Futurism EndPoint Secure

A cognitive approach to unified endpoint management

Futurism
EndPoint Secure

Highlights

- A smarter way to secure and enable endpoints, end users and everything in between
- Efficiently manage diverse devices, including laptops, desktops, smartphones, tablets, wearables and Internet of Things (IoT) devices
- Support all major platforms including Apple iOS and macOS, Google Android, and Microsoft Windows
- Provide broad Microsoft support, from legacy Microsoft Windows XP SP3 to the modern Microsoft Windows 10
- Unify endpoint visibility, management and security with a single console
- Identify risks, opportunities and efficiencies with insights and analytics from IBM® Watson® cognitive technology and IBM X-Force® threat intelligence

While it might be desirable to standardize end users on one or two types of devices that all run the same operating system, most organizations don't have that luxury. Today's users demand an extraordinary level of flexibility and convenience—which means most organizations support a vast assortment of endpoints, including laptops and desktops (both PCs and Macs), tablets and hybrid devices, smartphones, and even wearables and IoT devices.

Not only do employees use a variety of form factors, but they run a variety of platforms on those devices, including iOS and macOS, Android, and Windows.

To complicate the situation further, they run different versions of those platforms—for example, they may run Windows XP SP3, Windows 10, or anything in between.

To wrangle these mixed-device environments, many organizations end up relying on various point solutions to get the job done (e.g., a combination of mobile device management [MDM] and client management tools). These tools generally don't integrate with each other, don't provide a consolidated view of device security status and user activity, and don't allow IT administrators to consistently apply and enforce management policies. The solution? Unified endpoint management (UEM)—with a smarter approach that allows IT administrators to consolidate management of all types of devices, regardless of form factor, platform or operating system version.

Futurism
EndPoint Secure

Futurism Endpoint Secure for cognitive UEM

Futurism Endpoint Secure ® provides a cloud-based, comprehensive UEM solution that helps IT organizations manage and secure a het- erogeneous pool of endpoints, end users, and everything in between—including their applications, content and data.

Futurism Endpoint Secure delivers robust UEM capabilities across all major computing platforms, including iOS, macOS, Android and Windows devices. And where competing solutions offer incom- plete support for legacy Microsoft platforms, Endpoint Secure supports Windows XP SP3, Microsoft Windows Vista, Microsoft Windows 7, Microsoft Windows 8, Windows 10 and Microsoft Windows 10 Mobile. These capabilities include:

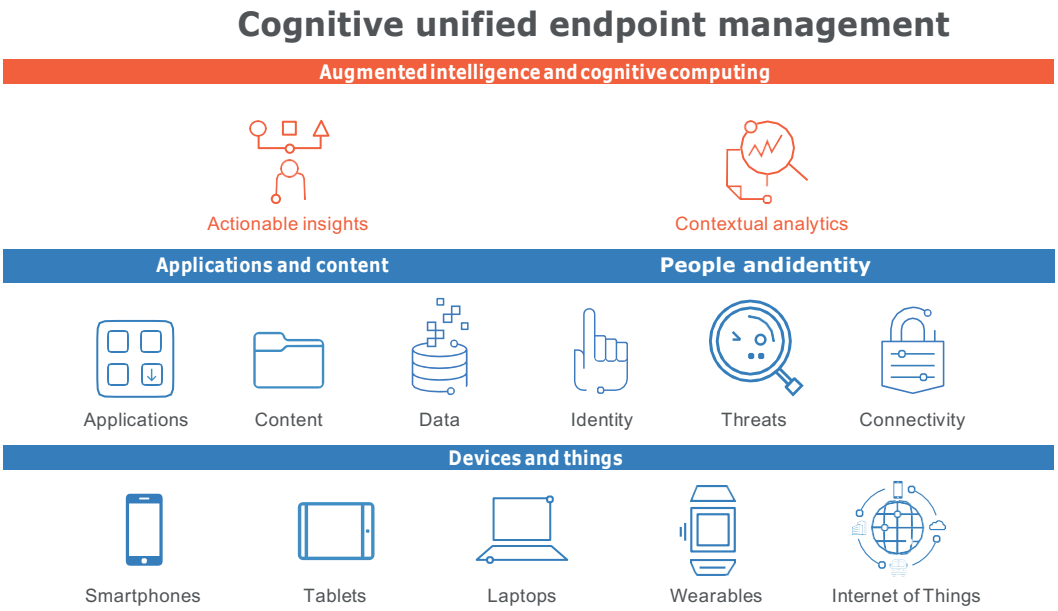
- Identity and access management (IAM) that allows a shift from a device-based context to a more comprehensive, user-based context
- Application management, including an intuitive, universal application catalog for iOS, macOS, Android and Windows, advanced bundling and promotion features, bulk application purchase and distribution capabilities, and fine-grained data controls
- A user-friendly, encrypted container to secure corporate email, web browsing and application data
- Insights and analytics from IBM Watson cognitive technology and IBM X-Force threat intelligence
- Detection and defense against malware and advanced threats with automated remediation capabilities
- Management and security of specialized use cases for wear-ables, ruggedized devices and the IoT

Endpoint Secure provides not only a single pane of glass for consistent endpoint visibility, reporting and analytics across diverse form factors, but also a single management console that consolidates endpoint management tasks across all devices, whether they are managed by application programming interface (API) sets, agents or both.

Endpoint Secure also provides:

- Robust security capabilities, including an automated enforce-ment rules engine
- Reporting dashboards and inventory capabilities for endpoints and their associated applications
- Granular control over operating system and software patch-ing policies, allowing IT administrators to customize mainte-nance and management of legacy devices

As an exclusively cloud-based offering, MaaS360 facilitates fast deployment, helps minimize your endpoint management footprint and costs, and ensures that you always have the latest software versions, including updated code as platform vendors release expanded APIs.



Converging APIs and agents

Thanks to API sets for iOS, macOS, Android and Windows 10, managing the devices that run on those platforms is far easier and more efficient than traditional agent-based client management. But legacy devices and platforms still require the agent-based approach to ensure they stay patched, updated and securely under IT control. In some cases, the most effective approach is to use both methods in tandem—a hybrid of API sets and agents. Endpoint Secure converges both methods, allowing organizations to leverage a single solution to manage all endpoints.

For those in IT management and security that are still supporting legacy Windows devices such as Windows 7-based laptops, Endpoint Secure allows a simple, seamless transition to Windows 10, eliminating the need to phase out old management tools and replace them with new ones. Thanks to Microsoft APIs for Windows 10, organizations can use Endpoint Secure to more easily migrate from traditional agent-based device management to API device management—all with one platform.

The Futurism Endpoint Secure with Cognitive Approach

While alternative solutions provide incomplete coverage across computing platforms, Endpoint Secure delivers cognitive UEM across all endpoint types including smartphones, tablets, laptops, desk- tops, devices designed for the IoT, ruggedized devices and wearables. And while competing solutions provide incomplete coverage of Windows devices, Endpoint Secure can support the full spectrum, from Windows XP SP3 to Windows 10.

Traditional mobile device management systems were built in a simpler time for tactical purposes and disparate mobility proj- ects. With the industry's first cognitive UEM platform, Endpoint Secure with Watson delivers a single, strategic management and security solution to drive your organization's digital busi- ness transformation.

Endpoint Secure delivers powerful insights and analytics so that businesses can make more informed endpoint

cognitive technology, IBM X-Force Exchange threat intelligence and cloud-sourced benchmarking data from the Endpoint Secure platform.

Insights and analytics from Endpoint Secure with Watson can help organizations maximize their return on investment for their mobile strategies—and realize it faster—by identifying business opportunities, increasing workforce productivity, boosting IT operations efficiency, minimizing security risks and helping the business make more informed endpoint decisions, including spending decisions. Endpoint Secure insights and analytics include three key capabilities:

- **Advisor,** which delivers actionable intelligence that is contex- tual to the organization
- **Mobile Security Index,** which provides the industry's first publicly available mobile security scorecard
- **Mobile Metrics,** which offers the industry's first cloud- sourced endpoint benchmarking data

As part of the larger IBM Security portfolio, Endpoint Secure also pro- vides key IBM technology integrations with solutions such as IBM BigFix®, IBM QRadar® SIEM, IBM Trusteer® and IBM Security Access Manager to maximize your IT investments.

EndPoint Secure offers the industry's first cognitive approach to unified endpoint management.