ascent

Thought leadership from Atos

white paper

Security for "Bring your Own" Concepts

Atos

Bring Your Own (BYO) concepts are now a reality in all areas of business. IT has to address it as a real world experience today rather than just being seen as pushing future concepts. At the same time Bring Your Own is no longer just about increasing user satisfaction and cost savings - the key challenge for IT in this context is to truly ensure the security of the corporate data without hindering access to user-owned data and applications.

This White Paper identifies core security challenges for BYO and maps those to strategic principles for building a methodical approach for solution designs. It shows which current solutions can be extended to meet the challenges and those that are likely to be subject to future research.

Published in June 2013

Security for "Bring your Own" Concepts

Contents

This white paper was written by the Atos Scientific Community's Security Track Team: Albrecht Becker, Marine Chaffanjon, Melanie De Vigan, Adam Dolman, Steven H. Jones, Minh Le, Martin Pfeil (Editor), Rob Price, Joël Stillhart, Chee Tan and Till Kolloge.

About the Atos Scientific Community

The Atos Scientific Community is a network of some 100 top scientists, representing a mix of all skills and backgrounds, and coming from all geographies where Atos operates. Publicly launched by Thierry Breton, Chairman and CEO of Atos, the establishment of this community highlights the importance of innovation in the dynamic IT services market and the need for a proactive approach to identify and anticipate game changing technologies.

Security for BYO - today and tomorrow

In today's workplace, one of the recent promises of evolved working practices has now become a reality - working with any device or Bring Your Own (BYO). This incorporates end users who own and provide their own smart device, ID and software to work in their company, as well as contract workers / consultants to use their device to work in other companies. Private, public and enterprise use of BYO are all increasing.

There is a growing trend in companies hiring an increasing percentage of contract workers and keeping permanent and full time staff to the minimum. Indeed, people will increasingly be contracted by more than one company at a time – working across these companies, using the same resources. There is an increased likelihood that data will therefore flow between these separate companies or domains. Different identities in different domains are not user friendly and impractical for applications that are distributed over many domains. Therefore a complete separation of the domains is not desirable. However comprehensive, cross-domain information control is nearly impossible, by law as well as by technology. In contrast, today's IT solution design is driven by requirements of company data-centric infrastructure and applications. Hence, current device management solutions try to keep the different domains separate.

It is obvious that there is no right or wrong implementation for every company, as the business model, culture, organizational spread and maturity of a company must be taken into account to define the best security concept. The table below summarises currently observed conditions regarding BYO implementations, as well as the corresponding challenges that have to be fulfilled in the future:

Currently observed conditions	Security challenge for BYO
Legacy security is enforced on the endpoint devices and by building big walls (perimeter security). The security is mostly based on the ownership of devices and networks.	▸ Security has to be shifted towards the data itself and differentiated application security services rather than legacy infrastructure and endpoints ▸ Perimeter security including endpoint security cannot fully satisfy BYO requirements. This implies the need for a disruptive mindset change about security design principles and policies ▸ Domains of use must be made permeable with respect to data without losing control. The data has to bring along its own policies that determine which kind of processing is allowed under a defined context or which actions have to be executed in case of context changes ▸ Efficient methods for semi-automated data classification have to be developed. Additional data classification efforts which cannot be automated have to be accepted.
Lack of control on the heterogeneous landscape of smart devices due to the non-standardized and highly volatile (esp. mobile) device ecosystem.	▸ Security has to be independent from the endpoint device as lack of control will even increase.
Interfaces to legacy applications are not built for mobile, service-oriented and federated system architectures.	▸ Migration of legacy systems to modern open standards including the challenge of integrating social media tools and other cloud-based applications without full control (bigger attack surface has to be handled).
Bandwidth and online time is limited. Devices and applications need an "offline mode" with secure local storage, processing and synchronization.	▸ Replace current Client / Server platforms with architectures that reflect the fact that most people in urban centers have online access to public and enterprise applications, with sufficient bandwidth at reasonable prices round the clock. Guest / Visitor Internet Services will be established in all places like planes, trains or corporate conference centers as a commodity service feature allowing the usage of the new application architecture.
Missing mobile CPU power and inadequate software platforms prevent secure online processing or more sophisticated features in web applications.	▸ Missing CPU power and battery capacity are not expected to be a major concern in the future due to the evolution of mobile IT.
We are living in a global village and government borders are not interfering in the flow of data.	▸ Increasing government awareness and matured technologies are causing the volume of IT regulations and controls to explode.

Market Capabilities / Existing Solutions

Consumerization or Bring Your Own (BYO) is not only focused on Device, although BYO Device is the most dominant due to the boom in mobile devices.

Devices in this context cover all types of device (Laptop, Desktop, Tablet, PDA, SmartTV, etc.) that can be used to work with corporate applications. The usage of BYO devices as real corporate assets is not in scope of this White Paper and is discussed in the Scientific Community White Paper, "Consumerization technology - is it really good for business?" (1)

Consumer services that support BYO for almost everything are currently available on the market. Examples of such are shown in the following figure:

Figure 1: Consumer Services for BYO

Besides the consumer services available on the market, companies follow the strategy to use a controlled implementation of consumer type of services inside the organization (e.g. blueKiwi within Atos). This strategy can increase security significantly by making corporate data more controllable and fulfill employee's expectations and legal requirements too. This strategy will continue to be implemented with many applications. The focus of this White Paper is to show how to secure usage.

It concentrates on three main services for corporates: Devices, Applications and Identity. For convenience the BYO email platform is seen as a special application using standard communication protocols.

In recent years different approaches of integrating private equipment into business infrastructure have been developed. Early device models with separated areas for private and business data came with the first virtualization solutions to be installed on client devices.

Since smartphones and tablets have entered the mainstream markets, a new era of consumerization has begun to spread throughout companies all over the globe. With high performance mobile processors and new methods of abstraction, like HTML5, more and more enterprises are forced by the rapid development to allow their employees to use private devices for work.

Important technologies that allow the acceleration of mobile services based on BYO Devices are shown in the following figure and described in more detail.

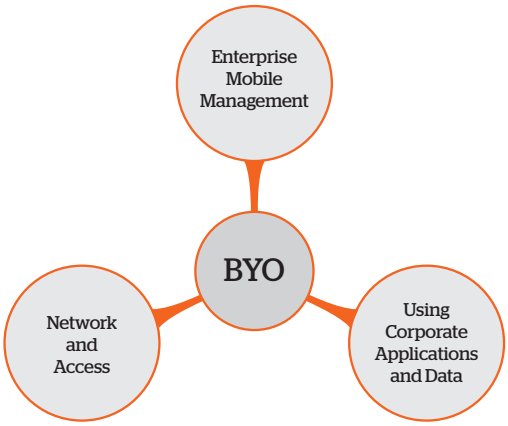


Figure 2: Technologies to accelerate Mobile Services

Enterprise Mobile Management

Enterprise Mobile Management is a fast moving market, with many mergers/acquisitions going on. Functionalities that are provided through different software are - and will get - more and more integrated:

Mobile Device Management (MDM)
Is a software solution that secures and manages mobile devices. Standard functionalities are device configuration, over-the-air distribution of applications, remote wipe and push of security policies (authentication, forbidden applications, etc.). These solutions are often considered as being too intrusive in a BYO approach as they function at the operating system (OS) level and provide control equally on the personal or corporate data and applications. For instance, a user may not want administrative access by the company to his private data on his device.

Mobile Information Management (MIM)
Public solutions such as Dropbox, SkyDrive, iCloud, etc. are heavily used by the consumer. Users have brought this behavior to work, causing serious worries for CIOs as they lose control over corporate data. The market is now seeing the outbreak of business solutions that provide the ease of use of public solutions while resolving business concerns. These solutions allow the creation of a real container that will store corporate data - fully isolated from personal data.

Mobile Application Management (MAM)
The market of Mobile Application Management is emerging and MDM software companies are currently looking at moving from MDM to MAM. The idea behind it is to enforce security and management functionalities at the application level rather than at the device level, in order to be less intrusive on a personal device. MAM describes software or toolboxes that help developing mobile applications. Standard features of MAM are user authentication, application management and application configuration management.

Enterprise App Store
Once an application is developed, it can be made available from an Enterprise App Store as an alternative to the Apple App Store, Android Market etc. that allows companies to distribute their own inhouse applications. Some examples of Enterprise App Stores are Atos MyMarket, AnyTime Files, Anytime Managed Mobile, and Canopy Mobility.

Enterprise Mobile Management solutions currently available in the market address different aspects of BYO. Balancing those with network & access as well as data and applications usage will pave the way for a successful BYO implementation.

Using Corporate Applications and Data

Using corporate applications and data has been a core topic since the beginning of enterprise computing. Many of the "new" concepts in today's open world like virtualization, partitioning, data-centric architectures or application distribution have already been employed for many years. In the context of mobile devices and BYO they are experiencing a revival.

Desktop Virtualization: With desktop virtualization, the idea is to separate the logical desktop presentation from the physical machine (see Figure 3). Companies can easily provide a logical virtual desktop following the company standards to their end users. The desktop can run either locally on the physical desktop (e.g. installation in a separate Virtual environment) or in the datacenter (Virtual Desktop Infrastructure - VDI) with a "remote" display on the end user devices. These solutions provide an easy way to implement a secure BYO device approach as the user works in a secured, corporate "bubble". But the drawback for the end user is the lack of flexibility for them and the missing end user experience as they will have to work in the corporate bubble and cannot take full advantage of their personal device and applications. For instance, if the corporate master provides an old version of Windows and Office, the user has to use them and cannot benefit from the latest versions that they personally own.

Mobile Virtualization brings the technologies of desktop virtualization to mobile devices such as smartphones or tablets. It is possible to run two instances of an operating system on a smartphone while splitting personal and professional environments just as it is done with desktops (see Figure 4). Such virtualization technologies are provided by for example, VMware, Enterproid or Red Bend Software. As of May 2013 most mobile virtualization software work only with Android, setting aside the most popular devices, iPhone and iPad.

Application Virtualization: Application virtualization includes different technologies that encapsulate the application and make it independent from the underlying operating system. The application is run on the device without being installed on it (see Figure 3). In a BYO approach, application virtualization can be a way to deliver a secure application to an unsecure device. Combined with application streaming, application virtualization makes it easier for the end user who can run a professional application on demand, next to a personal application, without any compatibility issue. The ability for virtualization of an application depends on the application architecture chosen as well as on the application layer level (e.g. device drivers are not suited for virtualization).

Strict separation of public, private and enterprise use of application & data does not fully match the user's demand. Combining applications to an individual optimized way of working is the vision we are heading to.

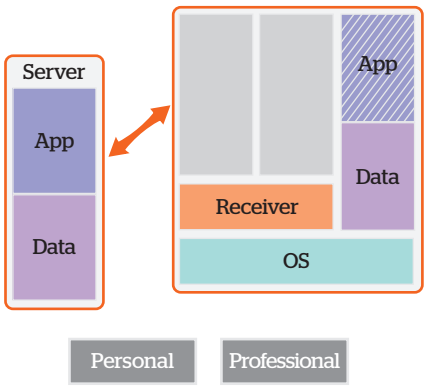


Figure 3: Desktop / Application Virtualization Domains

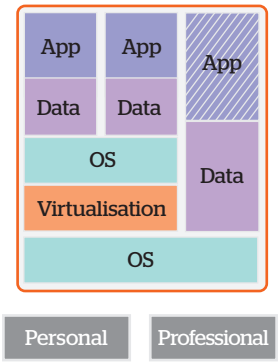


Figure 4: Mobile Virtualization Domains

A **web application** is accessed from a browser over a network. This type of application, with Cloud Computing when the application is delivered in a SaaS mode, makes it easier to deploy a BYO approach as applications are - by default - available from any device with a browser installed. Applications as well as data are not stored or processed on the local device. With the release of HTML5, it is possible to propose rich, interactive environments offering a similar look and feel like fat client applications.

The above technologies are not disjointed but overlapping. HTML5 Web Storage allows data storage locally, or the Sybase Unwired Platform by SAP Hybrid Web Container (2) which allows encrypted storage independently on the mobile device type can be classified as web application but also Mobile or Application Virtualization technology.

Network and Access

802.1X / Network Access Control
Are solutions that secure access to the network by checking the identity and conformity of the device to a security policy (anti-virus, system update, and configuration) based on certificates. In the case of a BYO approach, this type of solution can be difficult to implement, either technically or politically where personal devices are concerned. If it is necessary to implement such solutions for some critical applications with high security requirements, it might then be necessary to reduce the type of mobile devices in order to be able to force the owner to apply a minimum security set-up. On the other hand identifying a mobile device is not sufficient to allow access as mobile device ownership can easily change.

Clientless SSL VPN
When the end user device remains outside the corporate network, it can be granted access to a corporate application through an encrypted tunnel. In order to work from any personal device while not causing a breach into the datacenter, clientless SSL VPN is used. The application is reachable from any browser and security can be enforced, if the device is known or if it complies with the security policy, different accesses will be allowed.

Intrusion Prevention/Detection System
Intrusion prevention or detection systems provide the ability to identify malicious activity. It will become more and more important when you don't control the devices and their security to have the ability to identify which ones may create security issues.

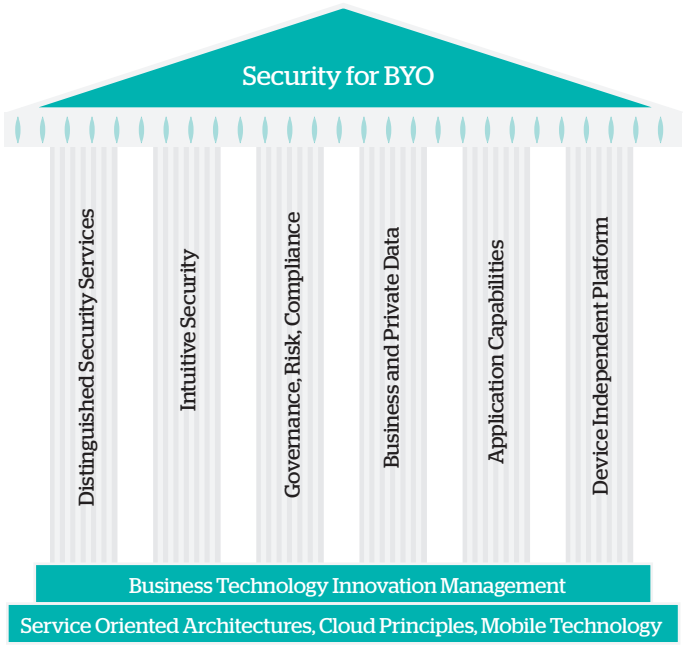
IPv6
The internet protocol version 6 provides some improvements like faster VPN connections, a more stable communication with mobile devices and ofcourse a considerably increased address space that allows trillions of new addresses to be created. From the security perspective this brings a higher level of complexity first of all, widening the gap between normal users and professionals, creating a new demand in awareness and education of network administrators as well as automation of the IP Asset Management (IPAM). This development, in addition to the complexity that BYO concepts bring to network management, will force organizations to withdraw from manual network address/asset management via spreadsheets or similar, as this method can no longer be maintained in complex environments. IP address assignment to individual applications and use of DMZs on the mobile devices can bring some theoretical separation but Mobile OS implementations for firewalling and routing is not solved as at May 2013.

Security Information and Event Management (SIEM)
In a BYO world where blocking and locking is not possible anymore, monitoring is key. SIEM provides real-time analysis of security alerts generated by network hardware and applications. This can be enhanced for mobile devices.

Borderless networks need solutions to control, approve, reject and report the access. Even the simplest solutions require some minimum security measures.

Security Areas for BYO

The security challenges for BYO can be mapped to six pillars. A strong methodical approach is paramount for coming up with a sustainable solution, flexible enough to react in a rapidly changing world.



Security Pillars for BYO concepts

- **Distinguished Security Services**
  Security cannot rely on classic borders and owned hardware anymore. Security has to support automatic security context analysis and classification of communication. Nevertheless the usage of modernized central security services is mandatory for all business services. Many of these new security services will provide federation and will work on application or data level.
- **Intuitive Security**
  Security design has to be intuitive and easy to use. All kinds of available information have to be used to achieve strong authentication.
- **Governance, Risk, Compliance (GRC)**
  A dynamic rule set engine has to be developed for semi-automated decision making regarding compliance.
- **Business and Private Data**
  Security will be integrated as part of the data itself.
- **Application capabilities**
  Architectural approaches have to be adapted to interface with modern, mobile and BYO technologies. Applications have to enforce that data processing policies are actually followed and that the programs cannot be manipulated without detection.
- **Device Independent Platform**
  A sustainable platform can be achieved only by avoiding device dependencies.

For each of the identified pillars, new innovative solutions and strategies have to be followed. The dimension of the challenges demands a well-planned approach regarding business technology innovation management. This is mostly driven by the shift from perimeter security to data-centric security which means:

- Access from unknown and/or un-owned devices to the Information System (loss of device ownership and perimeter protection)
- Trusting "foreign" credential suppliers for internal usage (Bring Your Own Identity as a consequence of loss of device ownership and insisting on specific credentials).

Security must cope with borderless environments that allow for devices an enterprise cannot fully control. Classic topics like GRC, Usability and Application Development, Deployment and Management need innovative solutions to support BYO.

Subsequently the following topics are derived from the above: complete data classification in time for big data (3), built-in security within components and services which interact with central authentication/authorization instances, general information encryption and federated key management.

In this context the approach to centralize security functions under the topics of Governance, Risk and Compliance (GRC) gains a new momentum: facing the challenge to overcome resistant behavior regarding general security practices.

Distinguished Security Services

Security in such dynamic environments as BYO must be built on the assumption that anyone or any device may get access to the data, but that only authorized users should be able to use it for the intended and agreed purpose, and under a defined context.

To prove someone's identity, secure and distinguished authentication mechanisms have to be available for all platforms. Providing highly standardized authentication methods allows for modular and open architectures and guarantees a homogeneous security level. The general problem in this case is the trustworthiness of the user owned devices. The company will have no (or only marginal) influence on the technology or installed software. Therefore authentication methods could be altered. Multi-factor authentication can mitigate this problem but will not avoid it. Multi-factor authentication is even more complex and expensive. The "quality" of an Identity gets more important, as the reuse of existing identities and related authentication methods is mandatory to reduce costs. Employees get a higher quality ID-rating than other end user IDs (e.g. Facebook removes fake accounts (4)). Global identities managed by federated high-performance identity and access management systems are necessary to overcome this problem. Federated security as a service, underpinned by Bring Your Own Identity, could form the basis of a new model for data-centric, platform-agnostic security frameworks that can be applied to highly dis-aggregated IT eco-systems.

Intuitive Security

User acceptance of the authentication is based on trust regarding the solution and its usability.

We identified two major trends which can support this solution:

- Bring Your Own ID (BYO-ID)
- Context, behavior and location-aware authentication and authorization.

BYO-ID is the access management concept to allow users to use their existing IDs. The usage of user-owned governmental ID cards, credit cards, OpenID, etc. for company purposes reduces the number of IDs users manage. Global, federated high performance identity and access management systems can provide Single Sign On to consolidate these individual IDs into a single wallet for applications, social networks and enterprises for ease of use. Using the BYO-ID concept removes the necessity for the company to produce corporate IDs for the employees. Thus further enabling the BYO solution and identity management cost savings.

A user's behavior can be used to improve security (e.g. by discovering abnormal user behavior as a sign of access control being compromised, or by allowing data processing only under defined conditions derived from a user's context), but behavior can also massively complicate security control. Knowledge of the "who, what, where, when and how" regarding usage of data, could be as valuable or as sensitive as the data itself.

Governance, Risk and Compliance (GRC)

GRC as a central security function has to overcome the resistance behavior regarding general security practices based on perimeter protection and device ownership. Following this approach the compliance requirements have still to be fully met. Major points of concern in view of BYO concepts are:

- Disclosure of classified data (company or personal)
- Non-compliance with regulations from state, work councils, or company-like data protection acts, export/import control, work safety
- Financial license, liability and tax issue problems
- Growing shadow IT, loss of governance
- Reliability of devices not company-owned and controlled (e.g. maintenance and support)
- Loss of data due to decentralized data storage on non company-owned devices
- Complexity of a broad spectrum of devices to support.

To fulfill most legal regulations a trustworthy classification of data is the general keystone. This is needed particularly for data privacy for business and personal usage as well as for import/export control. It is imperative to have tools which help to classify the amount of data. A dynamic rule set engine has to be developed for semi-automated decision building regarding compliance. Where a legal requirement specifically obligates the local country, an employment/work council agreement setting the rules has to be followed.

Business and Private Data

Following the BYO strategy means that users use their own equipment for their own purposes as well as for accessing and processing enterprise data. Using the same device or application for all these areas of application removes the traditional natural borders, where we had private equipment and separate devices provided by the enterprise. The borders between private and professional use become especially blurred.

On the other hand enterprise data must not be used except for the purpose that has been mutually agreed between the user and the enterprise. In the case of a negotiation between two parties, for example, the negotiators may share secret documents. A document is not owned by just one of them. Both parties need to have access to the document, but access may be restricted to the conference room and the agreed time; the documents cannot be copied. Data derivations like extracts for calculations or the calculations themselves are considered equally secret and therefore require the same or even stricter rules of data classification.

Hence, special attention is to be paid to how data can be protected against misuse. Misuse by definition is any kind of usage which does not conform to the agreed purpose or which is not subject to governmental regulations (see EU Directive regarding Data Privacy (5)).

Privacy control has to be an essential part of the security model ("privacy by design"); not only from a technical perspective, but also as far as the business model itself is concerned.

How can this happen in a shared environment? Segregating private from professional domains does not provide a solution. This means that Mobile Device Management in its traditional scope does not solve the data issues. MDM has to include a strong Mobile Information Management (MIM), which goes far beyond the data availability and synchronization tasks. It's the data itself that has to carry a policy with it, which rules its usage depending on the security level of the data, including Data Loss / Leakage Prevention (DLP) solutions or Digital Rights Management (DRM) solutions that will be integrated with MIM.

The data protection policies should be able to allow or disallow processing, like for example extracting data, printing or editing. The policies should also be able to trigger actions in case the user and/or the data is crossing defined borders, such as wiping the data when a user is leaving a conference room after a negotiation.

So far we discussed how to protect enterprise data, i.e. data owned by an enterprise. But the same general protection requirements have to be enforced for private personal data, which are not allowed to be processed by any party unless there is an agreed purpose, regardless of the ownership of data. Privacy protection can be enforced by the same data-centric security policies as discussed so far.

Without being compliant to a data policy the data cannot be accessed or processed, no matter where the data is stored or where the applications that process the data run.

As the examples show the data protection policy has to refer to a user's circumstances, for example his current location and the device context such as current connectivity. In addition, there will be policies needed to trigger remote actions, initiated by events happening in enterprise processes that change the user's status or profile, for example, when a user moves to a new department or when a user leaves his company, data may become inaccessible. (Similar policy-driven actions apply to the applications themselves: a user may not be allowed to execute apps after moving or leaving.)

When storing enterprise data on a user's own (no matter if mobile or stationary) device in decrypted form the data cannot be effectively protected against misuse, because a mobile device cannot be fully controlled by the owner of the data. Hence, decrypted enterprise data should never be stored on a user's device, not even temporarily.

After all it looks like if BYO security is more about data control and not about device ownership. But the disruptive approach to this big challenge is to provide applications with a programming framework, which ensures policy-compliant processing in runtime as well as in the software development lifecycle. Any attempt to manipulate a "secure" application must be detectable and prevent the data from being decrypted. The devices, and more than this the applications, have to provide means to fulfill the data-centric protection requirements. Hence data-centric security is nothing without strong application management.

Application capabilities

The key requirements regarding business services and applications are the

- Ability to run an application on any device (Smartphone, Tablet, Laptop)
- Ability to add security, compliance and management features at the application level, according to the company security policy
- Ability to handle the data security level and use the data as its policy allows it
- Guarantee that sensitive data processed by the application is stored encrypted.

Web applications are popular and will become default in the future. Thus application support for different end point devices should not be a big challenge by 2016. HTML5 will also support this evolution and will provide comfortable and easy to maintain user interfaces which will result in highly standardized interfaces and fewer fat mobile clients. This shift to online applications could result in a challenge if access is needed from the outside (e.g. wireless or mobile

Data centric Security either by embedding security policies in the data itself or by establishing an application framework is at the core of BYO.

network on the airport) where low bandwidth or limited online time could be a limitation. The evolution of high speed mobile networks will reduce this disadvantage. But there is still a need for offline work capabilities when no online connection is available or perceived as too expensive (airlines may offer online DOMESTIC connections (6)). The increasing evolution of web-based applications and 24x7 online connections will support security for BYO significantly because it is generally unnecessary to store corporate data locally. Due to the ability to control document upload and download on web-based interfaces the risk of a security breach decreases.

In order to reach this position, the operation must be controlled and follow the corporate guidelines on information classification. Local applications will no longer be able to access corporate data directly, i.e. directly accessing a file share. Each component in the application/ services ecosystem has to protect itself and the data given over, because it cannot rely in general on any other component invoking its services.

Applications (Apps, Web browser, etc.) on end-point systems must be secured (signing/ hashing of software) to prevent manipulation by other applications. In addition strong authentication on an application level and secured communication between local and corporate applications must be implemented. Solutions for strong authentication and secured communication are mature and already state of the art. Secured web-based applications should be sufficient to work within the corporate network or through a connection from another high speed network.

In special cases, there is still the need for a secure offline solution (e.g. international flights or outside of urban centers) with additional security features on all execution layers (platform, OS, virtual machine, etc.). Such a solution must be implemented with secured local applications and a separation between domains (private and corporate). Transition of data between those domains must be managed by a security policy which needs to be implemented in the application. An uploaded document can be controlled by security scanners and further processes (information classification, etc.). The download process is critical as it creates the biggest challenge of protecting the offline data on an insecure and difficult to control user-owned device.

For companies who are not there yet, solutions such as VMware Horizon or Citrix Cloud Gateway 2 are interesting options. The promise of these solutions is to deliver applications and data to any endpoint device, while to include security and policy.

Device Independent Platform

Recent market research (7) points to tablets overtaking notebooks in terms of sales from 2016, yet already it appears that this may happen much earlier, in 2013 (8). The key area to support BYO in 2016 will be tablets and their descendants (e.g. wearable computers), along with smartphones. We see these as the two key device segments. Although notebooks will still be present in the corporate environment, we see BYO as concentrating on tablets and smartphones far more for corporate interactivity.

Achieving maximum security allowing the widest range of support, a 'thin client' solution can provide the same end user experience across multiple devices over ubiquitous 4G and higher speed of internet access. Evolution of high speed wireless technologies such as 4G allows for far less data needing to be stored on the client, but delivered in real-time. This means the worry over the sensitivity of data on the end device is heavily reduced, as it doesn't store locally, but simply accesses the corporate systems through a controlled 'sandbox' -like environment.

Today, device management is largely based on end users having unrestricted access to corporate information, e.g. email, and storing all this data locally. Issues such as remote wipe, which can be a sensitive topic for a user's own device, aren't such a concern in case there is no local data. A secure method of authentication is still required, which can be enforced through the application itself.

The Software Defined Network Security (SDNS) strategy could be another mechanism to impose granular policy-based security control and implement network isolation providing service interposition between application and the user-device based on the pre-defined level of trust relationship.

With the new paradigm that we cannot secure the end user device, the corporate application and provisioning infrastructure will have to be "smarter" than the smart device. The application design and the provisioning infrastructure architecture will have a higher level of security mechanism built-in. For instance, security software manufacturers have joined forces (9) to define a software taggant system in order to improve the chances of catching rogue operators and allowing antivirus software to more efficiently process legitimate executable files created by packer software. The same is happening to the Application Store Ecosystem which is significantly different from desktop/ laptop computers application provisioning.

Today, these security controls and mechanisms are built into the end user's devices and require the end user to approve or reject certain actions occurring on their device. We firmly believe in tomorrow's smarter application environment, where the application will verify and make decisions on events occurring in the service ecosystem.

Undoubtedly, there must be some measure of minimum requirements to support this. However, by going through the thin client approach, it does reduce the potential load on the end device. Equally from a security perspective for instance, if a device had a known screen scraping security vulnerability, we may want to look at blocking access from such devices.

With all users carrying around their tablets, the need to print is greatly reduced. Now when going to a meeting you may take a copy of the agenda, some prepared slides for instance. Now this can be stored on a device barely larger than a piece of paper. Although where printing or interfacing with other corporate resources such as scanners is necessary, this can all be handled on the application side, rather than using the device's native printing capabilities.

A computer actually embedded in a person, e.g. a tattooed computer, can in theory identify that person automatically. However, this in itself may still prove insufficient (who knows what measures corporate espionage might go to in some areas!).

Conclusion

We recommend CxOs focus on concrete BYO implementations based on their organization's maturity level:

1. **Defend:** The first level of security should be towards defending the organization's assets and information towards external threats and concentrating on controls that focus on lowering vulnerabilities to those threats
2. **Identify:** The second level focuses on security from within, knowing about values, identities and the communication, interaction and cooperation in between those involved
3. **Cooperate:** Having both protection and identification in place, security should focus on the communication and interfaces to third parties, as vendors, suppliers, partners and customers
4. **Optimize:** Having established each of the previously defined levels, the focus for security should be on continuously improving the security of the organization, enabled by creating transparency, accountability and risk-based decision making.

Possible use cases for BYO security are linked to the security areas defined in chapter

Maturity Level	Distinguished Security Services	Intuitive Security	Governance, Risk and Compliance (GRC)	Business and Private Data	Application Capabilities	Device Independent Platform
Defend	▸ Security Incident and Event Management (SIEM)		▸ Security Policies regarding BYO ▸ BYO Risk potential	▸ Data Loss / Leakage Prevention (DLP)	▸ Sandboxed Solutions ▸ Encrypted Data Stores	▸ Host based Services
Identify	▸ Identity and Access Management (IAM) ▸ Biometric Services	▸ Bring Your Own Identity ▸ Context, behavior and location aware authentication and authorization	▸ Asset Managemen	▸ Mobile Information Management and Digital Rights Management (DRM)		▸ Central Entitlement Services and Single Sign-On (SSO)
Cooperate	▸ Federated Identity Management (FIDM)			▸ Enhanced Online Services (HTML 5)	▸ Enhanced Online Services (HTML 5)	▸ Enhanced Online Services (HTML 5)
Optimize	▸ Centralized Governance Risk and Compliance (GRC) Services		▸ Centralized Governance Risk and Compliance (GRC) Services	▸ Data Centric Security with centrally applied policies (by GRC Tool)	▸ Centralized Governance Risk and Compliance (GRC) Services	

Figure 5: BYO Use Cases based on the organisational Maturity Level

Keep in mind that BYO concepts will remove the walls between private, public and enterprise use. Current device management solutions try to separate the different domains from each other, thus extending existing perimeter security concepts to BYO devices. But, existing perimeter security has many holes and probably cannot be repaired. Full Endpoint-Security is not possible on user-owned devices. Furthermore, existing management solutions for mobile clients have developed in proprietary directions. The development toward BYO demands a more open approach like other trends such as cloud services and service-oriented architectures to therefore enable more adequate security solutions.

The breakthrough to future secure information technology in the presence of BYO comes with

- A globally unique ID that allows strong authentication for accessing distributed applications residing in different domains
- Data-centric processing policies that allow data to flow through the domains without compromising data protection demands
- Immutable application capabilities that enforce data-centric policies, authorized access to authenticated users and compliance rules.

These security foundations are not specific to BYO but applicable to any borderless environment serving distributed applications.

Global unique IDs are more an organizational than a technological challenge. CIOs will redesign their IT landscape to allow external IDs instead of issuing their own enterprise IDs.

Since enforcement of data security is shifted from a device or operating system level to the applications, security measures must be developed as an intrinsic part of the applications in future. The operating systems or device management systems, in return, must provide frameworks to support the application developers.

With the shift of security towards data and applications software, security testing as intrinsic part of the development process becomes inevitable. Security extended Lifecycle models like Microsoft Security Development Cycle (SDL) or best practices like the Open Web Application Security Project's (OWASP) will increase their footprint in R&D departments.

Until achieving this breakthrough, realistic approaches have to consider centralized access gateways to data. Unified messaging and collaboration platforms with web-based interfaces prove to be very interesting approaches. Combined with a strong identity and access management system this platform can deliver a hardware-independent work environment as well as a hidden document management system. Today HTML5 enables those platforms to have the same look and feel as a fat client. The sandbox in the browser could be highly standardized like java.

As complete trust to non-company-owned hardware platforms cannot be established, multi-factor authentication using all possible means becomes paramount. The reality of BYO needs to be accepted as fact as well as the permanent loss of perimeter control and endpoint-security.

Today cultural shifts are forcing IT managers to reconsider security in a borderless environment and in designing smart applications to provide proper security levels. They also require the employees to have the right mindset and awareness. Ultimately the biggest gap in any security plan comes from human beings. Human nature causes users to use overly simple passwords and fail to change them on a regular basis. Human beings lose devices or view sensitive data casually where others may see or hear (planes, trains, airports), etc.

So no matter how robust the BYO security solution, making data access easier and more accessible via BYO will increase risk due to the human factor. While data-based security can address much of the risk, the human element should be addressed in any BYO solution.

In the future security will be fully established on data / application level only, but not on the level of operating systems.

Abbreviations and Bibliography

Abbreviations / Terminology

BYO: Bring Your Own

ESN: Enterprise Social Network

MAM: Mobile Application Management

MDM: Mobile Device Management

MIM: Mobile Information Management

SIEM: Security Information and Event Management

Domain: Area / Resource group in a given environment / operatiing system / device that is separated in regards to access control.

DMZ: Demilitarized zone

Bibliography

Atos Scientific Community. http://atos.net/en-us/about_us/insights-and-innovation/thought-leadership/bin/can_consumer_technology_really_help_businesses.htm. [Online] 12 10, 2012.

Sybase a SAP company. http://www.sybase.com/files/White_Papers/Sybase_SUP_Hybrid_Web_Container_Article_wp.pdf. [Online] 3 30, 2013.

Atos Scientific Community. http://atos.net/en-us/about_us/insights-and-innovation/thought-leadership/bin/wp-open-source-solutions-for-big-data-management. [Online] 12 10, 2012.

ComputerActive Dinah Greek. http://www.computeractive.co.uk/ca/news/2213180/facebook-removes-fake-accounts-and-likes. [Online] 09 28, 2012.

European Parliament, Council. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT. [Online]

Murph, Darren. Lufthansa launches in-flight WiFi in intercontinental flights. [Online] 12 2010. http://www.engadget.com/2010/12/04/lufthansa-launches-in-flight-wifi-on-intercontinental-flights-u/.

DisplaySearch, NPD. Tablet Shipments to Surpass Notebook Shipments in 2016. [Online] 2012. http://www.displaysearch.com/cps/rde/xchg/displaysearch/hs.xsl/120703_tablet_shipments_to_surpass_notebook_shipments_in_2016.asp.

Digitimes Research. http://www.digitimes.com/news/a20121119PD209.html. [Online] 2012.

ICSG, IEEE Industry Connections Security Group -. IEEE STANDARDS ASSOCIATION . [Online] 8 2011. http://standards.ieee.org/news/2011/icsg_software.html .

Atos Scientific Community. http://atos.net/en-us/about_us/insights-and-innovation/thought-leadership/bin/wp-open-source-solutions-for-big-data-management. [Online] 12 10, 2012.

About Atos

Atos SE (Societas europaea) is an international information technology services company with annual 2012 revenue of EUR 8.8 billion and 76,400 employees in 47 countries. Serving a global client base, it delivers Hi-Tech Transactional Services, Consulting & Technology Services, Systems Integration and Managed Services. With its deep technology expertise and industry knowledge, it works with clients across the following market sectors: Manufacturing, Retail & Services; Public sector, Healthcare & Transports; Financial Services; Telecoms, Media & Technology; Energy & Utilities.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. It is the Worldwide Information Technology Partner for the Olympic and Paralympic Games and is quoted on the NYSE Euronext Paris market. Atos operates under the brands Atos, Atos Consulting & Technology Services, Atos Worldline and Atos Worldgrid.