KEYNOTE

Future-Proof Unified Endpoint Management (UEM) integrates Security

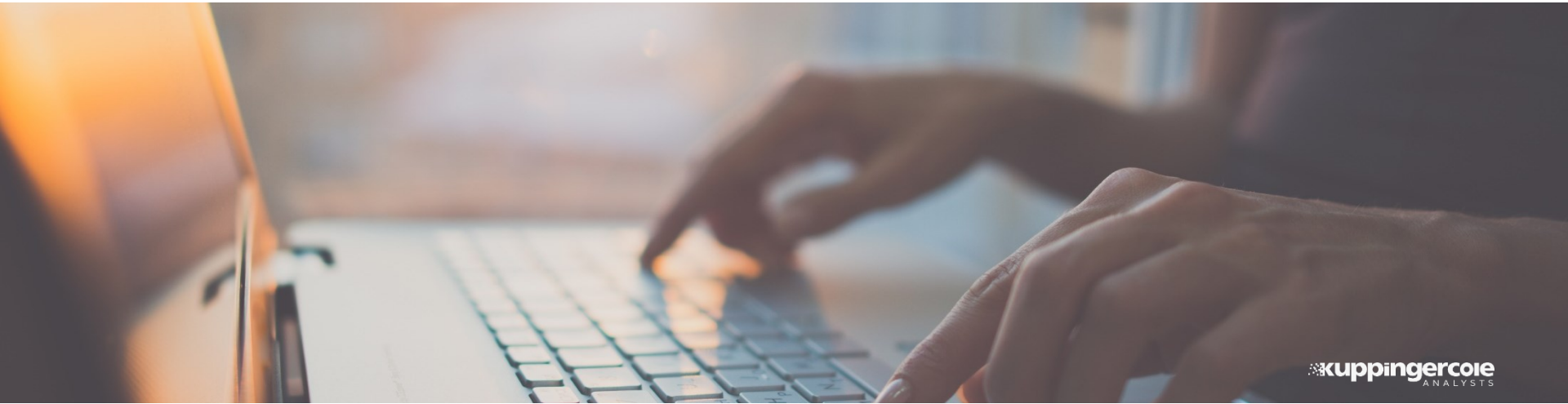
MARTIN KUPPINGER
PRINCIPAL ANALYST
KUPPINGERCOLE ANALYSTS AG

UEM DEFINED

Unified Endpoint Management (UEM) covers solutions unify Endpoint Management in two ways:

1. Unification across all types of endpoints, specifically including Windows systems and mobile devices running iOS or Android.
2. Unification of capabilities, including Endpoint Lifecycle Management, Application Management, Endpoint Security, and Endpoint Content Management.

Thus, UEM covers way more than traditional Client Lifecycle Management solutions did.



The History of Unified Endpoint Management

Unified Endpoint Management has evolved from point solutions to fully integrated suites

UNIFIED ENDPOINT MANAGEMENT

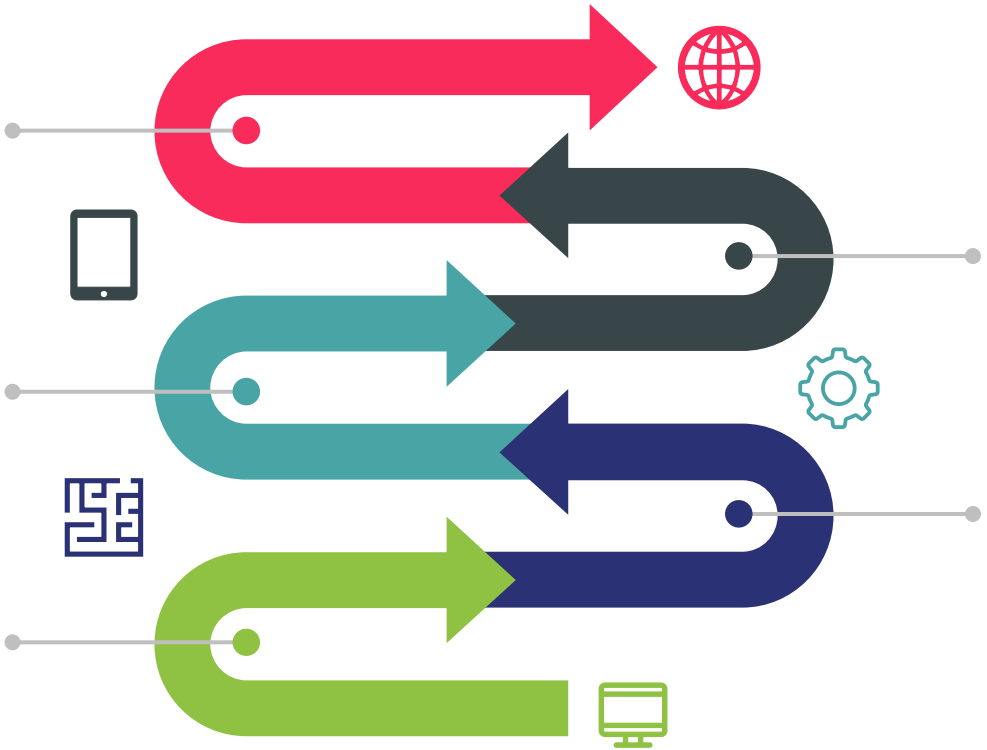
Fully integrated solutions covering all types of devices and integrating management and security.

CLIENT LIFECYCLE MANAGEMENT

Integrated solutions, combining key capabilities into suites of products.

DECENTRAL ADMINISTRATION

Local system administration, lacking central tools.



SEPARATE ENTERPRISE MOBILITY MANAGEMENT

Isolated solutions focusing on mobile devices only.

POINT SOLUTIONS, E.G. OS DEPLOYMENT

Variety of specialized solutions targeting only isolated capabilities.

Capability Areas of Unified Endpoint Management

The Five Key Capability Areas of Unified Endpoint Management and what Analysts expect to see

LIFECYCLE

Traditional key capabilities such as endpoint onboarding, provisioning, decommissioning, remote access, wiping, patch management, and OS deployment and management.

APPLICATIONS

Application-centric capabilities such as enterprise app stores and enrollment, software delivery and packaging, application policies and controls, and blacklisting/whitelisting.

SECURITY

Endpoint security capabilities such as authentication, access policies and context-based access, certificate management, application signing, and analytics. Might also include more comprehensive EPDR capabilities.

CONTENT

Segregation of business from personal data an apps, data leakage prevention, policies and controls for documents and other content, audit trails around access to sensitive content.

ASSETS & MORE

Advanced capabilities beyond inventories, including management of assets, licenses, and contracts, but also help desk features and other capabilities beyond the core feature set.

You are not alone: UEM and other Technologies

Unified Endpoint Management overlaps and partially incorporates other IT disciplines

ENDPOINT SECURITY

Standard endpoint security solutions, specifically centered around anti-malware.

EPDR (ENDPOINT PROTECTION, DETECTION, RESPONSE)

Advanced solutions for endpoint security, covering endpoint protection, detection features and integration with threat intelligence, and automated response such as process termination and rollbacks.

IT SERVICE MANAGEMENT

Solutions supporting the full range of IT Service Management, including Help Desk capabilities and ticketing.

WORKPLACE DELIVERY

Automated delivery of workplaces in different models, including VDI (Virtual Desktop Infrastructures).

ASSET, LICENSE & CONTRACT MANAGEMENT

Management of assets beyond inventory of endpoints, software licenses including analysis of licensing state and mapping to assets, and the related contracts.

ENTERPRISE MOBILITY MANAGEMENT

Solutions focused only on mobile devices, supporting their management.

Not that new: The Role of Security in UEM

Security Management always has been part of Client Lifecycle Management

INTEGRATING ENDPOINT SECURITY

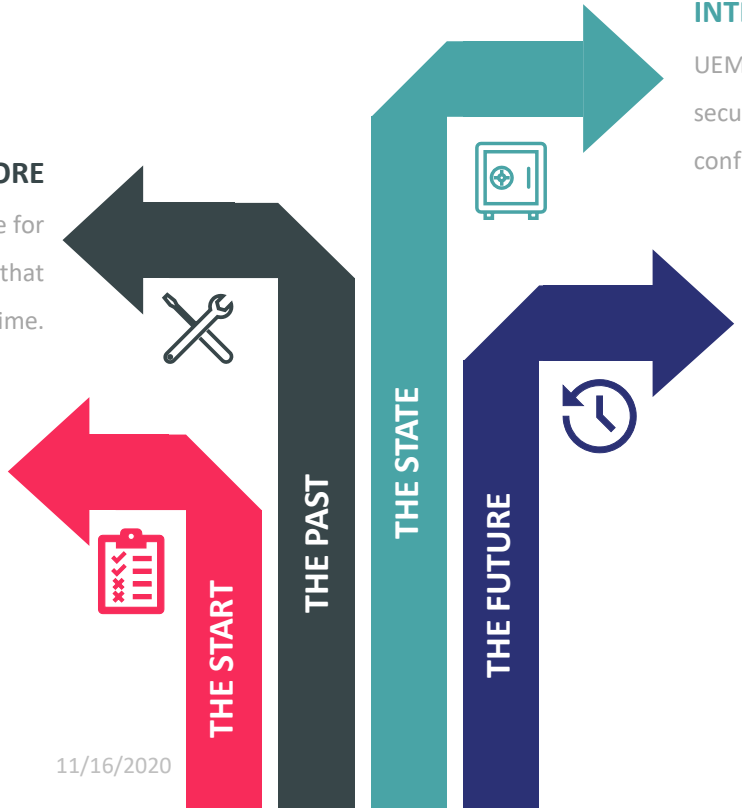
UEM as of now integrates parts of endpoint security, specifically the ones that require configuration and management per endpoint.

PATCH MANAGEMENT & MORE

Patch Management is the best example for further capabilities around security that have been added over time.

MANAGING SECURITY SETTINGS

GPOs, local configuration settings, etc. – these always have been focus of Client Lifecycle Management. And configuration management relates to security, always.



ENABLING RAPID RECOVERY & MORE

Future focus must be on enabling rapid recovery, e.g. in case of ransomware attacks. Beyond that, there is a potential for further convergence with full EPDR solutions.

Major Security Capabilities we see in UEM

Key security-related capabilities we see, we expect, or we would like to see in UEM solutions

CONFIGURATION MANAGEMENT

Managing device configurations for all devices and across a range of settings is a foundation for security – many settings are security-specific or at least security-related.

PATCH MANAGEMENT

Patch Management including the reporting about the status is an essential management, ever more in these days of ever-increasing cyberattacks.

DEVICE MANAGEMENT

Managing devices and reporting about their security, e.g. around authentication, is another key capability we expect to see. Known, managed devices and the information about their health status is essential.

DATA MANAGEMENT

Managing data on devices and segregating personal from business data also counts amongst the key capabilities.

CONTENT MANAGEMENT

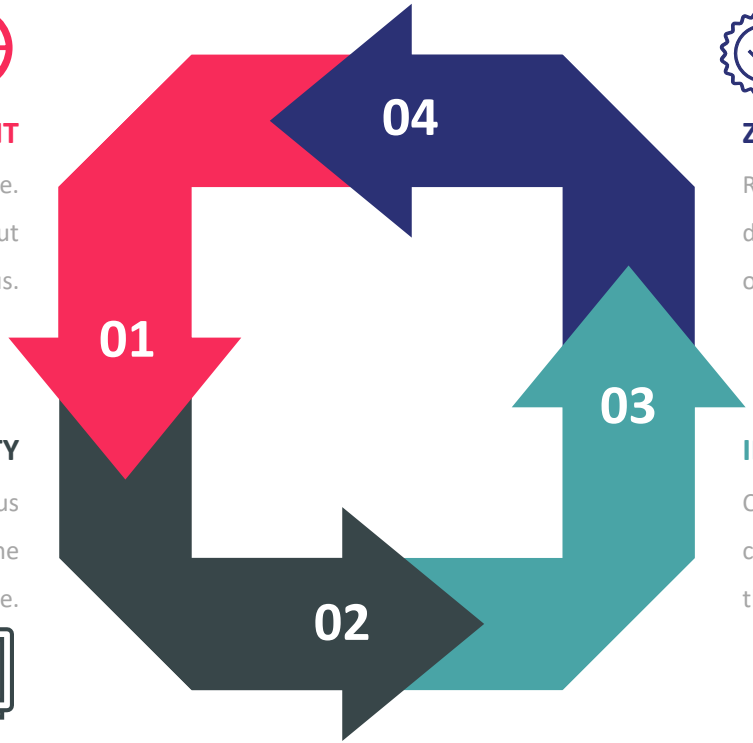
Beyond just segregating personal and business data, data encryption and access control are additional elements in a comprehensive UEM solution.

APPLICATION MANAGEMENT

Application management, from delivery to black-/whitelisting to configuration, also adds to a comprehensive security approach.

Zero Trust: UEM, Endpoint Security & IAM

How integrating and connecting different technologies helps in making Zero Trust models a reality



UNIFIED ENDPOINT MANAGEMENT

Knows the device. Knows the state of a device. Protects a device. Can deliver information about the device status.

ENDPOINT SECURITY

Adds local security. Should provide status and health information back to the device.

ZERO TRUST

Relies on continuous verification of devices and identities, building on what other technologies deliver.

IDENTITY & ACCESS MANAGEMENT

Can map identities and devices. Should consume current status information. Should use that context for authentication decisions.

Elements of a Successful UEM Strategy

Five recommendations for your UEM strategy and why the interplay of UEM and security is essential

Don’t keep Mobile Device Management segregated

First and foremost, UEM is about unifying management across all types of endpoints – don’t go for a separate MDM.

Go for a broad set of capabilities in UEM

UEM also is about comprehensive capabilities, another aspect of “unified” in the term and concept of UEM.

Define the required security features and interoperability

Understand which of your security features should be in UEM and where interoperability is key – but don’t look at this isolated.

Understand the role of UEM in Zero Trust Architectures

UEM then will and can play a vital role in your Zero Trust architectures, delivering information about the device state to other services.

Go beyond the standard use cases, look at the worst case

Just setting up new devices and managing standard use case is not sufficient anymore – the ability for rapid mass restore become essential.

SUMMARY

UEM is more than Client Lifecycle Management

Traditional Client Lifecycle Management isn't sufficient anymore – unification beyond the standard capabilities is key.

UEM is about security, but don't go over the top

UEM must (and will) support security. However, not all security capabilities must and shall be part of it – understand what should be in and what better is integrated.

UEM is an essential element for Zero Trust

There is no comprehensive approach on Zero Trust without UEM. Device management and device state information is essential to Zero Trust.

UEM must prepare for rapid recovery

The next important step is thinking beyond the standard use cases and looking at worst case scenarios, e.g. wide-spreading ransomware attacks.

KuppingerCole Analysts AG
Wilhelmstr. 20 - 22
65185 Wiesbaden | GERMANY

P: +49 | 211 - 23 70 77 - 0
F: +49 | 211 - 23 70 77 – 11

E: info@kuppingercole.com
www.kuppingercole.com