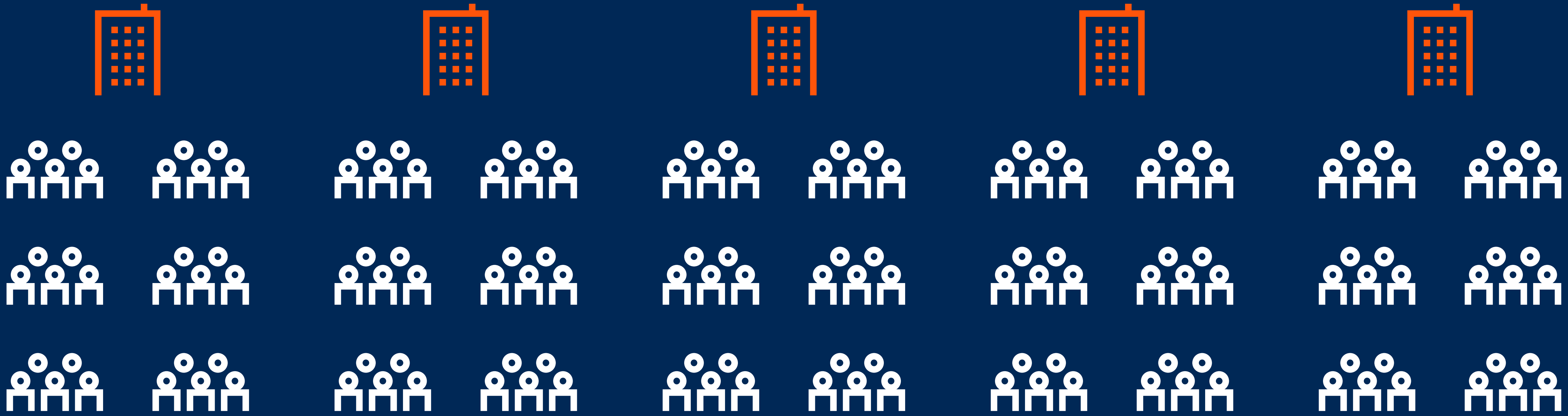
Device Management and Security in a Post COVID-19 World

Rob Smith
@Mastidon

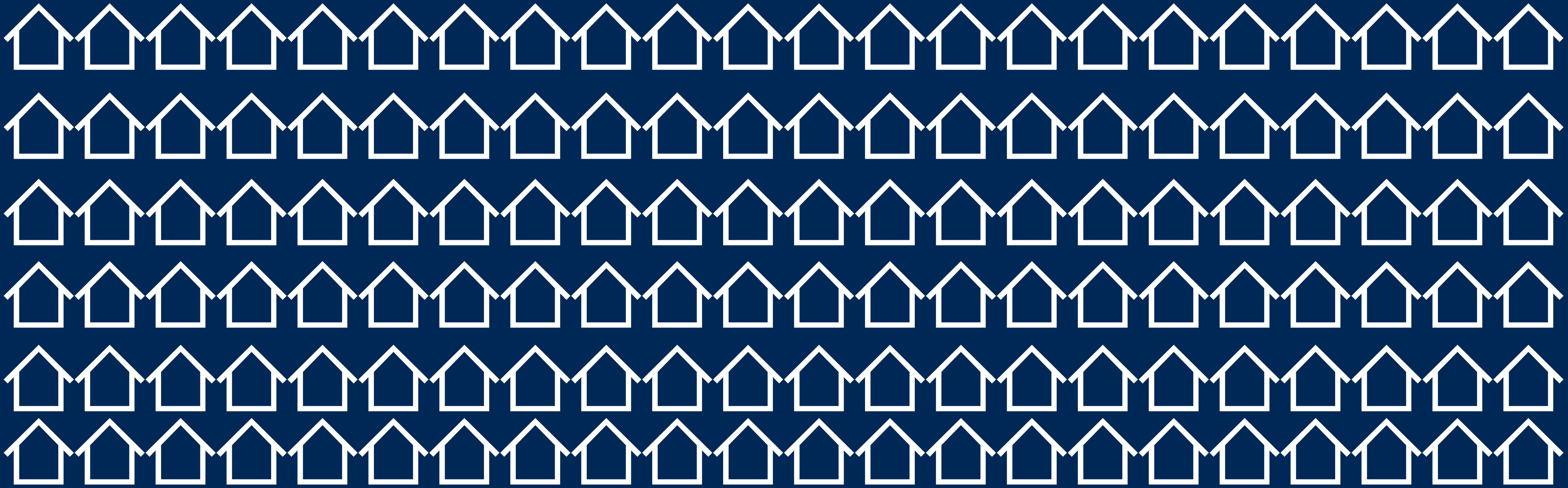
Prior to COVID-19 —

A typical enterprise might have had 5,000 people working across five offices



But Now …

They have 5,000 offices.



COVID-19 Response Is a Three-Phase Process for IT

1. Get everyone back online as fast as possible

2. Take existing user connections and make them safe

3. Make existing connection smarter and more efficient

Where are you in this process?

All Users Are Not Equal

Executives

≠

Office Worker

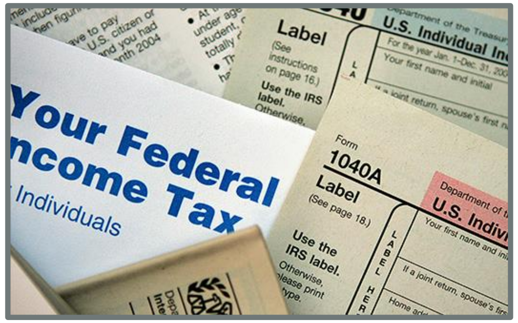
≠

Frontline Worker

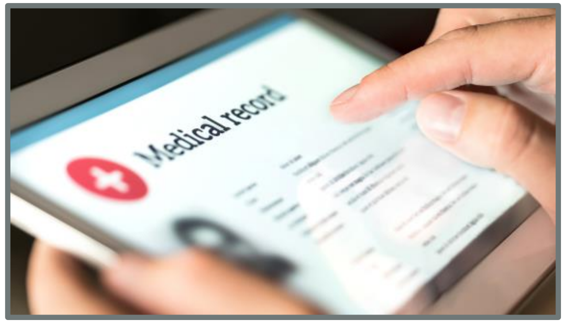
Not All Data Is Equal Either!

≠

≠



≠



The First Step Before Talking Technology Is to Define Your Use Case!

Who are the users and what is their job function?

What kind of device is being used and who owns it?

What kind of applications and data do users need access to and is it on-premises or in the cloud?

Where in the world is the user located?

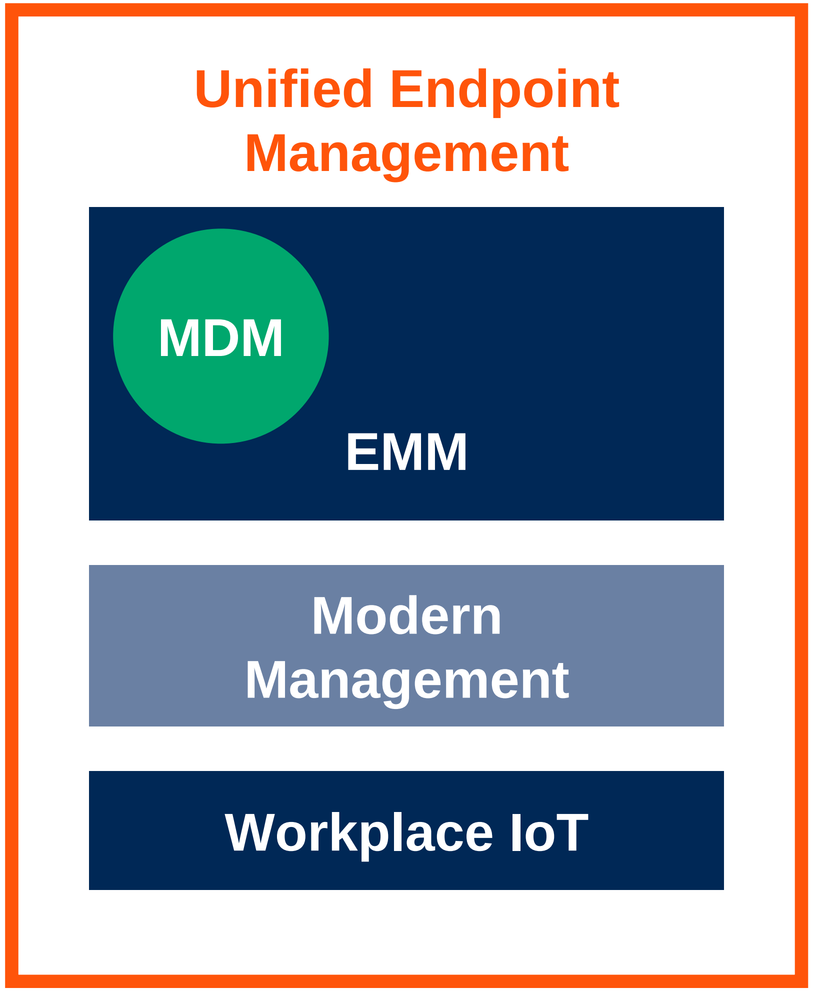
The Evolution to UEM

2011 Mobile Device Management (MDM):

- Policy Enforcement
- Device Information

2014 Enterprise Mobility Management (EMM):

- MDM as a Feature
- Mobile Application Management (MAM)
- Mobile Identity
- Mobile Content Management (MCM)
- Data Containment



Unified Endpoint Management

MDM

EMM

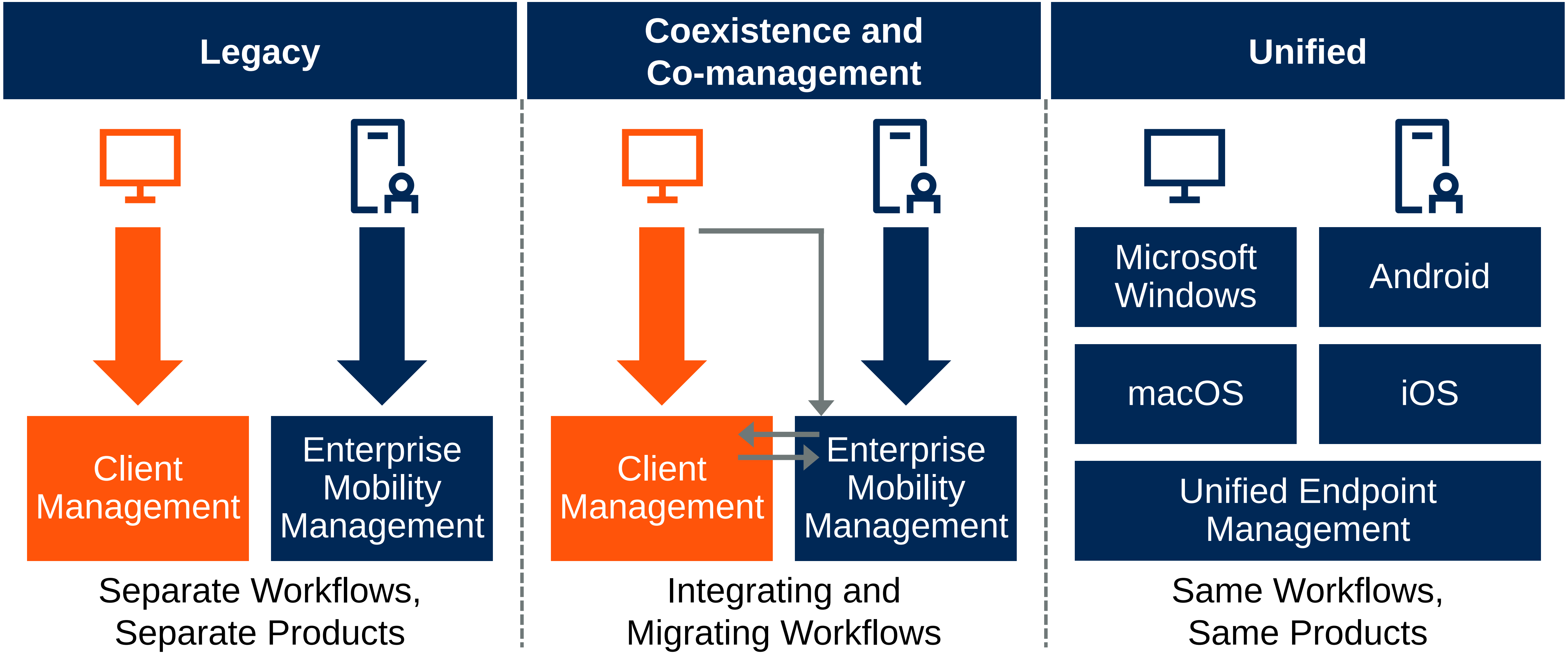
Modern Management

Workplace IoT

2018 - 2020 Unified Endpoint Management (UEM):

- EMM as a Feature
- Modern Management:
  - Windows 10, macOS management
- Migration tools to modern management
- Can include legacy Client Management Tools (CMT)
- Analytics
- Unified Endpoint Security
- Workplace IoT:
  - Wearables Devices
  - Smart IoT devices

Three Models for Management



Legacy

Client Management

Enterprise Mobility Management

Separate Workflows, Separate Products

Coexistence and Co-management

Client Management

Enterprise Mobility Management

Integrating and Migrating Workflows

Unified

Microsoft Windows

Android

macOS

iOS

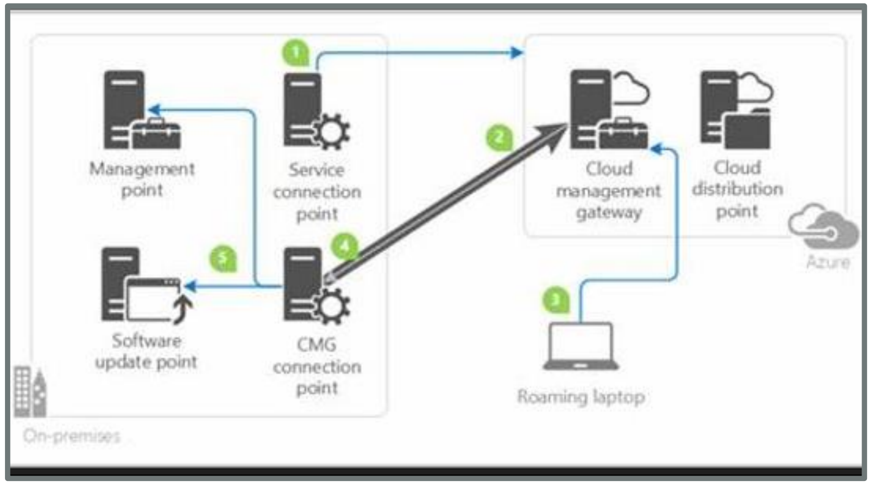
Unified Endpoint Management

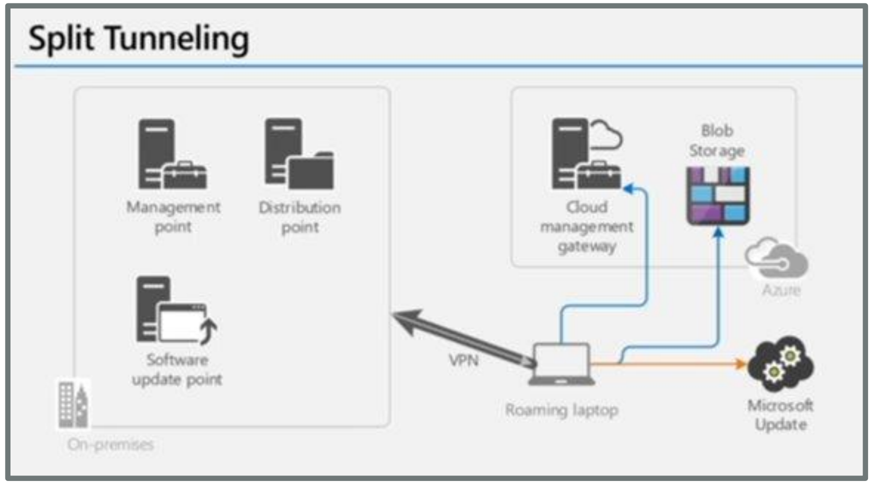
Same Workflows, Same Products

Solving the Patching Problem...

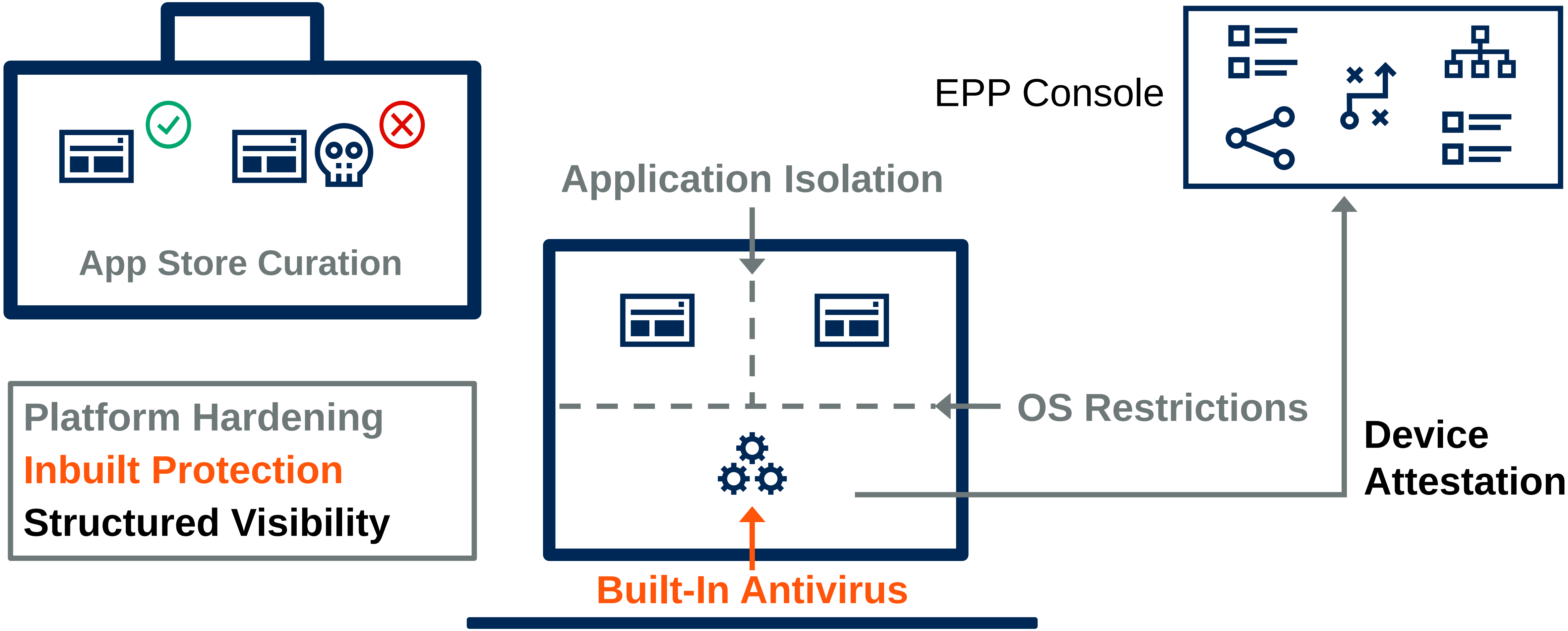
Patch Tuesday kills remote access VPNs. The solution is to choose an Internet-based Client Management Tool

- Internet-facing or hosted ConfigMgr server (DMZ, Proxy, SSL, etc.) so clients can communicate when not on LAN/VPN.
- Requires PKI certificates and limited split-tunneling (if always on VPN)
- Most CMT vendors offer migration to cloud hosting





Endpoint OSs Provide Maturing Security Controls



Platform Hardening

Inbuilt Protection

Structured Visibility

The Evolution of Endpoint Protection Tools

Antivirus

Definition Based

- File Scanning
- Allow List/Block List
- Memory Protection

Add-ons:

- Device/Application Control
- Data Leakage Prevention
- Patching/Compliance

Advanced Antivirus

With Machine Learning

As per Antivirus plus:

- Machine Learning or Behavioral Detection
- Recognition of Malware/System Administrator Tools Used as Exploits
- Pattern Detection and Identification of Rogue Network Activity/C2 Call Home

EDR

Detect and Respond

- Streaming of Endpoint Telemetry to Server/Cloud
- Lookup of “Unknowns” Remote Control and Device Intervention
- Big Data Analytics
- Threat Hunting

EDR + Automation

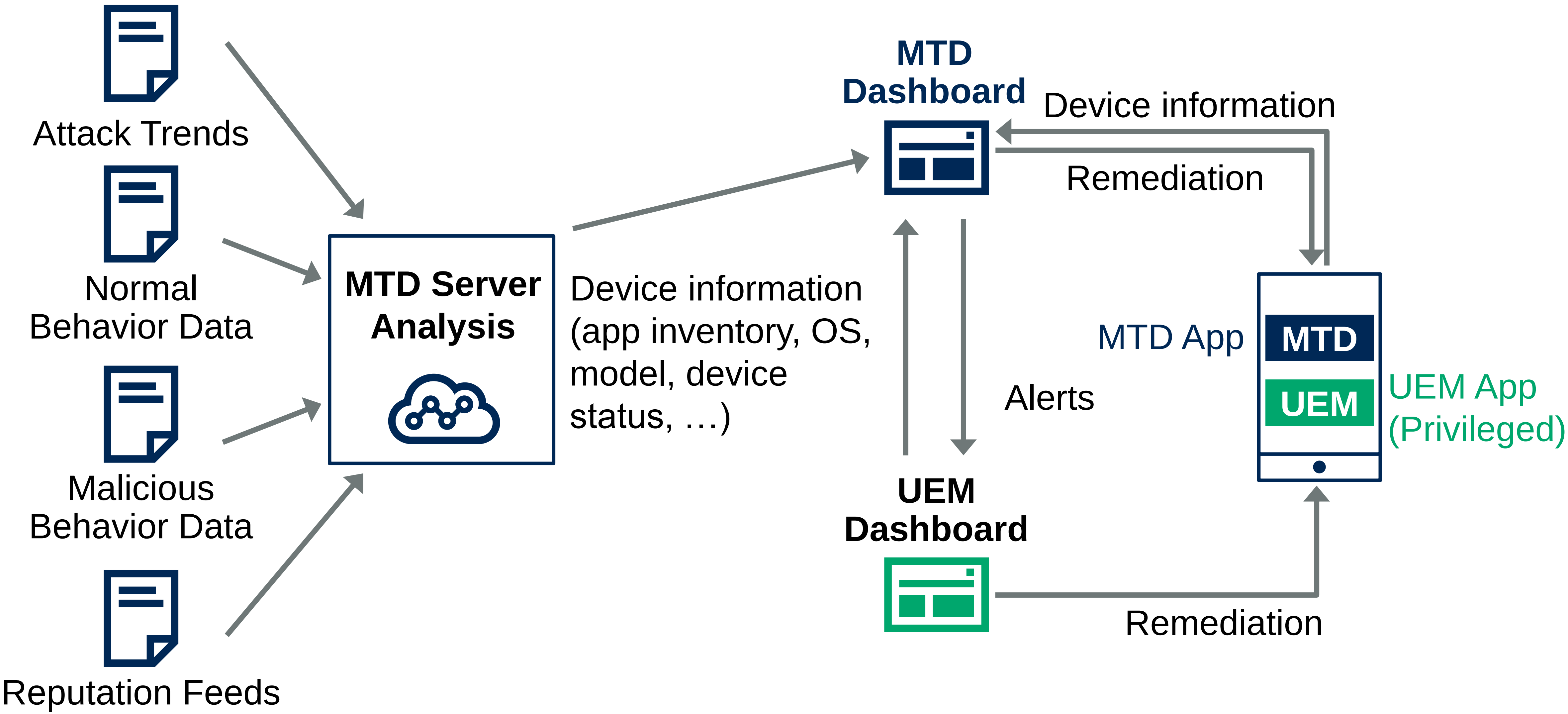
Fully Featured

As per EDR plus:

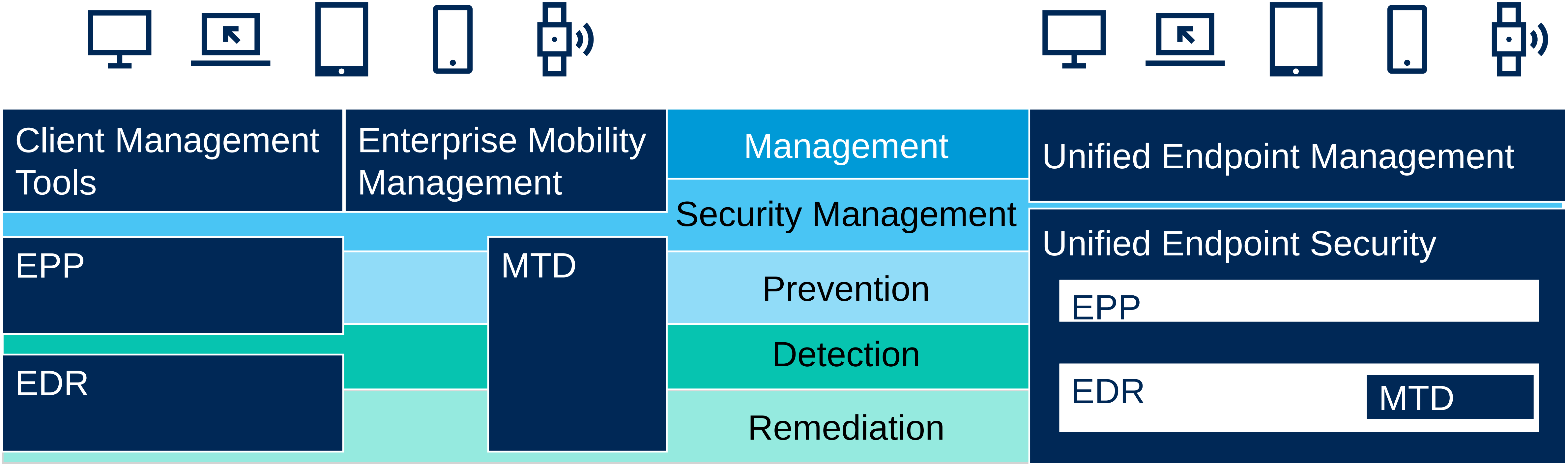
- Automated Rollback/Remediation
- Threat Intelligence
- SOAR/API Integration
- Real-Time Response

Source: Gartner

MDM Is Not the Same as Mobile Threat Defense



Evolution to a Single Unified Endpoint Security (UES) Product



Client Management Tools

Enterprise Mobility Management

Management

Security Management

EPP

MTD

Prevention

EDR

Detection

Remediation

Unified Endpoint Management

Unified Endpoint Security

EPP

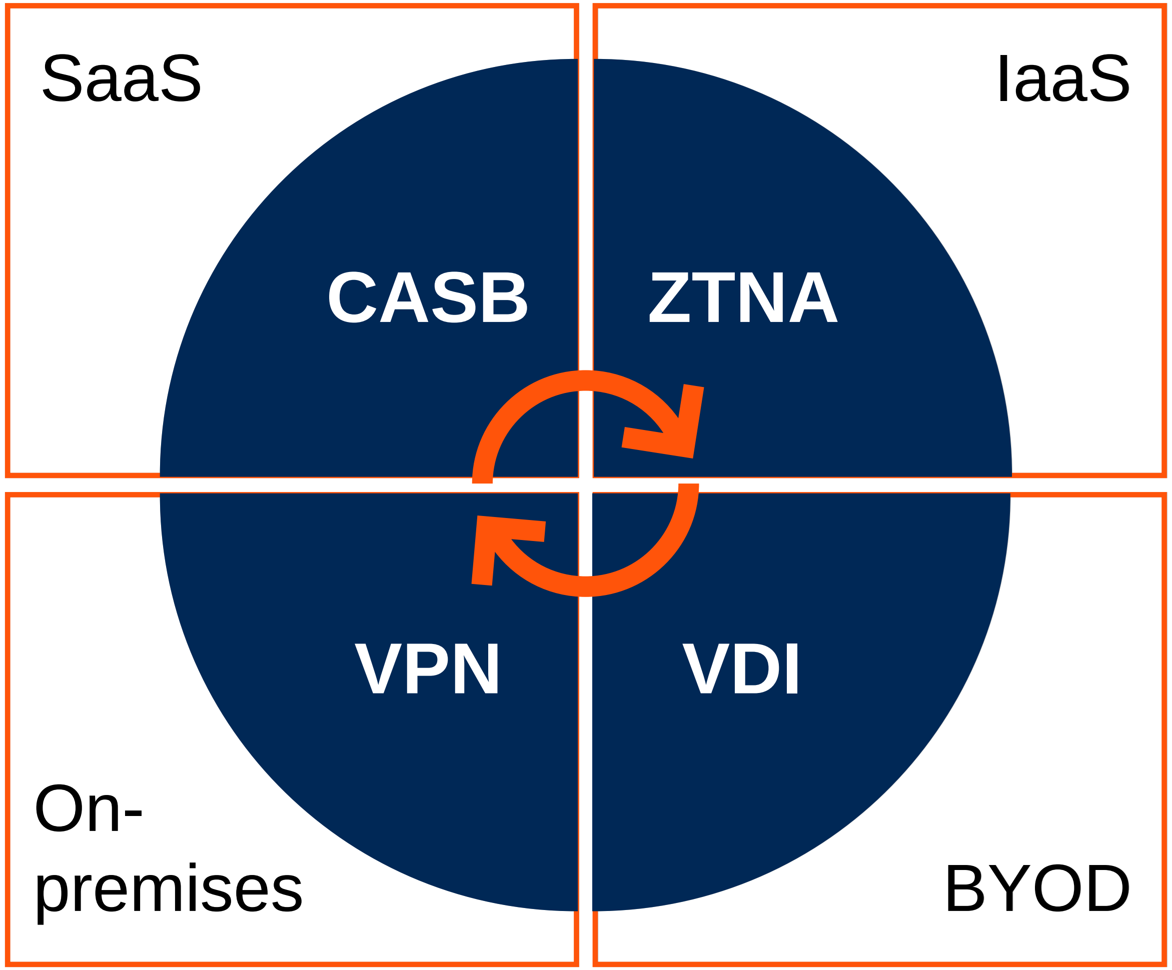
EDR

MTD

Today we use a mishmash of different tools

But they are becoming a single tool for management and security

Are You Still Doing Always-On VPN?



SaaS

IaaS

CASB

ZTNA

VPN

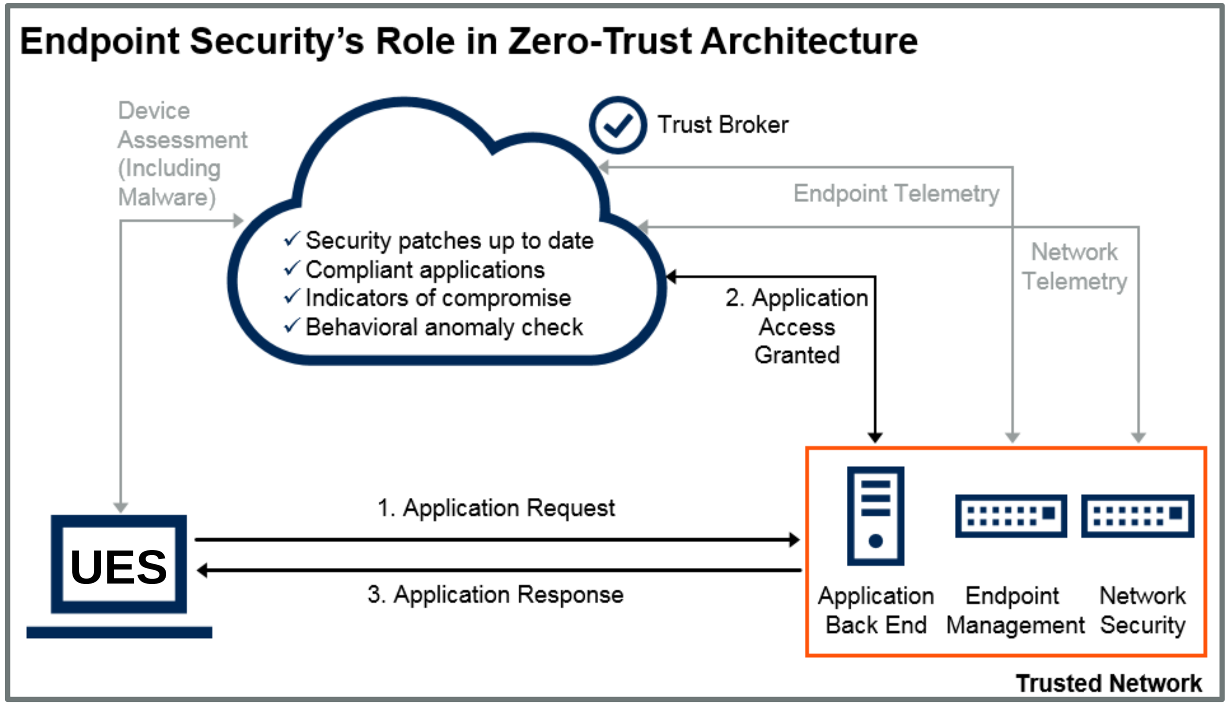
VDI

On-premises

BYOD

ZTNA

- For the use case of IaaS applications, a ZTNA product can be the right choice
- Combines strong identity and authentication controls
- Can also restrict access based on device, and network
- Can forcibly install UES as part of authentication
- Ideal solution for BYOPC/BYOD



Endpoint Security's Role in Zero-Trust Architecture

Recommendations

- There is no longer remote working, only working.
- Identify the groups and use cases, now and in the future, and specify a product or service against the superset of both.
- Solve the patching problem by transitioning to a cloud CMT/UEM.
- Plan for the evolution of endpoint security to a single UES console.
- Stop using always-on VPN to solve all remote access.
- ZTNA with UES to protect access in a cloud world without the need to manage the device.
- In a post-COVID-19 world, it is important to deploy, then improve as you go!

Recommended Gartner Research

- **Magic Quadrant for Unified Endpoint Management**
  Dan Wilson, Chris Silva, Rob Smith and Others (G00450413)
- **Hype Cycle for Endpoint Security, 2020**
  Dionisio Zumerle and Rob Smith (G00450232)
- **Solving the Challenges of Modern Remote Access**
  Rob Smith, Steve Riley, Nathan Hill and Jeremy D’Hoinne (G00722990)
- **Market Guide for Endpoint Detection and Response Solutions**
  Paul Webber, Prateek Bhajanka, Mark Harris and Brad LaPorte (G00380177)
- **Endpoint Detection and Response Architecture and Operations Practices**
  Jon Amato, Anton Chuvakin and Augusto Barros (G00367740)
- **Market Guide for Mobile Threat Defense**
  Dionisio Zumerle and Rob Smith (G00376573)

For information, please contact your Gartner representative.