nCrypted Cloud

470 Atlantic Avenue
Boston, MA 02210
Office: +1.617.520.4120

DATA CENTRIC BYOD IT MOBILITY STRATEGY

Data-centric security is the cornerstone of a successful BYOD and consumer-centric mobile computing strategy.

As BYOD, mobile computing, social collaboration, and consumerization trends continue to gain traction, more and more sensitive enterprise information travels and is stored outside the network perimeter. Information is increasingly being accessed using personal, mobile, and unmanaged devices.

To gain the competitive and cost advantages that BYOD and consumerism-based computing promise, enterprises will need data-centric security safeguards. Information must now be secured whenever it travels, wherever it is stored, and whenever it is accessed.

A first-rate, data-centric security infrastructure provides the capabilities that an enterprise requires to unleash the benefits and advantages of BYOD and consumerization, without compromising its privacy and security posture.

The New Data-Centric World

By its very nature, the Internet is data-centric. People use the Internet to search for information, send and receive emails/text messages, make video calls, and share documents, pictures, and movies. Enterprises are increasingly using the Internet for business collaboration, using cloud services to share and store files, and using social networks to offer better consumer-centric services.

The rapid adoption and extensive use of mobile devices, such as smart phones and tablets, means that the personal computer is starting to become just one of many device choices. Many consumers are replacing their personal computers with tablets and smart phones just as many workforce members are only using mobile devices when travelling. Moreover, enterprises are increasingly deploying mobile devices instead of laptops or PCs for special purpose applications (e.g., home health care, UPS delivery, etc.).

Mobile computing, social collaboration, and consumerization trends are dramatically changing personal and business computing practices. These trends are changing how we work together, how we do business, and how enterprises interrelate with consumers. Additionally, they are also changing how we access information, how we store information, and how we secure data.

Enterprises will have to become more consumer-centric in order to deliver better services, support BYOD, and improve collaboration and data sharing for competitive purposes.

In a BYOD and consumer-centric world, information must have the ability to be stored anywhere and accessed from any device. Because enterprises are increasingly storing and sharing sensitive information using cloud provider services (e.g., Dropbox), that information is travelling beyond the network perimeter.

In order to gain the competitive and cost advantages that BYOD and consumerism-based computing promises, enterprises will need data-centric security mechanisms to protect sensitive information.

Data-Centric Security

Data-centric security is providing information to consumers, such as employees, when they want it, where they want it, and on their preferred channel, all while ensuring that the information is adequately protected.

Traditionally, enterprises secure networks, systems, and devices. In a BYOD and consumer-centric mobile computing world, enterprises will secure the physical data wherever it goes. The data will be persistently secured

470 Atlantic Avenue
Boston, MA 02210
Office: +1.617.520.4120

regardless of where the data is transmitted, stored, and what device is used to access it.

A data-centric security infrastructure is required to enable BYOD and customer-centric mobile computing services without compromising the enterprise privacy and security posture.

Characteristics of a Data-Centric Security Infrastructure

The major characteristics of a data-centric security infrastructure include:

Protecting the information while it is in flight and at rest.

Identifying and authorizing who is accessing the information.

Capturing all key events for auditing and monitoring purposes (who, what, when, where).

Provisioning and administrating capabilities to deploy and manage activity, including means to:

- De-provision access when required.
- Recover data for business continuity or forensic purposes.
- Prevent data loss.

Encryption is the core underlying technology in a data-centric security infrastructure. This means that public and private key management is critical. Encryption key life cycle management and practices need to be robust. Strong standard based encryption algorithms should be used.

Optimally the data-centric security infrastructure should support any or most popular cloud-based storage service providers. Additionally, a first class data-centric security infrastructure should respect the privacy of non-enterprise data stored on personal devices.

Finally, to ensure consumer adoption and successful deployment, the user interface should be consumer-centric and blend seamlessly into the mobile user' computing experience.

Conclusion

Mobile computing, social collaboration, and consumerization are dramatically changing personal and business data computing practices.

Sensitive enterprise information is increasingly travelling beyond the network perimeter as a result of the increased use of cloud provider services (e.g., Dropbox). Information is now being accessed using personal, unmanaged devices.

A data-centric security infrastructure provides the necessary safeguards to enable mobile computing (e.g., BYOD), social collaboration, and consumerization.

About nCrypted Cloud

nCrypted Cloud delivers ground breaking cloud storage and collaboration security solutions. nCrypted Cloud's consumer-centric design, data-centric security architecture, enterprise strength encryption, and auditing features make it the undisputed leader in the mobile collaboration and file sharing security marketplace.