Say ‘yes’ to Bring-Your-Own-Apps

Symantec and NTT are leading the way

It was inevitable. As soon as bring-your- own-device (BYOD) became a mainstream practice, bring-your-own-apps (BYOA) was bound to follow.

As each new tech-savvy generation enters the workplace, they bring with them expectations and demands for flexible working practices, including working location and choice of tools to get the job done.

And with good reason. Forbes reports that 49% of users say they are more productive using their own devices, while a Cisco study suggests that using personal devices can lead to individual productivity gains of USD 300 to USD 1,300 a year.

BYOA continues and enriches this trend. Today, it’s estimated that the average organization has up to 1,000 cloud apps in use[1], including productivity tools such as WhatsApp, Dropbox and Evernote. However, compare that figure to the 30-40 apps that CIOs are reporting, and the scale of the issue is clear.

On one hand, the security risks this poses will send alarm bells ringing throughout the IT team.

But the opportunity that BYOA presents to transform the reputation of the organization and enable it to safely embrace new innovations, is too significant to ignore.

That’s why we have joined forces with Symantec to offer a comprehensive suite of cybersecurity solutions and integrations to support the cloud generation. And with two industry leaders working together, BYOA transforms into something IT can get behind, rather than something they have to get over.

[1]*Source: State of Cloud Application Access Survey 2013 https://resources.onelogin.com/WP-2013-Cloud-Application-Access-Survey.pdf?path=wp-content/images/2013_Cloud_Application_Access_Survey.pdf*

From gatekeepers to business enablers

Crafting a solid cybersecurity strategy for BYOA

The challenge for IT – managing the risks

While many enterprise-grade applications meet the needs of the organization today, it would unreasonable to expect the IT team to be able to keep pace with the advances and conveniences of new and free applications available in the open market. In that respect, BYOA is inevitable.

Saying 'no' to BYOA isn't a realistic option either. Not for an IT organization looking for ways to enhance productivity and innovation. The trick for IT leaders is to find the right balance of empowerment and control through an agile cybersecurity posture that accepts that security incidents will happen, but to reduce the likelihood of it causing harm: to the business, and to its partners and customers.

71% of employees **are using apps not sanctioned by IT.**

Stage 1: Lay the ground rules

Let's start at the beginning. If you want to embrace BYOA rather than block it, you need to assess the reality behind the risk. So here are the first three questions you should be asking yourself:

1. **What are our legal obligations?**
   Essentially, when risk isn't even an option and by law you need to follow data and privacy regulations.
2. **Where am I absolutely not willing to take risks?**
   For instance, how you allow your intellectual property to be accessed and shared.
3. **Where am I willing to take risks?**
   This is about things like the level of risk you're comfortable with, in exchange for productivity benefits, like supporting remote workers or contractors.

With those questions answered, you then have a starting point from which you can assess how the business uses apps in the context of BYOA, the threats, risks and vulnerabilities you need to be aware of, and how to protect against them.

Stage 2: Assess, assess, assess

- **The what**
  Once you've established your risk profile, you need to identify what apps are being used, by who, and how often. How risky are those apps to your enterprise security? Is there a way you can audit all your apps and how they're used? If not can a third party help you?
- **The how**
  Got a handle on your apps? Great. Now you need to understand how your users are sharing, using and storing your information through BYOA. What are your legal and regulatory obligations, and what's the risk to your data governance policies if that information is compromised? What assessment tools are available to help you understand this?
- **The where**
  The days of managing your users and devices from within the safe confines of the network perimeter are over. Your users work everywhere, so you need to assess the security and integrity of the devices being used in BYOA and the wireless networks they access. For instance, what controls do you have (or need) in place for users operating on public or shared networks?

Stage 3: Put the tools in place

Let's be honest here: BYOA is going to poke holes in your security. But there are things you can do to mitigate it. It's important to give users the right tools to ensure you minimize the risk of exposure and improve the security of BYOA. For instance, having an incident response plan so that when something does happen, you can act immediately and remediate swiftly.

Perhaps most importantly though, having the right tools means having the right technology and solutions for you to plug the gaps in your security that BYOA can (and most likely will) create for your users, devices, access and information. And that means talking to the right partners.

Security considerations for BYOA

Users	How are you **identifying, authenticating and protecting employee** identity?
Devices	How are you **protecting employee devices** and the systems they access?
Access	How can you empower your people to **work securely** from anywhere they need or want?
Information	How can you enable **safe collaboration** by protecting your information as it travels across apps and services?

NTT and Symantec can help

We use the power of technology to help you achieve great things in the digital age. We can help you design and implement a secure BYOA strategy that balances your users' needs for flexibility and autonomy, without sacrificing security or compliance. And through our partnership with Symantec, we have access to a wide range of industry-leading security technologies, helping you confidently embrace BYOA by putting in place the right security solutions for users, devices, access and information.

Secure BYOA with NTT and Symantec

Delivered by NTT:

Cybersecurity Advisory for Digital Workplaces: We can help embed cybersecurity into your digital workspace strategy, making it secure by design.

Technical and Support Services: We can analyse, design, implement, support, and optimize your security infrastructure, improving your operations and reducing costs.

Managed Security services: We engineer the right set of services, tools, platforms, people and processes to help you achieve the business outcomes you want.

Powered by Symantec: The recognized market leader for multiple cybersecurity technologies.

Web Security Service (WSS) Tracks, monitors, and controls web access by scanning for malware, and blocking risky sites and links that may be introduced by unknown apps.

Cloud Access Security Broker (CASB) Gives you visibility into what apps are being used, and how risky they are, while helping you understand what data is being stored/ shared, and where extra security controls should be applied.

Data Loss Prevention (DLP) and Integrated Content Encryption (ICE) Helps track intellectual property as it leaves the organization and if needed, encrypts it.

Symantec Endpoint Protection (SEP) Multi-layered security techniques, including AML and behavioral analysis, protect the OS from infection.

Symantec Endpoint Protection for Mobile (SEPM) Assesses each device's security risk and enforces advanced protections as required.

Take your first step

Building your BYOA security strategy is easy with the right people. To learn more about security services and solutions for your Digital Workplace, speak to an NTT representative today.

Disclaimer: The work described in this whitepaper was performed while the company was known as Dimension Data.


NTT