Columbus

E-Book

Why Dynamics 365 Business Central Offers Better Security

IT teams managing on-premise software juggle security on multiple fronts:

- Protecting hard drives, server rooms and software, as well as keeping unauthorized users away from power or reset switches
- Managing data backups, ideally storing them offsite in fire- and waterproof containers
- Limiting access to products and features to only those employees who need it, and keeping disgruntled employees out after they leave
- Keeping up with security fixes and patches for operating systems and applications from Microsoft, and managing individual computer updates and security

All of this was made even more difficult with the pandemic, when workers left the four walls of the office in droves to work remotely and access corporate data from less secure home networks. This caused security headaches for even the most sophisticated IT teams.

IT professionals are right to be worried:

Hackers launch on average 50 million password attacks a day

Microsoft

Most attacks originate on-premises.

Microsoft

93% of organizations have been attacked by malware/ransomware in the past 24 months.

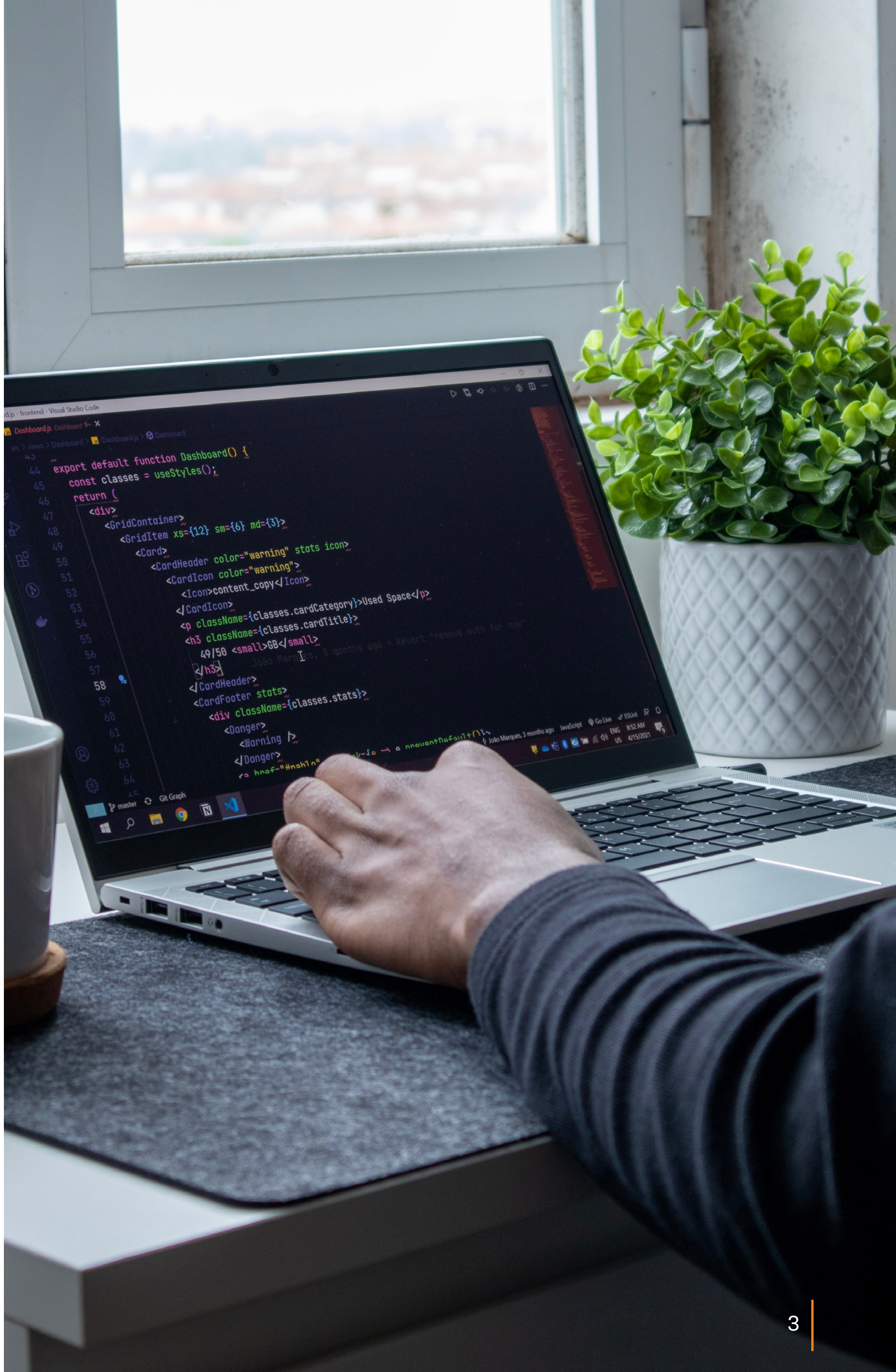
IDC

Two-thirds of SMBs experienced a cyberattack and 63% experienced a data breach in 2019

Ponemon Institute

The pressure is highest on Small and Mid-sized Businesses (SMBs), who may not have the money or enough trained manpower to successfully thwart security threats to their organization.

If you're considering a move from Dynamics GP to Dynamics 365 Business Central in the Microsoft Cloud, Azure, you'll want to be confident that Business Central protects your business. Here's a look at key areas where you'll see an upgrade in your security – and a downgrade in your stress levels.



The cloud shifts the burden

Not surprisingly, three-quarters of SMBs in a Ponemon Institute Report agreed they needed more emphasis on security. As a result, SMBs have increased their use of the cloud, saying that it's helped their IT teams do more with less – especially when it comes to security.

Flexera's 2020 State of the Cloud found that 70% of SMB workloads and data will reside in a public cloud over the next 12 months. Microsoft found the same in a survey of Microsoft Intelligent Security Association partners; 90% said customers have accelerated their move to the cloud due to the pandemic.

Many Dynamics GP users are considering a move to Business Central in the cloud as Microsoft says it has no plans to build a true cloud version of the GP product. And while GP can be hosted in the cloud, it's not a true cloud solution. Business Central is. Hosted in the Microsoft Cloud, SMBs don't have to worry about patching or upgrading server software or managing other security concerns. Microsoft's team fixes bugs and makes updates.

Consider the breadth of Microsoft's attention to security:

Microsoft offers multilayered security across data centers, infrastructure and operations. More than 3,500 global cybersecurity experts work to safeguard your business assets and data in Azure.

Microsoft is continually analyzing billions of Bing web pages, emails, Windows device updates and authentications. Using machine learning, behavioral analytics and application-based intelligence, Microsoft's data scientists analyze this data and the results inform Azure security and help customers detect threats faster.

All of that adds up to a much bigger reach than any one individual business has with an on-premise solution. In other words, with Microsoft Azure-based Business Central, your IT team just got a lot bigger so you can sleep more soundly.

Data is locked down

One of IT professionals' top concerns over the past year was the increase in people accessing corporate data across home networks. That's made data protection a top priority, as attackers often go after data storage first.

For cloud-hosted applications, Microsoft stores data in state-of-the-art data centers the company owns and manages itself. Microsoft's cloud services are also subject to scrutiny under ISO 27001, which contains hundreds of guidelines on how a CSP should manage its infrastructure to keep its customer data secure. Microsoft is regularly audited by the ISO to confirm its compliance with its rules and regulations.

Although Microsoft acts as custodians of your cloud data, you are the sole owner and administrator of that data. Microsoft doesn't mine data for advertising, and if you ever terminate service, you can take the data with you.

In the case of disaster, you're covered

Disaster recovery is how your organization responds to a natural or manmade disaster. Minimizing the impact on the business is a top priority. If you think it can't happen to you, you're wrong. Unfortunately, fewer than 50% of applications are protected by a disaster recovery plan, according to IDC.

Even seemingly simple "disasters" such as prolonged electrical outages or a server room flooding can have a devastating financial impact on an organization. Attacks on a company's infrastructure and data can also result in a big hit.

IDC reports that average per mission-critical workload downtime cost ranges from $2,500 per hour for smaller businesses to $50,000 an hour for large companies.

To respond, IT organizations need a disaster recovery plan, including backup/recovery to a secure and reliable site in the cloud and integrated with backup. According to IDC, on-premise backup solutions have always been "prone to both human error and infrastructure component failure" and that contracting through a third party is often too expensive for more than the largest companies and most critical systems.

An Azure-backed cloud solution like Business Central enables backup and disaster recovery more cost-effectively to prevent an expensive business disruption. IDC research has shown that backup in the cloud can be 76% faster than on-premise and data recovery can be 66% faster.

Peace of mind

Security is one of those parts of the job description that, for a dedicated IT professional, falls under the category of “things that keep you up at night.” The pandemic exacerbated that.

Forrester expects a 300% increase in employees working remotely post-pandemic compared with pre-pandemic. Walls are falling between business and personal activity, and that has brought home networks and devices into the corporate network and raised security risks.

What’s at risk? System downtime and lost revenue due to financial damages. An SMB is also less likely to survive a big hit.

If you’re considering Business Central for your next move, rest assured that Microsoft Azure provides industry-leading security on all fronts so you can spend less time controlling user access and making updates and more time focusing on the bigger strategic IT picture.

Contact:

☎ 888 209 3342 ✉ us-marketing@columbusglobal.com

About Columbus:

Columbus is a global IT services and consulting company with more than 2,000 employees serving 5,000+ customers worldwide. We help ambitious companies transform, maximize and future-proof their businesses digitally. Our industry expertise is in manufacturing, food & beverage, distribution and rental equipment. We offer a comprehensive solution portfolio with deep industry knowledge, extensive technology expertise and profound customer insight. Columbus has offices and partners all over the world so we can deliver our solutions and services locally, but on a global scale. www.columbusglobal.com

Columbus®