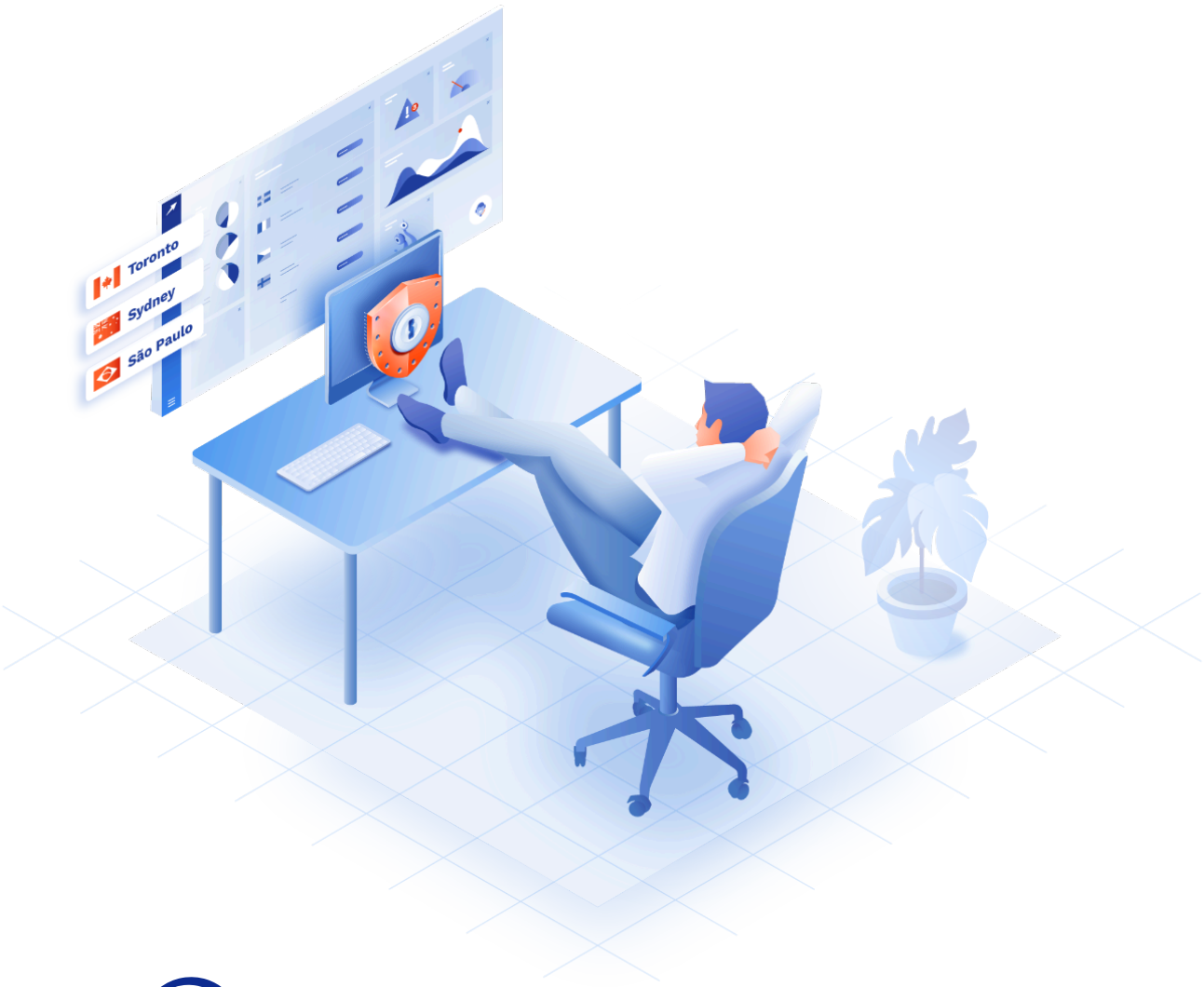
BYOD in Mid-Sized Enterprises:

A secure and cost-effective way to empower your workforce



GoodAccess

Table of contents

Executive summary 3
What is BYOD 4
Advantages of BYOD 5
Disadvantages of BYOD 7
Key challenges of a BYOD security policy 11
Why mid-sized enterprises struggle with BYOD 12
How GoodAccess enhances BYOD security 14
Conclusion 15

Executive summary

The proliferation of BYOD has made it a common practice among organizations that incorporate remote work. While BYOD offers benefits like flexibility, increased productivity, and reduced costs, it introduces significant security risks as well.

Companies must tackle challenges like diverse device types and platforms, compliance requirements, or lack of experienced IT staff, the latter being particularly challenging for medium-sized organizations.

However, by implementing Zero-Trust Architecture as a service, the organization can outsource a large part of the burden and meet the security requirements while keeping the benefits of BYOD.

What is BYOD

BYOD stands for ***b**ring **y**our **o**wn **d**evice* and usually refers to the practice of employees bringing unmanaged devices to the workplace. Typically, this involves smartphones, but may include laptops, tablets, and other appliances.

When applied to employees BYOD is often considered a benefit or a cost-saving decision, but when it comes to contractors, partners, and suppliers, some form of BYOD is often a necessity. It's not often within the means of every organization to provide every contractor with a device for work, and not every contractor would welcome that.

Advantages of BYOD

BYOD offers multiple advantages that increase company performance and improve employees' quality of life.

User familiarity

Employees are comfortable with their own devices and it's easy for them to work with a device they always have readily at hand. This improves their well-being and contributes to talent retention.

BYOD also requires less training, at least as far as device make and OS are concerned. Users are more sure of themselves and can handle technical issues better when working with their own device.

Increased productivity

BYOD can also increase employee productivity. In fact, the 2021 BYOD Security Report by Cybersecurity Insiders states that 68 % of respondents consider increased productivity the main benefit of BYOD.

Employees and contractors are more productive using their own devices mainly in two ways:

- They are familiar with the UI and capabilities of the device. For example, some employees (such as graphic designers) may prefer using their own device because it gives them more computing power than a company-issued device.
- They are more available, even during lunch hours, off-hours, or vacation time, as long as they have an internet connection and are willing to respond during this time.

Cost savings

The cost of providing every employee with a device depends greatly on the country and the organization's device rotation cycle. However, in all cases, BYOD offers significant savings.

It can be estimated that a company would spend around $2,500 per employee every three years on device purchases and related costs like maintenance and connectivity costs.

This makes approximately $800 per employee per year if the company issues work devices to its employees.

Under BYOD, maintenance cost will be reduced by about 50 % and onboarding and training time is also reduced, bringing an average annual cost of $30 per employee.

However, it is also fair that the company reimburses the employees for some of their expenses, whether it is cost of purchase or connectivity bills. A reimbursement program is commonly around $500 per year per employee.

Below is a comparison of annual device-related costs with and without BYOD in companies of 50, 500, and 5,000 employees.

Company size	No BYOD	BYOD	Annual savings
50 employees	$45,000	$26,500	$18,500
500 employees	$450,000	$260,500	$185,000
5 000 employees	$4.500,000	$2.600,500	$1,850,000

Tab. 1—Annual cost of employee devices with and without BYOD

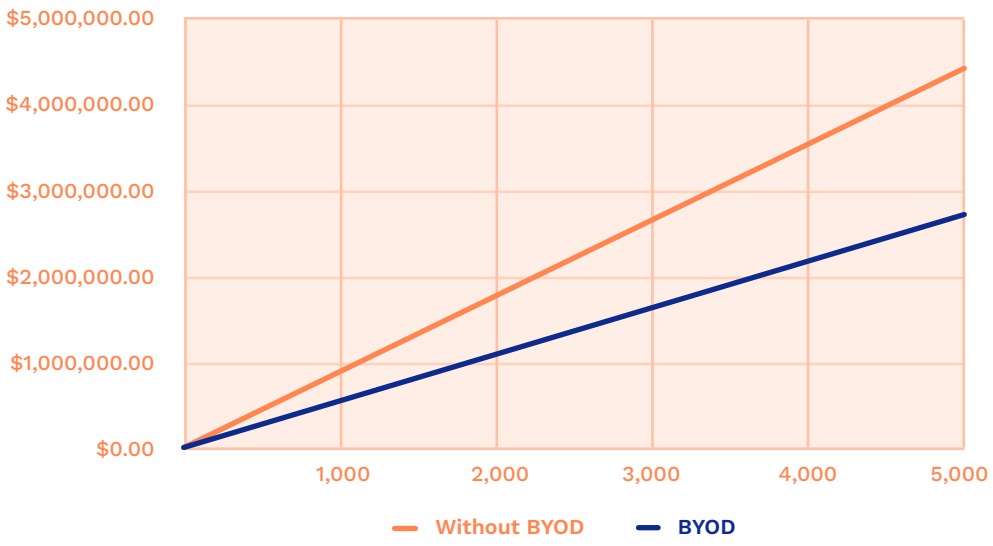


Fig.1—Annual cost of employee devices with and without BYOD

The data shows that implementing a BYOD policy can reduce device-related costs by 30–40 % per year.

Disadvantages of BYOD

Despite the advantages, BYOD comes with significant risks as well, since the organization has no guarantee that the employee or contractor devices will have the necessary security controls and vulnerability patches.

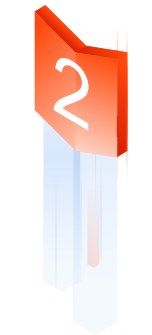
It is mainly for this reason that some companies prohibit BYOD completely, a practice that is particularly common among larger enterprises.

Data security risks

The first concern surrounding BYOD is security.

For example, these devices may lack up-to-date antivirus software, encryption, or even basic authentication. Users can also use unsecured public networks to connect to company resources, which leaves sensitive data (like access credentials) exposed to interception and theft.

In short, users tend to take fewer precautions with their own devices, which increases the risk of a data leak.



Lack of auditability and control

BYOD policies reduce the number of ways to check whether devices meet the required security criteria and to deny access for non-compliance.

Lost or stolen devices become a security hazard, since they provide an unchecked entry point to company data, and the organization lacks ways to deny their access.

A related factor may be that the employees themselves may resist using their device for work due to privacy concerns in cases where the organization requires monitoring software to be installed.

Support issues and compatibility

In any BYOD scenario there is going to be a variety in operating systems, software versions, or screen sizes. But not every business application may function correctly on all of these devices, which might lead to issues and additional support costs.

There is also the factor of unpredictability, as employees may change devices every few years.

Key challenges of a BYOD security policy

Despite the drawbacks, an increasing number of organizations see value in BYOD, and are willing to invest in measures that counter the security risks. Below is a description of the most common challenges and security measures to make BYOD a safe, practical and legally compliant reality.

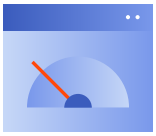
Platform diversity and compatibility

One of the biggest challenges in BYOD is the diversity of devices and operating systems. Employees and contractors bring devices running a wide range of operating systems—Windows, macOS, iOS, Android, and even Linux—each with unique vulnerabilities.

Additionally, the variety in software versions and hardware specifications introduces further unpredictability. Some business applications may not work optimally on all devices, creating compatibility challenges that can hinder productivity.

SOLUTION

Standardized access protocols and device management tools can bridge this gap, enabling centralized management, device monitoring, and remote troubleshooting. Regular compatibility testing and clearly communicated technical requirements are also crucial.

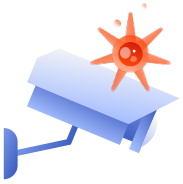


Central security management

Without Mobile Device Management (MDM) tools, organizations will struggle to enforce consistent security protocols across diverse devices. For example, ensuring that every device uses encryption, antivirus, and firewall becomes very complicated when none of the devices are issued by the company.

SOLUTION

Implementing cloud-based zero-trust architectures, which manage access based on device posture and user identity, can streamline this process. Organizations can enforce policies remotely, ensuring that only compliant devices gain access to critical resources.

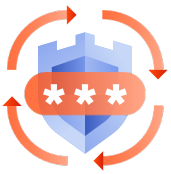


Incident detection and response

Another crucial aspect of a BYOD policy is the ability to detect and respond to security breaches on personal devices. Lost or stolen devices, malware infections, and unauthorized access attempts are a constant threat in a BYOD environment. Organizations need reliable means to detect these in real-time and cut off access automatically.

SOLUTION

A robust BYOD policy includes automated device posture checks, granular access logs, and configurable lockdown protocols. This means MDM solutions should work in tandem with access control solutions or be part of a Zero Trust Architecture because they generally cannot ensure access denial to non-compliant devices.



Enforcing updates and vulnerability patches

Devices running outdated software or lacking security patches pose a security risk, as they can be exploited by attackers using known vulnerabilities. A well-crafted BYOD policy should automatically detect devices with obsolete operating systems and block their access until the necessary updates or patches are installed.

SOLUTION

Policies should require regular software updates as a condition for accessing company resources. Automated detection systems can identify non-compliant devices and deny access until updates are applied.

Data privacy and compliance

Compliance with industry standards and regulations, such as NIS2, SOC2, HIPAA, or ISO/IEC 27001 can become difficult in BYOD scenarios where sensitive data is in personal devices beyond the protective reach of the organization's security countermeasures. In order to ensure compliance and avoid legal sanctions, organizations must ensure that personal devices do not compromise the privacy of customer or business data.

SOLUTION

Data classification and network segmentation strategies, alongside identity-based access protocols, can ensure compliance. For example, sensitive data can be restricted to virtual environments or encrypted storage that separates it from personal files.

Device posture check is also often required by standards and regulations, while some, like NIS2 explicitly recommend implementing a comprehensive security approach like Zero-Trust Architecture that combines all the measures mentioned above.

Why mid-sized enterprises struggle with BYOD

Not all companies have the resources to tick off every requirement listed in the previous section. Small and medium enterprises (SMEs) are at a particular disadvantage when it comes to cybersecurity in general, not just BYOD. However, that makes them no less susceptible to cyberattacks nor does it lessen their obligation to follow the requirements of cybersecurity standards and regulations (if the organization is obligated to comply).

SMEs lack the resources of large enterprises to implement robust BYOD security policies in-house, notably they suffer from smaller budgets and therewith connected shortage of qualified IT staff, which is why SMEs often look to outsource their security and compliance to external vendors and providers.

BYOD in Creative Dock

Creative Dock, a globally successful venture builder, **abandoned their legacy in-house solution for remote access and decided to implement a zero-trust architecture as a service** using GoodAccess' cloud platform.

This simple step allowed them to bring all the user and contractor devices under control without making any major changes to their existing infrastructure, and thus pave their way toward ISO/IEC 27001, which they sorely needed to continue doing business with some of their important clients.

CASE STUDY

How GoodAccess enhances BYOD security

GoodAccess is a cybersecurity platform that provides cloud-delivered zero-trust network access.

It envelops your critical systems, users, and their devices in a secure software-defined perimeter. Simply put, it ensures that no path leads to your sensitive data unless secured by GoodAccess.

This means that every device trying to connect must have an agent (client app) installed on it. This agent's primary function is to establish secure, encrypted connections with the zero trust network, which ensures that only authenticated and authorized traffic passes behind the perimeter.

However, the agent does more than that. One of its other functionalities is conducting regular device posture checks and comparing them to the security policies defined by your administrator in the Control Panel.

How central device management and BYOD work in GoodAccess

Before a device connects to the network (and optionally at regular intervals for the connection's duration), GoodAccess checks it for a number of security policies that you specify. Most common checks are whether antivirus software is installed, up-to-date, and running, whether a firewall is enabled, whether the system is up-to-date, and whether screen protection is enabled.

Devices that fail to meet the requirements are recorded and denied access (depending on configuration). The user will then receive a notification with an explanation of the violation, so that the vulnerabilities can be remedied.

Device Posture Check enables organizations to enforce their device policy instantly and automatically over every device in any location, and ensures that only verifiably secure devices will be allowed access to critical systems.

Your device security policy can consist of various requirements. For example, Windows devices can be checked for the following:

- Operating system version and latest update,
- Running and up-to-date antivirus software,
- Disk encryption,
- Windows Firewall status,
- Screen lock protection,
- Membership in a specific Windows Domain,
- Registry settings,
- A specified file on the hard disk,
- A specified process running, and more.

Your policy settings take effect immediately. This allows you to update your policy in real-time, e.g. when you find out a new vulnerability in a particular type of device or OS version.

Our observations tell us that organizations using GoodAccess manage on average two to three devices per user. A rule of thumb to multiply the number of Team Members by three, which gives you the number of devices you need to manage.

But the good news is that GoodAccess does not care if 50 or 50,000 devices log in. The automated mechanism enforces the device security policy immediately and for all the devices in your organization, even if you don't own them and there are thousands of them. Your critical resources will be accessible only to secure devices and properly authenticated and authorized traffic.

Conclusion

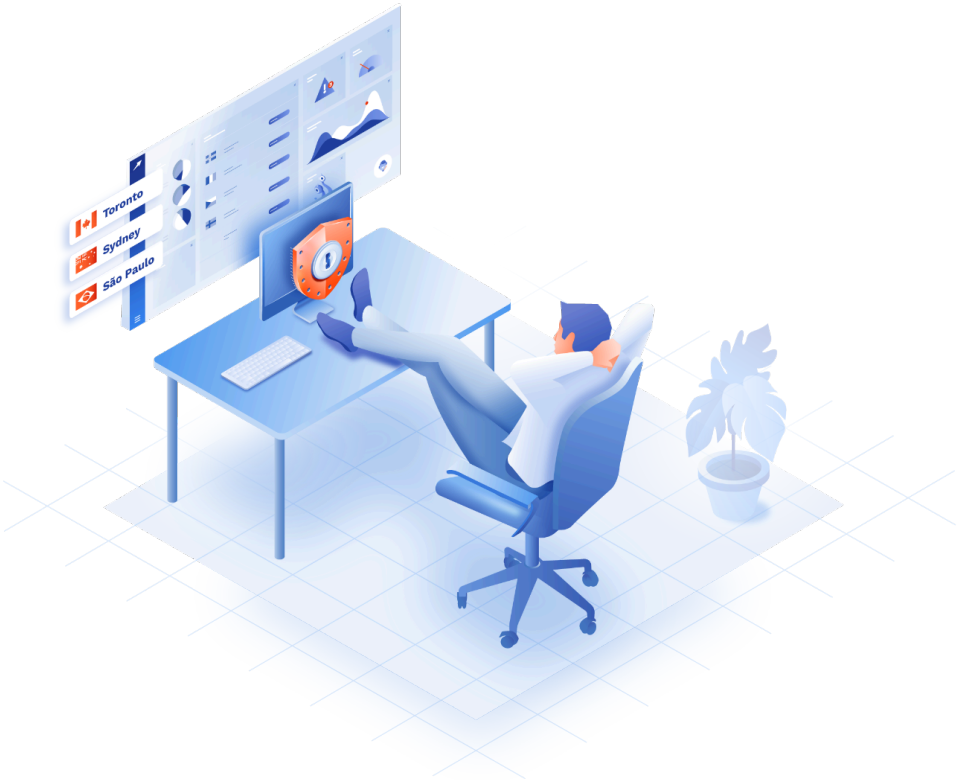
BYOD offers an opportunity for small and medium enterprises to enhance flexibility, increase employee satisfaction, and reduce costs.

However, it also introduces complex security challenges that the organization must address, such as the risk of data breaches, compliance violations, and operational disruptions demand a comprehensive approach to securing devices and managing access.

Small and medium enterprises (SME) are in a unique position due to their lack of in-house expertise and limited resources, which often limits them in their options of implementing an effective BYOD policy. However, this predicament is well addressed by implementing Zero-Trust Architecture.

Providers like GoodAccess can offer a tailored, scalable security platform that enables businesses and organizations to enjoy the benefits of BYOD without risking exposure of their sensitive data or breach of critical resources. By adopting robust policies and utilizing modern tools, SMEs can transform BYOD from a liability into a strategic advantage.

An effective BYOD strategy is not just about enabling access but about consistently securing the entire business environment and ensuring compliance while remaining cost-effective. When implemented properly, BYOD improves employee well-being, boosts productivity, and supports long-term organizational goals, making it a vital consideration for any forward-thinking organization today.



About GoodAccess

GoodAccess is a cybersecurity platform (SASE/SSE) that empowers medium-sized enterprises to easily implement Zero Trust Architecture (ZTA) in their infrastructure, regardless of its complexity or scale. By leveraging a Low-Code/No-Code approach, GoodAccess delivers a hardware-free, rapid deployment solution within hours or days, allowing companies to enhance their security without the need for in-house IT experts. Start your 14-day full-featured free trial at www.goodaccess.com.

Michal Čížek
CEO GoodAccess

E: **ceo@goodaccess.com**
W: **www.goodaccess.com**