The Evolved BYOD Secure Solution

Increase productivity, connectivity and security through Cisco Identity Services Engine (ISE).

The Challenge

The increase in mobile connectivity and people bringing their own device into the workplace is presenting a new headache for IT departments as they look to keep their networks secure, whilst enabling staff the flexibility of using a device of choice.

Depending on the figures you read, less than 10% of organisations feel they were fully aware of the devices accessing their network, even though over 60% allowed staff to bring their own devices into work each day. These are alarming statistics for organisations that spend thousands of pounds securing their network infrastructure only to be infiltrated by a mobile device that could cost less than £100.

In order to strike a balance between network security and staff productivity, organisations need to develop a BYOD security policy that addresses the overall needs of a business and its BYOD environment. The policy needs to identify the type of devices that could be connecting to the network and provide users with seamless access to corporate networks regardless of the device type, or where it is connecting from.

As the borders between personal and professional lives continue to merge into one, network security is no longer about how to keep people out, but more about how to let them in. IT departments are tasked to strike a balance between IT security and employee enablement – allowing users to collaborate their applications in line with the needs of the business.

What's your BYOD policy?

A successful BYOD implementation needs to be able to track all connections to the network, prevent unauthorised access, enforce role-based profiles for authorised users, follow compliance requirements, and ensure security policies are adhered to.

Finding the right partner who has access to the technical expertise, vendor accreditations, security certifications and business acumen to deliver a successful BYOD deployment is paramount if organisations want to remain secure and operationally efficient by empowering their workforce.

Policy	Limited Access	Basic	Enhanced	Advanced
Enforcement	Corporate-only devices	Broad range of device types but access to the Internet only	Multiple device types and access methods	Multiple devices with new services
Example	Financial services - company restricts access to confidential financial data	Educational institution - allows basic services to everyone (e.g., email)	Healthcare organisation - offers differentiated services based on role (e.g., email and select corporate data)	Mobile sales enterprise - offers videos and collaboration sessions

Solution

The Evolved BYOD Solution provides a comprehensive approach to effectively design, manage, and control the end-to-end deployment of a secure BYOD network. The solution focuses on user experiences and productivity, creating a seamless integration of technology that complements the needs of a business.

This overall solution based on Cisco Identity Services Engine (ISE) technology starts with design guides and professional services that lead you from planning and design into day-to-day operations. This BYOD solution also provides the necessary infrastructure, including:

- Access points
- Controllers
- Security
- Link failures
- Network management

This infrastructure supports a highly secure, high-performing network that is accessible to a wide range of devices that brings a number of benefits to an organisation and its workforce.

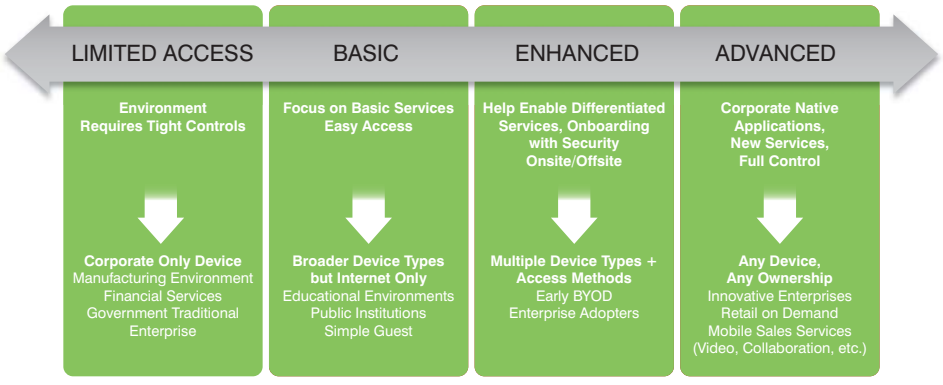
Evolved has access to a broad range of design guides that provide tested and proven architectures to help you implement a scalable, highly secure mobile solution. These designs help decrease deployment risks and accelerate the benefits.

The Evolved Secure BYOD Solution, based on Cisco ISE technology, delivers a unified security policy across the entire organisation, as well as an optimised and managed experience for users with diverse device, security, and business requirements. This truly experience-centric solution also delivers context-aware on-boarding and secure access to resources. It transforms the workspace, resulting in a productive user and IT experience without sacrificing security, visibility, or control.

Core components of Evolved's secure BYOD solution include:

- Policy-governed unified access infrastructure
- Efficient and seamless security
- Simplified management

The Evolved BYOD range of services



Policy-Governed Unified Access Infrastructure

A policy-governed unified access infrastructure ensures secure access to data, applications, and systems with high-performance connectivity for every device. Evolved can provide customers with a single source of policy across the entire organisation for wired, wireless, and VPN networks, dramatically increasing security and simplifying network management.

The Cisco Identity Services Engine, is a unified, policy-based service enablement platform that helps ensure the corporate and regulatory compliance of devices connected to your network. It uniquely gathers real-time contextual information from the network, from users and from devices, then makes proactive governance decisions by enforcing policy across the network infrastructure.

The policy decision is based on who is trying to access the network, what type of access is requested, where the user is connecting from, when the user is trying to connect, and how (with what device). The Identity Services Engine includes guest posture, device profiling, network access, and mobile device management, and offers simple device registration and on-boarding for the customer.

The Cisco Intelligent Network infrastructure includes a complete portfolio of wired, wireless, and VPN access points. Security is uniquely embedded into selected network infrastructure to provide greater visibility and enforcement.

With Cisco solutions, the network acts as a platform to offer services such as video and to protect people and organisations. Cisco's network leadership and expertise sets Cisco apart from other providers in its ability to provide highly secure BYOD environments.

Once an organisation determines its BYOD policy, Evolved will install Cisco network products and the Cisco ISE, allowing you to provision and deliver cross-domain application and network services more securely and reliably across all network environments.

Policy-governed unified access infrastructure creates a highly intelligent network that enables easy business transformations with superior protection.

The Cisco ISE Partner difference delivered by Evolved

- Single source of policy for the entire organisation: wired, wireless, or remote networks; physical or virtual devices.
- Highest-performance, highest-quality wireless infrastructure: up to 30 per cent faster compared with the competition, delivering the best user experience.
- Broadest mobile device OS support through Cisco AnyConnect VPN software, including iOS, Android, and Windows Mobile.
- Deepest, broadest, and most accurate device knowledge.
- Scalable and flexible next-generation enforcement mechanism using existing identity-aware infrastructure.
- Simple end-user on-boarding and device registration to ensure end-user and IT productivity.
- Secured and encrypted wireless data from the device to the controller, delivering more protection and compliance.
- Optimised experience for virtual and native desktop infrastructure.
- Unified management across wired and wireless and policy.

Benefits

Businesses that adopt a BYOD policy allow themselves to save money on high-priced devices that it would normally be required to purchase for their employees. This approach then facilitates a choice for employees who are able to decide on the technology that they wish to use for work, rather than being assigned a restrictive company device. This can improve productivity, morale and loyalty that an employee has with a firm whilst the company benefits from newer, faster technology enabling their workforce. In many circumstances employees also tend to take better care of devices that they view as their own property.

- Move towards a 'universal desktop on any device' architecture.
- Improve productivity and loyalty by empowering employees with the option to select their device of choice.
- Best-of-breed secure BYOD solution Based on Cisco ISE technology.
- Implement a secure infrastructure that encourages the use of BYOD through user enablement.
- Reduce Capital Expenditure (CAPEX) on IT infrastructure with less need for company-owned devices.
- Drive best practice recommendations to meet stringent data privacy and compliance requirements.

Looking ahead

As organisations become more confident around the security of BYOD, users will increasingly demand a 'universal desktop on any device' environment where the network intelligence is stored in a central location and accessed from a device of choice. This will see BYOD and the increased use of tablets such as iPads driving the need for organisations to move over to a Virtual Desktop Infrastructure (VDI) where vendors such as Citrix (Xen App) and VMware are able to virtualise the software applications on a network. This will reduce the need for large capital expenditure on IT hardware as people's own devices will be accessing the network in the same way as a desktop or laptop does. In addition, moving over to a VDI also reduces the amount of bandwidth required as all data is stored centrally, with the device only making updates to a file or document rather than downloading the whole file.

For more information please contact us today:
Tel: +44 (0) 1279 437 444
www.evolvedis.com