BARAMUNDI MANAGEMENT SUITE 2019 R2

Enterprises struggling to manage and secure their desktops and mobiles need a unified endpoint management (UEM) solution to wrest back control. The baramundi Management Suite (bMS) is a very capable UEM product and its smart modular design means you can customise it precisely to your IT department requirements and budget.

baramundi has an answer for everything, as the suite comprises no less than 19 modules, ranging from compliance and patch management, vulnerability scanning and automated software updates, through to mobile device management (MDM), hardware and software inventory, OS deployment and even energy management.

This latest version adds several valuable new features, as the Defense Control module can inventory managed systems that use BitLocker, report on the status of encrypted partitions and allow administrators to centrally manage encryption. The Mobile Devices module can now natively separate company and personal data on Android devices by applying bMS work profiles.

bMS is truly unified, as every module can be managed centrally from a single console and it's also very easy to install. We loaded it on a Windows Server 2019 host and used the supplied SQL Express 2017, which is sufficient to manage around 350 endpoints.

The bMS console is very well designed and presents a single pane of glass for managing all aspects of your IT environment. It opens with a clear overview that provides six charts showing managed clients, job status, detected operating systems and Windows vulnerabilities, along with macOS and mobile device compliance.

Each managed device requires an agent and, for our Windows desktops, we could deploy this manually or automate it with the Active Directory Sync import feature. Mobile devices are added manually, require an enrolment token and, once they are registered, the mobile agents can be installed.

It was also a manual affair for our macOS MacBooks, although it didn't take long as we downloaded the install package to each one, pointed them at the bMS server and entered the supplied authorisation codes. The macOS agent is completely transparent to users and, from the bMS console, we could assign compliance rules to control app usage or check OS versions, and detect jailbreak attempts on iOS and Android devices.

Once the agent was deployed to our systems, we viewed them from the Environment page, which offers filters for Windows, macOS, iOS, Android and Windows Mobile devices. A separate section is provided for adding VMware vCenter or vSphere virtualisation hosts and, after creating a scan with an SNMP profile, bMS discovered all our network devices with this service running and populated its Environment page with them.

The Compliance Management module provides tools for running regular vulnerability scans on selected systems and groups. Scan results are viewed from the console's Compliance overview page where it provides clear breakdowns of critical vulnerabilities and configuration rule violations for Windows, mobile and macOS devices.

The Patch Management module can replace Microsoft's WSUS or work alongside it and provides facilities for scheduled rule-based automated patching, using a centralised distribution point either on the bMS host or another location of your choosing. A key advantage of this module is it can fully manage and deploy patches for third-party applications and bMS maintains up-to-date lists of thousands of apps, so you can ensure users are always running the latest versions.

We were impressed with bMS, as it's surprisingly simple to deploy, while its smart central console provides easy access to every feature. baramundi delivers a sophisticated modular UEM solution that can be easily customised to suit, and is clearly capable of putting endpoint control and security firmly back in the hands of IT administrators.

Product: Management Suite 2019 R2
Supplier: baramundi software AG
Web site: www.baramundi.com
Sales: sales@baramundi.com