Whitepaper

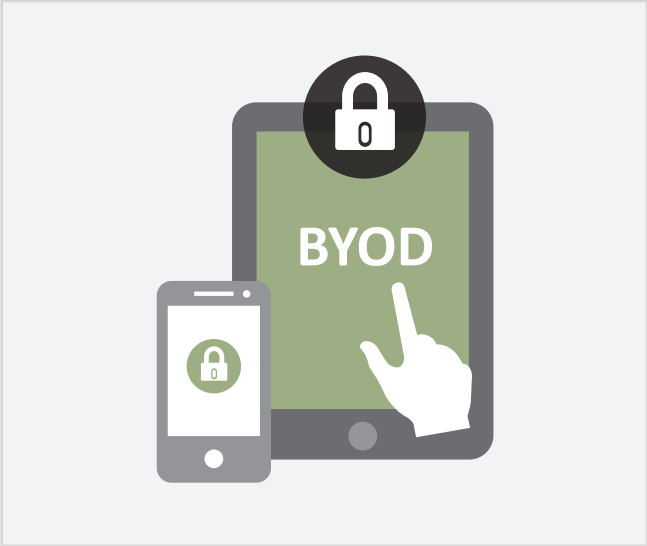
BYOD Program Best Practices for Data Protection & Security

Infrascale™

BYOD Program Best Practices for Data Protection & Security

Bring your own device (BYOD) has evolved. From simply having a personal device at work, employees now bring their laptops, tablets & smartphones, expecting the convenience and productivity of these devices in the workplace. As a result of the BYOD evolution, IT must balance the demands of security and convenience, protection and efficiency. Best practices are emerging to help IT achieve these twin goals, supported by technology, process and policy.

According to analysts, and a recent survey by ZDNet1, BYOD-related issues top the list of CIO concerns. Questions surrounding BYOD that keep CIOs up at night include everything from risk management to employee satisfaction, and expanding the efficiency of mobile devices to greater collaboration. Many organizations start the BYOD process by drafting a policy document outlining the organization's rules and guidelines addressing issues as varied as personal ownership and device time-out requirements. While there are many BYOD policy templates available as a starting place, much less advice is available to discuss the next level of concern – the intellectual property created on employee devices, and how to assure it is secure and protected.



BYOD increases security risks, strains IT

Endpoints, by definition, are not tethered to the LAN. As a result, they cannot be treated by central IT in the same way they have traditionally approached data security and protection. In addition to their ability to disconnect from the network at any time, mobile endpoints operate outside of the perimeter. They are mobile and at much greater risk for being stolen, lost, or the victim of an accident, which can be as varied as a bad drop or spilled coffee. While a device can be easily replaced, it is the digital assets on BYOD endpoints that present the greatest risk to the organization.

Employees are creating, sharing and collaborating on corporate intellectual property on endpoints that may not be backed up, that IT doesn't have control over and that all too often resides on the endpoint device. Exacerbating the problem is the wide variety of platforms and geographies involved in the BYOD movement.

While IT has a variety of security technologies in place today, most do a poor job addressing endpoint data protection because they were not designed to address issues associated with mobility such as devices disconnecting from the network, interrupting scheduled backups. Further, legacy systems are often not designed to address tablets or smartphones, leaving these devices completely vulnerable. And, if a technology does address these devices, they frequently do so in an interruptive way, allowing users to intervene and potentially postpone or change settings and schedules.

Endpoint Data Protection that Facilitates Productivity

Endpoint access to corporate data carries unique needs that are incremental to the needs of protecting on-premises workstations. As a result, a complete endpoint solution must incorporate data protection, productivity enablement and the ability to manage it all.

Endpoint *Data Protection*

Eighty percent of BYOD activity goes unmanaged which goes a long way to explain why CIOs are consumed with the issues of endpoint data loss prevention and employee productivity. Any IT department ignoring endpoints needs to understand that their work protecting the enterprise does not stop at the LAN perimeter.

Data loss prevention is a core tenet of any BYOD best practice. Enterprises should ensure that their approach includes the ability to track, geo locate, and authorize endpoints. Should the CEO, for example, leave his laptop on a plane, IT should be able to locate the laptop and remotely remove data from the device. Remote wipe is a business imperative as it protects corporate intellectual property from potentially falling into the wrong hands. Moreover, it can help organizations avoid compliance issues associated with data that may contain protected information. For these reasons, secure organizations have created policies to prohibit BYOD without the ability for remote wipe.

Security access is the other key consideration IT should give to protecting endpoint data. Best practice dictates that three-tier encryption that protects data in all stages – from the endpoint, in transit, and backup server – is imperative.

Productivity *Enablement*

Balancing endpoint data protection with user productivity is of critical importance as users increasingly rely on their own devices for content creation and collaboration. In fact, 24% of surveyed consumers said that they rely on their BYOD solely as their primary, work-related device. Best practices indicate that IT include the following components in their BYOD strategy.

User transparency – To avoid users skipping, rescheduling or dismissing data backups, employee transparency is important. With backup happening in the background, users remain working and uninterrupted. Moreover, this transparency should include resource throttling to minimize bandwidth and CPU issues to maintain system performance and user productivity.

Breadth of coverage – Any technology solution IT chooses to help implement their BYOD data protection strategy should offer breadth and depth of coverage. Enterprises should look for solutions that backup a wide variety of files and email archives, and supports a variety of endpoints – from laptops with Mac or Windows OS to tablets and Droid smartphones. Last, the solution should also support heterogeneous cloud backup strategies.

User experience self-restore – Should an employee's device be lost, stolen or irrevocably broken, self-restore is a critical best practice. Self-restore saves user preferences and settings, providing the ability to get users easily up and running on a new device with their personal settings and data – saving both IT and the user time traditionally spent re-configuring a new system.

Management *Functionality*

Not to be overlooked is IT management, the third component of an endpoint protection best practice strategy. Management is critical to ensure that patches and security updates are effectively and efficiently rolled out across enterprise endpoints, all from a single dashboard. Moreover, central management allows IT to assemble detailed reports that help ensure it has executed an effective security strategy across employee devices. Best practice management functions that IT should include are:

Centralized IT Management – Allows IT to deploy, backup and otherwise manage endpoints globally without user involvement, all from a single, convenient dashboard. For IT productivity and to ensure endpoint compliance and coverage, central management should include the ability to mass deploy and remotely backup data in compliance with corporate policy controls. A side benefit of this approach is that it allows IT to easily add, remove and otherwise manage users. Central management should also allow IT to control endpoint data with fine-grain control, separating for example, personal content from corporate IP, delegate specific tasks and report on any number of metrics.

Intelligent data detection – Allows IT to specify data backup. In this way, central IT can ensure that only corporate data, not personal data, is backed up and archived if necessary, preserving individual privacy and storage resources. It also allows IT to search for data on a machine using familiar search terms like "documents" or "pictures" rather than working with file names (*.pptx) or with cumbersome folder path taxonomies such as c:\some\folder\.

Data reduction and advanced de-duplication – As employees often share documents, it is important to also consider data de-duplication as a data reduction strategy. By checking and ensuring that multiple copies of the same asset are not duplicated, enterprises can save on both bandwidth and additional storage costs.

WAN Optimization – Is the ideal approach to manage endpoint backup as it increases data-transfer efficiencies, and allows for quicker backups regardless of the endpoint network.

As 62 percent of enterprises embark upon BYOD support this year, data security and protection at the endpoint must be an organizational priority. Important corporate intellectual property leaves the front door of every office every day, traveling on laptops, smartphones and tablets. Protecting this sensitive information, and ultimately defending the brand is of the utmost importance. With these best practices in hand, enterprises have the tools to build on their BYOD policy with properly chosen technology and processes to ensure endpoint data protection and security is tightly woven into the organization's overall IT management.

About Infrascale EndGuard

Infrascale **EndGuard**™ is a centrally managed, cloud endpoint data protection solution that protects corporate data everywhere where it lives – on laptops, tablets and smartphones. Secure backup, best–in class data loss prevention, geotracking, remote wipe and heterogeneous restore capabilities are combined in a single, unified application to simplify management for IT, improve business productivity and reduce security risk.

Infrascale connects people, devices and their data in ways that are truly secure.Headquartered in El Segundo, California, Infrascale's cloud platform runs from eleven data centers on five continents. Infrascale software spans mobile, desktop and cloud and powers **EndGuard**™, **FileLocker**™, **Infrascale Backup**, **SOS**™ **Online Backup** and over one-thousand independent cloud service companies, VARs and MSPs. Visit http://www.infrascale.com.