Address today's BYOD challenges

HP Intelligent Management Center for BYOD

Who are you?

Is your device compliant?

Assigned to virtual app networks

Identity authentication ①

Authorized user

Device authentication ②

Clean

Authentication ③

Corporate network

I'd like access

Unclean

Quarantine area

Behavior monitoring ④

Ongoing compliance management
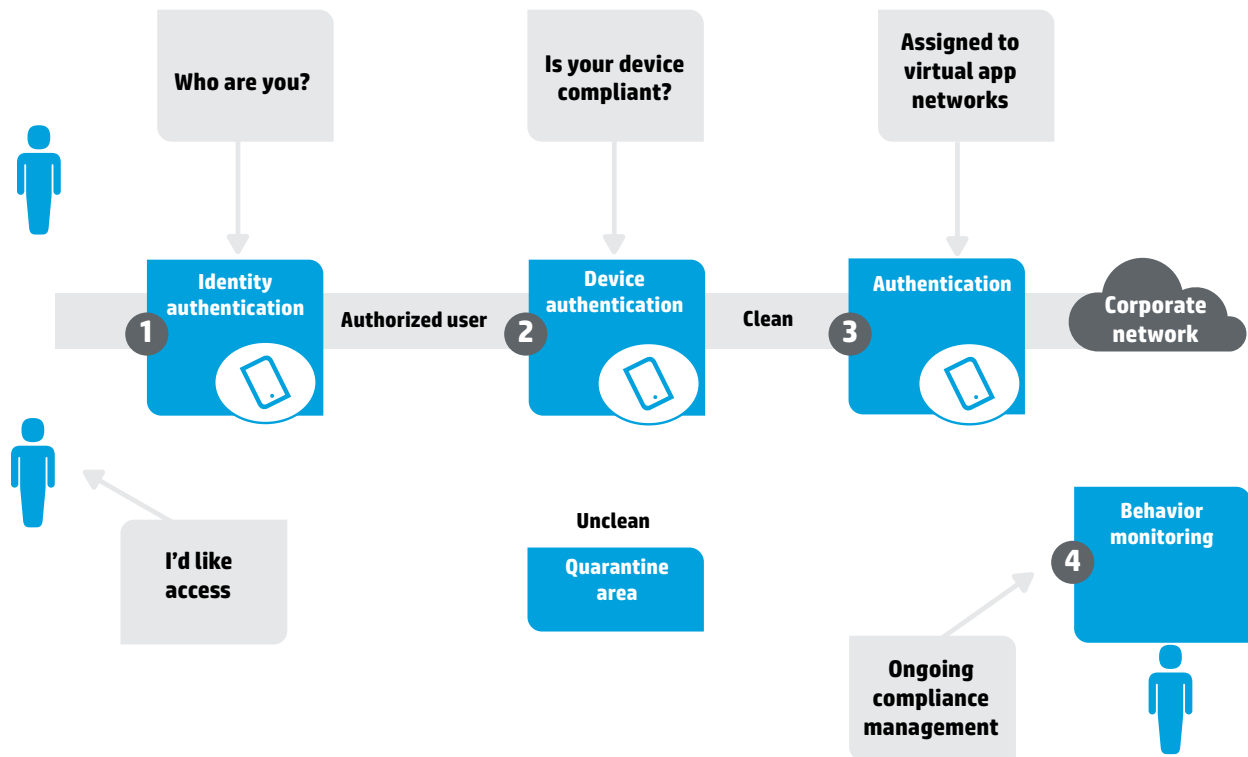
What do you need for "Bring Your Own Device" to be effective?

Mobile devices are an attractive choice for employees, since they help in increasing their productivity and flexibility yet providing a cost effective option for enterprises. While more and more organizations are adopting the new initiative of "Bring Your Own Device" (BYOD), IT organizations are facing challenging issues such as preserving network integrity, securing user access, and controlling wired and wireless networks.

Based on a recent SANS BYOD/Mobility security survey[1] of 500 IT professionals, customers require a BYOD solution that offers:

• Centralized functionality

• Logging and monitoring

• Ease of deployment

An effective BYOD solution should deliver an access-agnostic solution that leverages a universal security and compliance policy across wired and wireless devices while reducing the IT burden with an easy-to-use self-registration process. It also should integrate with your current infrastructure management tools to ease deployment. In addition, you require a solution that provides adequate visibility of network traffic and application usage for capacity planning and compliance reporting.

[1] "SANS Mobility/BYOD Security Survey,"
 Kevin Johnson, SANS, March 2012.

Complete, unified bring-your-own-device (BYOD) solution
Simple, scalable, and secure
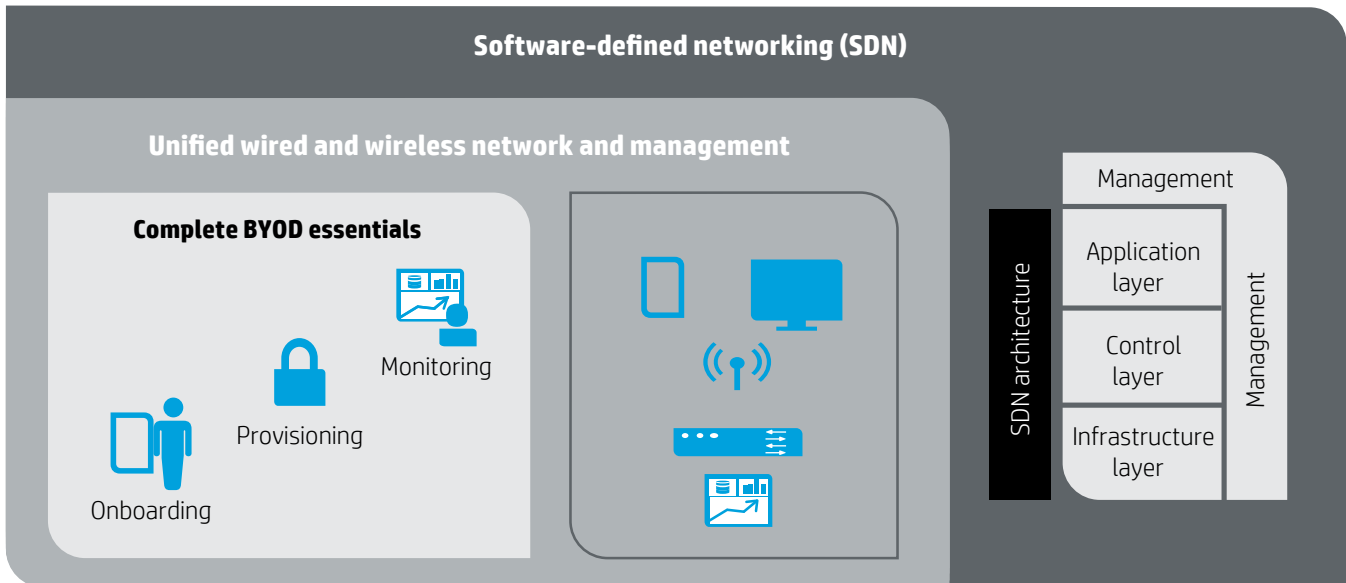
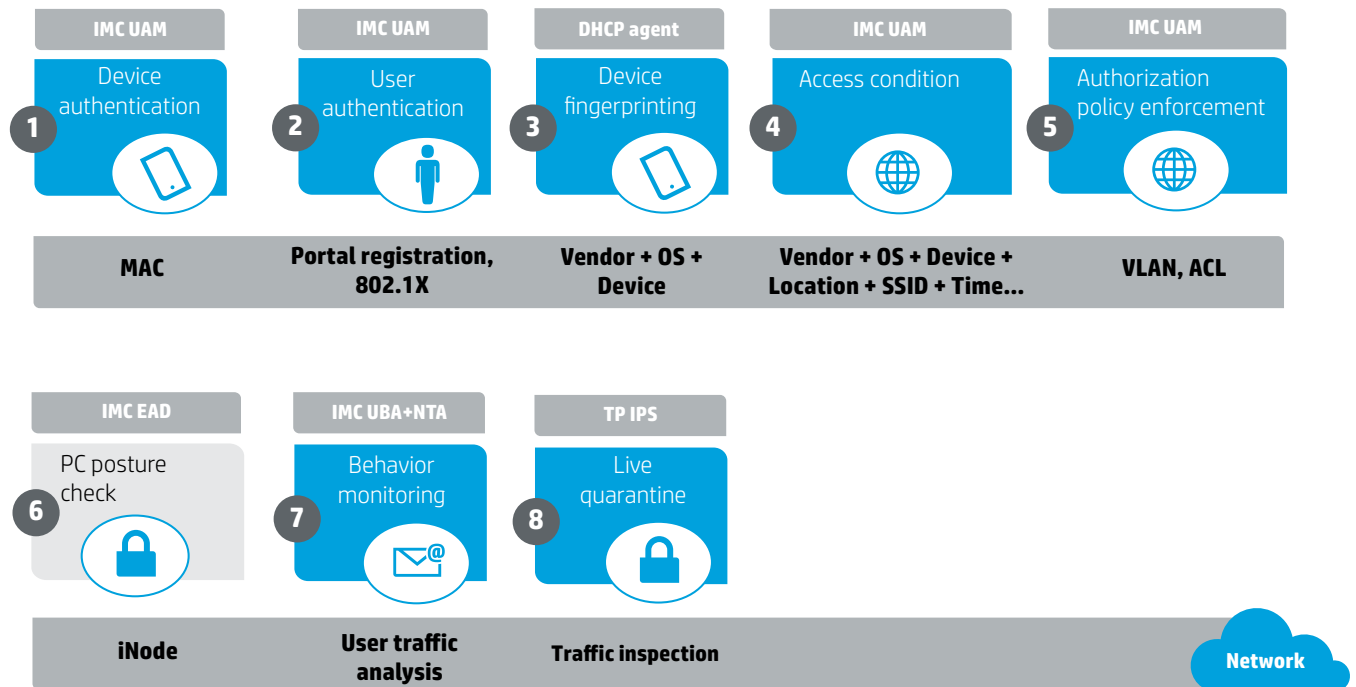## Protect your network with HP Intelligent Management Center BYOD Solution

HP Intelligent Management Center (IMC) BYOD solution is based on IMC which delivers single pane-of-glass management with complete visibility across the entire enterprise network.

IMC is part of the HP BYOD solution which goes beyond what is offered in the market with a complete, unified approach to solving BYOD challenges. The HP BYOD solution starts with the BYOD essentials—simple and secure on-boarding, provisioning, and monitoring, delivered by IMC.

BYOD essentials functionalities include:

• Secure user authentication, advanced device profiling, and real-time traffic quarantine

• Centralized authentication, authorization, and accounting support

• Seamless policy enforcement across wired and wireless infrastructures from HP or other vendors

• Unified monitoring of device traffic and user behavior

• Comprehensive, unified network management with third-party network support

IMC further pushes the BYOD essentials to deliver unified network management creating single network for wired as well as wireless connectivity. Finally, the HP BYOD solution will prepare your network for Software-Defined Networking (SDN).

IMC UAM	IMC UAM	DHCP agent	IMC UAM	IMC UAM
1 Device authentication	**2** User authentication	**3** Device fingerprinting	**4** Access condition	**5** Authorization policy enforcement
MAC	Portal registration, 802.1X	Vendor + OS + Device	Vendor + OS + Device + Location + SSID + Time...	VLAN, ACL

IMC EAD	IMC UBA+NTA	TP IPS	
6 PC posture check	**7** Behavior monitoring	**8** Live quarantine	
iNode	User traffic analysis	Traffic inspection	**Network**

HP IMC BYOD solution—key components

The HP IMC BYOD solution is extremely flexible and can be tailored to meet certain BYOD requirements. This flexibility is afforded by IMC's modular and expandable architecture.

To get started with the IMC BYOD solution, you will need the base platform IMC Standard Edition and IMC User Access Manager (UAM) which provides secure, policy-based network access. To that, you can add modules to the base solution to expand your BYOD's solution capabilities to cover posturing, user and traffic monitoring or wireless management. Alternatively, HP also offers BYOD solutions delivered as a virtual appliance, also based on IMC.

The IMC Smart Connect Virtual Appliance is a great solution for smaller deployment as it offers all the necessary tools for your BYOD requirement. However, if you are looking for growth and flexibility, the HP IMC Standard with additional modules could be the right choice.

A comprehensive BYOD solution will rely on the following IMC modules:

- **IMC User Access Manager (UAM)** provides user access, guest access management, device fingerprinting, and self-registration.
- **IMC Endpoint Admission Defense (EAD)** reduces network exposure and monitors the endpoints.
- **IMC Network Traffic Analyzer (NTA)** provides traffic monitoring and capacity planning.
- **IMC User Behavior Auditor (UBA)** provides usage monitoring.
- **IMC Wireless Services Manager (WSM)** provides converged wired and wireless management.

IMC User Access Manager

The IMC UAM module provides all the capability required for network access. It supports user identity authentication and extends management to wired, wireless, and remote network user enabling the integration, correlation, and collaboration of network device management and user management on a single unified platform.

This solution provides centralized authentication, authorization, and accounting management of endpoints that connect and use network services. The module helps reduce vulnerabilities and security breaches through its policy management and through live quarantine, enabled by integration with HP TippingPoint Intrusion Prevention solutions. User Access Manager includes device fingerprinting to enable granular user policy management.

IMC Endpoint Admission Defense

The IMC Endpoint Admission Defense (EAD) module reduces network exposure by integrating security policy management and endpoint posture assessment to identify and isolate risks at the network edge.

In addition, the module reduces the risk of malicious code infections or other security breaches by detecting endpoint patches, viruses, address resolution protocol attacks, abnormal traffic, the installation and running of sensitive software, as well as the status of system services. EAD provides continual monitoring of endpoints.

IMC Network Traffic Analyzer

The IMC NTA module is a graphical network-monitoring tool that provides real-time information about users and applications consuming network bandwidth. The IMC platform functionality enables the operators to apply varying levels of bandwidth traffic to different services and applications.

The IMC NTA module's network bandwidth statistics help plan, monitor, enhance, and troubleshoot networks, as well as identify bottlenecks and apply corrective measures for enhanced throughput. The module also monitors Internet egress traffic, helping administrators to analyze the bandwidth usage of specific applications and monitor the impact of non-business applications.

IMC User Behavior Auditor

The IMC UBA module provides enhancement of overall network performance by enabling network administrators to audit user behavior. Administrators can also audit user activity by email sender or receiver addresses, database access and operations, file transfers, and FTP access.

The UBA module provides control over filtering, data aggregation, and application identification and definitions. UBA generates summarized audit reporting with the ability to query, sort, and group audit results by many fields as well as the ability to save audit results to a file for download.

IMC Wireless Service Manager

The IMC WSM integrates wireless service management into IMC's network management platform. Together, they provide unified management of wired and wireless networks.

The WSM module provides WLAN device configuration, topology, performance monitoring, RF coverage and planning, WLAN intrusion detection and defense, and WLAN service reporting for HP wireless infrastructure. The module detects wireless attacks as well as rogue access points and alert on vulnerabilities in the network. WSM generates historical reporting, enabling operators to monitor how wireless network usage, performance, and roaming patterns have changed over months or years.

HP IMC BYOD solution bundles

IMC Smart Connect Virtual Appliance

The IMC Smart Connect Virtual Appliance edition makes it easy for you to deploy BYOD as a single software package. The virtual appliance comes in two packages—IMC Smart Connect Virtual Appliance and IMC Smart Connect Virtual Appliance with WLAN Manger. The IMC Smart Connect Virtual Appliance includes IMC Standard Edition and IMC UAM that provides user access, guest access management, and device fingerprinting and self-registration.

IMC Smart Connect Virtual Appliance with WLAN Manager

The IMC Smart Connect Virtual Appliance with WLAN Manager offers all the capabilities of the previously described virtual appliance and in addition includes a single policy enforcement and converged network management across wired and wireless environments.

Unified BYOD monitoring further enables administrators to plan for capacity and comply with regulatory requirements. This software is offered as a virtualization appliance to allow for zero installation and easy deployment. As a bonus, IMC Smart Connect solutions provide comprehensive network management which includes third party network management.

IMC solutions	Network Management	User Access	Device Health	User Monitoring	Wireless Management	Traffic Monitoring
Base components						
IMC Standard Edition	✓					
UAM		✓				
Additional components						
WSM					✓	
EAD			✓			
UBA				✓		
NTA						✓
Virtual appliance						
IMC Smart Connect Virtual Appliance	✓	✓				
IMC Smart Connect Virtual Appliance with WLAN Manager	✓	✓			✓	

Why choose HP IMC BYOD solution

Simple, secure, and scalable, the HP IMC BYOD solution is designed to address the complex challenges that IT professionals are facing by the proliferation of personal devices across the enterprises. The IMC BYOD solution provides a single pane-of-glass management with centralized security, visibility, and control. The modular design allows you the flexibility to customize solutions based on your needs. You could also select IMC Smart Connect Virtual Appliance or IMC Smart Connect Virtual Appliance with WLAN Manager for zero installation and ease of deployment.

For more information

Global citizenship
Developing solutions to major social and environmental challenges
hp.com/hpinfo/globalcitizenship/

To learn more about HP BYOD solutions visit
hp.com/networking/byod.

To learn more about HP Intelligent Management Center
hp.com/networking/imc.

Sign up for updates
hp.com/go/getupdated

Share with colleagues   Rate this document

4AA4-5149ENW, February 2013