About This White Paper

This white paper examines the key requirements that are emerging for BYOD (Bring Your Own Device) implementations in public sector networks. It reveals ContentKeeper’s approach to a variety of BYOD requirements and why this approach offers significant advantages and savings over other offerings.

After reading this white paper, the reader should have a greater understanding of the implications of BYOD adoption in network environments and what factors must be considered to ensure optimum mobile Web security.

Introduction

The proliferation of Smartphones and other Web-enabled mobile devices has dramatically altered the way government agencies and employees utilize the Internet. Users are no longer physically tethered to workstations in fixed locations. Today, employees can utilize multiple types of devices and computers to connect to the Web in a wireless network environment. Many agencies want to enable this kind of agnostic device flexibility, commonly known as Bring Your Own Device (BYOD), due to budget constraints but are hesitant or unsure about how best to deploy it due to security and compliance concerns.

BYOD is fraught with a multitude of serious IT security risks, potential costs, regulatory compliance loopholes and data privacy issues. There is a clear need to approach the security concerns around BYOD with a degree of caution and informed advice.

What is required is a simple and secure solution for BYOD scenarios in network environments that is cost effective, flexible, proven, reliable and (perhaps most importantly) easy to support and implement.

Mobile Device Accountability and Control

At ContentKeeper we call this solution concept Mobile Device Accountability and Control (MDAC). This is merely a way of defining the security capabilities that many agencies are typically looking for to answer the risky questions around BYOD adoption. For ContentKeeper, MDAC is a built-in capability in our standard Web Filtering technology solution.

Enabling BYOD means that agencies can harness the full potential of the Web with next-generation mobile technology, and do this affordably, without additional IT resources or effort. It also means that agencies can enable staff to work how they want to work, without compromising security or compliance standards.

What is Fueling BYOD Adoption?

BYOD is a rapidly growing concept driven by the exponential growth of Web-capable mobile devices and Smartphones. This coupled with widespread and readily available wireless Internet access has meant that employees are bringing their own mobile devices to work. IT staff want to be able to monitor these devices on the network and users want to be able to utilize their favorite devices at work, which are often prohibited.

A 2013 survey on Bring Your Own Device (BYOD) uptake by Holger Schulze that polled 160,000 IT professionals found the biggest positive benefits of adopting BYOD included:
• Greater worker satisfaction by enabling users to utilize their preferred mobile device.
• Improved mobility and flexibility enabling workers to access the Web when and where they need to.
• Improved efficiency and utilization of online resources as a result of greater flexibility and enabling users to work on devices that they are most familiar with.

However, BYOD introduces many challenges to maintaining IT security, legal compliance and safeguarding confidential data and employee privacy. The same Holger Schulze survey found that the biggest concerns with BYOD were:

• Ensuring authorized Web/network access and maintaining security policy compliance
• Preventing data loss
• Increased exposure to malware attacks

Government agencies are looking to enable BYOD because of the aforementioned benefits. But, many are hesitant to do so or unsure how to approach it with limited budgets, resources and already established Web filtering technologies which don’t natively support BYOD requirements. There are numerous questions that make the challenges of implementing BYOD almost seem to outweigh the potential benefits.

What devices do you support? Which ones are the most secure or prone to security vulnerabilities? Can you be device agnostic? How do you identify devices and authenticate users without having to “touch” the device in an administration sense? How do you ensure secure and appropriate Web use for mobile devices and mobile data transactions?

This Whitepaper examines how agencies can support BYOD and managed device deployments with ContentKeeper technology while mitigating and even eliminating many of the common pitfalls. We will look at how BYOD is driving major changes in IT requirements and how agencies can achieve the level of Mobile Device Accountability and Control (MDAC) they desire with a minimum of effort, cost or disruption to their existing IT infrastructure.

**What is BYOD?**

BYOD essentially refers to the ability for a known employee or guest user to bring his or her own mobile device onto an agency’s network and connect to the Web in a secure and properly authenticated manner. They can then access the Internet or if allowed, other internal network resources while being policy compliant even though on their personal device.

BYOD takes advantage of a user’s personal device. To offer the greatest benefits devices should ideally be managed and users authenticated without having to install software on the device. A proper BYOD strategy allows the use of any device (device agnostic), enables the IT department to identify the user, enforces the right policies and reports on the user’s activities, without necessarily requiring a client to be installed on the device or requiring major IT configuration changes.
**What Devices are Supported?**

ContentKeeper supports any type of device running any operating system. This includes:

- Laptops and notebooks (Apple, Android, Chrome or Windows)
- iPads and other tablet devices
- Smartphones, iPhones and other Web-capable mobile devices using TCP/IP and Web Protocols

Because ContentKeeper is an in-line solution (a Layer 2 Ethernet bridge design) the application of filtering and deep packet inspection is both device and O/S (Operating System) agnostic. Put simply, this means that MDAC can be applied to any Web traffic, to or from the Internet, regardless of the device used. Additionally, due to this design, Web filtering is faster and more scalable than traditional proxy-based technologies which process Web traffic at the application layer (layer 7).

**User Authentication and Directory Integration**

ContentKeeper customers are able to effectively support a proper BYOD strategy within their existing environment by using the “Form-Based Authentication” method of user resolution. This enables your agency to support any number of devices without the need for client software installation or previously registering the device.

To the user, a proper BYOD strategy means simply connecting whatever mobile device they have to the wireless network. When a user first tries to browse the Internet, an authentication page appears in their device Web browser as displayed on the top of the next page. Users can either authenticate to get their normal Web browsing policies enforced on that device, or if they are a guest user they can ignore this authentication request and be treated as an unauthenticated user. In this scenario the default browsing policy or restrictions can be whatever you wish to set for this purpose. The screenshot on the top of the next page shows the authentication page as seen on an Apple device, it can be fully customized:
The “New BYOD / Desktop Registration” screen, as shown on the next page, shows a generic device registration browser prompt that can be displayed on any device. This process requires no software installation and ensures a user must register a new BYOD mobile device they bring onto the network. This system allows users to bring their own devices, but requires network access authentication which in turn provides activity reporting for all devices users browse the Web from. This consistent tracking of authenticated Web use across multiple devices is essential to maintaining accurate reporting and effective security policy compliance.

A network administrator can create any number of groups of related account types for employees or guest users. This means that when a user registers their device they can be granted controlled Web access based on the privileges granted to their account type. Users can be authenticated using a variety of methods:

- **Guest Account** – this can be used for unknown users or visitors and enables access to a limited set of Websites such as Intranet and approved websites.
- **Directory Authentication** – ContentKeeper integrates with many common User Directory services such as Active Directory, eDirectory, OpenDirectory, Radius and LDAP. Authenticated users can then browse the Web from their device according to their account privileges.
- **Federated Authentication** – Supports authentication with Google directory services.
- **Open Registration** – Requires the user to provide information about themselves and links the user with the device MAC address.
- **Secure Registration** – Requires the user to register an email address or phone number and dynamically generate an access password.
With this process, the user is normally authenticated as long as the Web browsing session remains open. Flexible options within ContentKeeper enable you to set time-out periods, requiring re-authentication once a session is inactive for a set time. Or, if you prefer, ContentKeeper can be configured to “remember” the device and every time that recognized device is seen on the network it can be linked to the registered user account automatically.

Mobile Device Accountability and Control

Once a device is registered on the network and the user is authenticated as either a known or guest account, ContentKeeper continually tracks Web use generated on that device. Network administrators can see, at a glance, what devices are being used on the network, by whom and for what.

This screenshot above shows the ContentKeeper administration view of devices as they appear on the network. The administrator can see:

- What type of device is being used and the manufacturer
- What software version of the operating system is installed
- Which user is browsing on the device and how the user was authenticated
- How long the user has been browsing the web in the current session
- The device IP address and MAC address

In Conclusion

ContentKeeper ensures that BYOD can be seamlessly supported in government agencies with centralized device management and no requirement of special software or costly disruption to your current IT infrastructure. ContentKeeper’s in-line Layer 2 Ethernet Bridge design allows you to deploy BYOD quickly and easily and works with any existing network infrastructure or can be hosted in the cloud if desired.

ContentKeeper also supports large scale statewide network deployments that maintain systems for multiple offices or locations. In this case where a single IT provider may be responsible for multiple locations with different policy requirements, ContentKeeper can still enable seamless Mobile Device Accountability and Control for all of those networks or domains and different devices without additional costs or special hardware.