAD PROTECTION ACROSS A WIDE SPECTRUM OF OEPRATING SYSTEMS

Source: Distribution of Operating Systems among Enterprise Endpoints WW as of 2017, Statista

Deepest and Broadest Protection

Enabling Diverse Use Cases Requiring Diverse Protection

Corporate Managed – Traditional & Modern | Modern Lightly Managed | Unmanaged

Disconnected

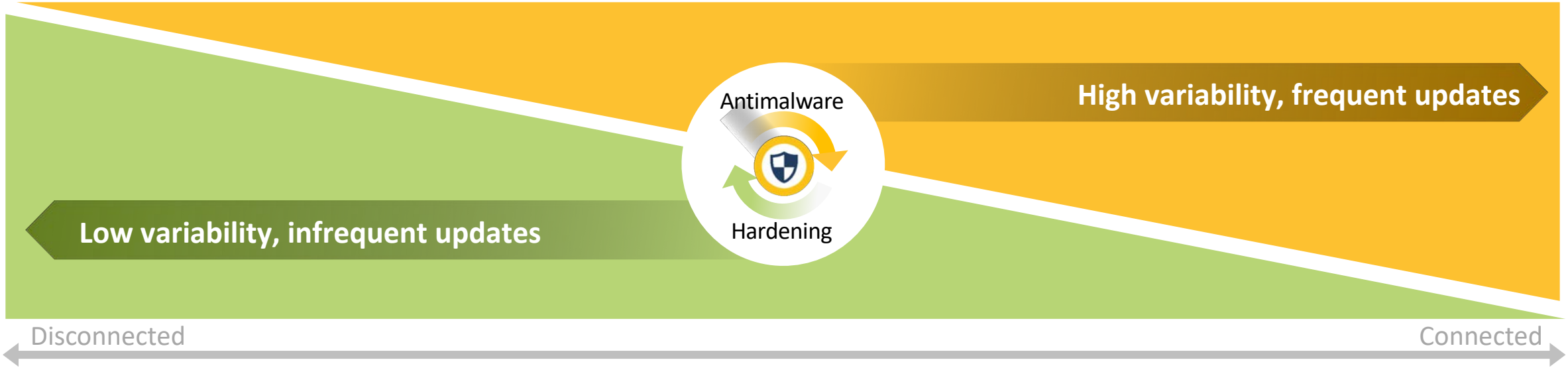
Intermittently connected

Fixed Function

Connected Traditional

Connected Modern

BYOD



Modern Management

Integrated Cyber Defense Manager (ICDm)

The thinking console…

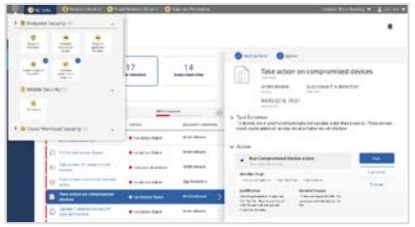
Symantec™

Symantec Integrated Cyber Defense Manager (ICDm)

Symantec

Symantec Integrated Cyber Defense Manager (ICDm) is a cloud-based intelligent security management console and framework for Symantec's Integrated Cyber Defense Platform. ICDm combines analytics, task-based recommendations, workflow automation and open interfaces for data, detection, remediation and management and delivers unified visibility and control to protect enterprises from sophisticated threats.

SINGLE UNIFIED CLOUD CONSOLE



Single pane of glass for all products

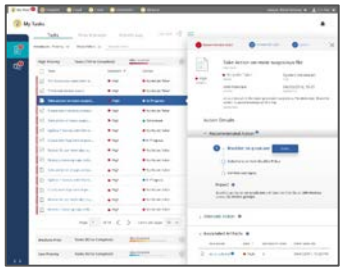
Hosted in the cloud and delivered as SaaS

AUTO-MANAGED

ML-driven evaluation and recommendations

Adaptive and self-learning

TASK-DRIVEN



Task-driven to help admins be more productive

Workflows that simplify every job

MODERN & OPEN

Modern management and modern app

orm airwatch by vmware

Intune

Open Platform

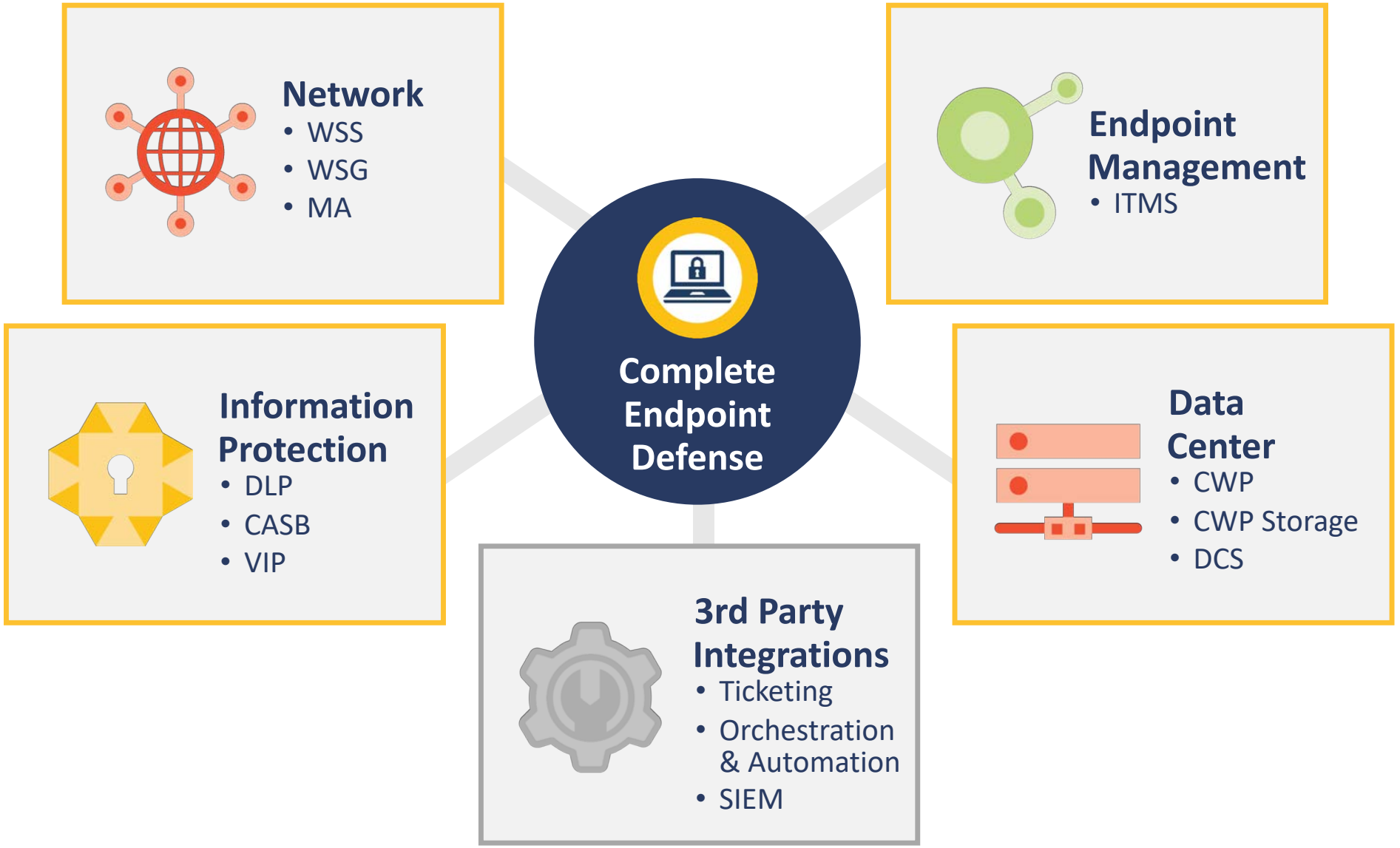
ICDX OpenC2

MS Graph API

SMART AND MODERN MANAGEMENT FOR IMPROVED SECURITY POSTURE

Integrated Architecture

Integrated with Symantec and Third Party



Symantec™

Thank You!