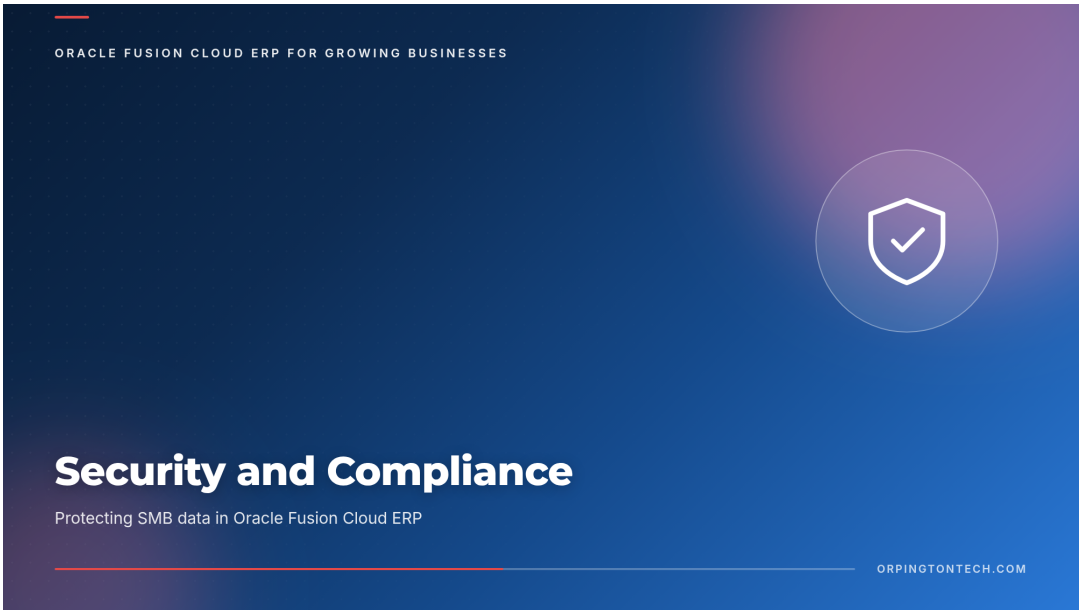


ORACLE FUSION CLOUD ERP FOR GROWING BUSINESSES

Security and Compliance: Protecting SMB Data in Oracle Fusion Cloud ERP

What growing companies must get right before they trust the cloud

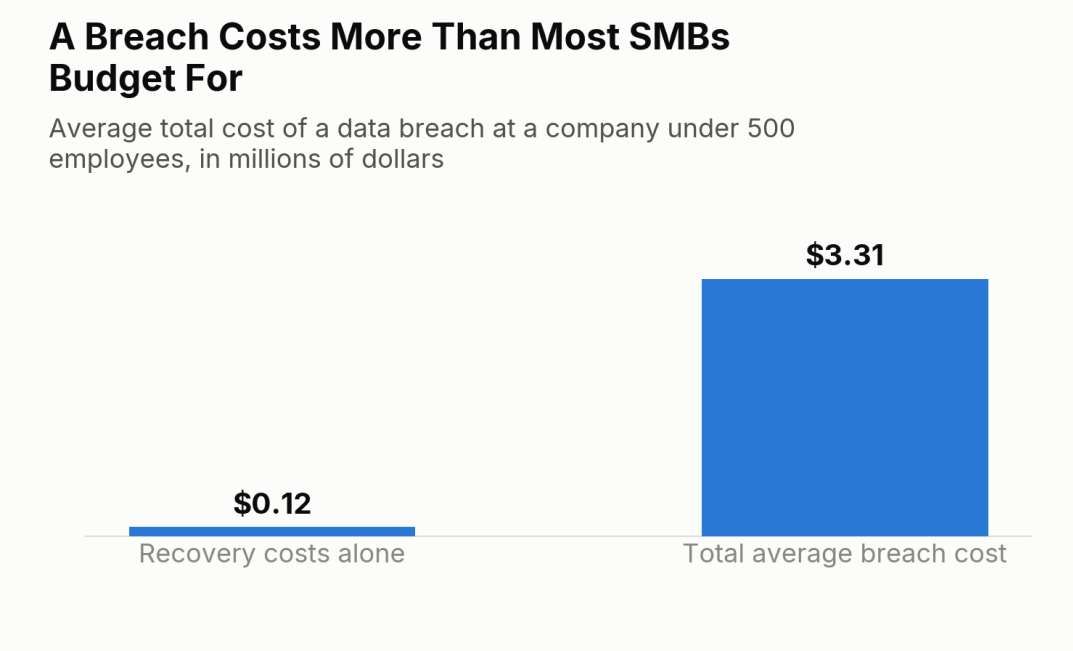
There's a common assumption among smaller companies that cybercriminals mostly go after large, high-profile targets — banks, hospitals, household-name retailers. The data says the opposite. Small businesses aren't collateral damage in a world of big targets; they're often the preferred target, precisely because they tend to have weaker defenses and less dedicated security staff than the enterprises that make headlines when something goes wrong.

That gap between perception and reality is exactly why security and compliance deserve their own serious conversation in any discussion of moving core business systems to the cloud — Oracle Fusion Cloud ERP included.

The numbers are more alarming than most owners assume

Roughly 43% of all cyberattacks target small businesses specifically, and research from Verizon and others suggests small companies are about three times more likely to be targeted than larger organizations. The financial consequences, when an attack succeeds, are not scaled down to match company size the way a smaller business might hope. The average total cost of a data breach at a company with under 500 employees runs an estimated $3.31 million, with recovery expenses alone

averaging around $120,000 and downtime costing roughly $53,000 for every hour systems are unavailable.



Breach recovery costs are a fraction of the total financial impact — downtime, lost business, and remediation add up fast. Source: StationX, 2026.

The existential stakes are real, too. Verizon's 2025 Data Breach Investigations Report found that 19% of small businesses that suffer a breach face bankruptcy as a direct result, and separate research from VikingCloud found that 40% of small and mid-sized businesses say an attack costing $100,000 would be enough to end their operations entirely. For a company running lean, without deep cash reserves, a security failure isn't just an IT problem — it's a genuine survival risk.

3x

how much more likely small businesses are to be targeted by cyberattacks compared with larger organizations — despite typically having far fewer resources dedicated to defending against them.

Source: Verizon / StationX, 2026

Why moving to the cloud changes the security equation, mostly for the better

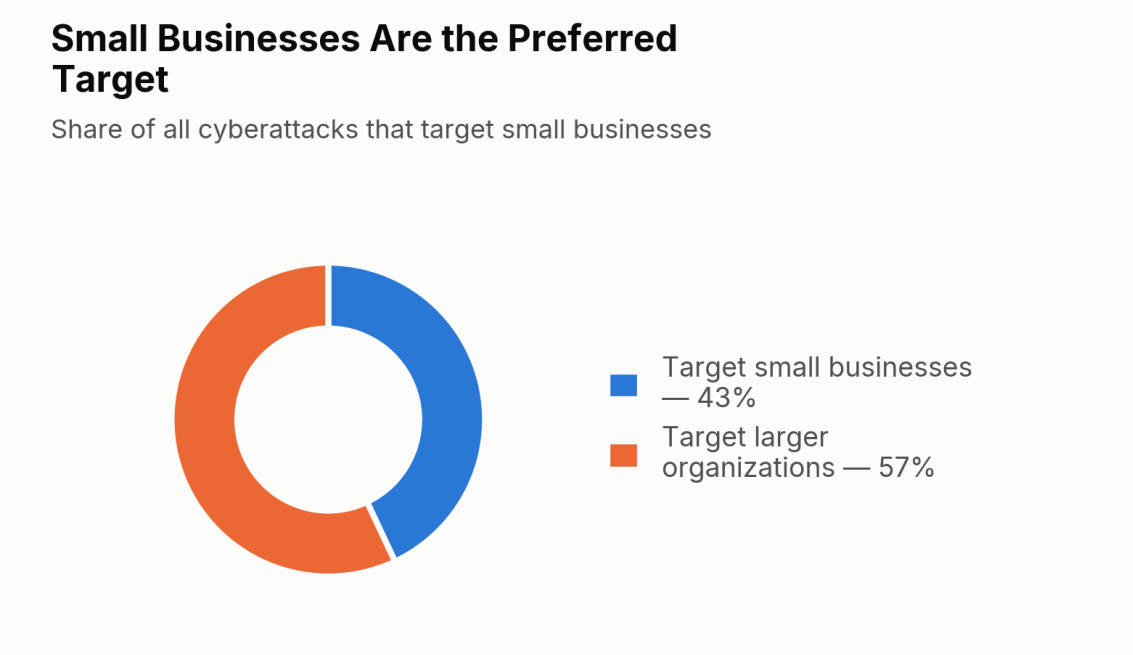
It might seem counterintuitive that moving financial and operational data to a cloud platform improves security, given how much attention cloud breaches get in the news. In practice, for most SMBs, the comparison isn't between "cloud" and "perfectly secure on-premise infrastructure" — it's between a cloud platform backed by a vendor with dedicated security teams, continuous patching,

and enterprise-grade infrastructure, versus an on-premise server that hasn't had its software updated in eighteen months because nobody at the company has the bandwidth to manage it properly.

Oracle Fusion Cloud ERP's security architecture includes data encryption both at rest and in transit, granular role-based access controls that determine exactly what each user can see and do within the system, detailed audit trails that log who accessed or changed what and when, and infrastructure-level protections that most SMBs would have no realistic way to replicate on their own hardware and budget. None of this makes a company immune to attack — nothing does — but it shifts a substantial share of the security burden onto a vendor whose core business depends on getting it right at scale.

Where responsibility still sits with the business, not the vendor

This is the part that gets glossed over too often: moving to a secure cloud platform does not mean security becomes someone else's problem entirely. Cloud security operates on what's generally called a shared responsibility model — the vendor secures the infrastructure and the platform itself, but the customer is still responsible for how they configure it. Weak password policies, overly broad user permissions granted out of convenience, poorly managed integrations with third-party tools, and employees who fall for phishing attempts are all risks that exist regardless of how secure the underlying platform is, and they're squarely the customer's responsibility to manage.



Small businesses face a disproportionate share of cyberattacks relative to their size and resources. Source: StationX / Verizon, 2026.

This is also where compliance requirements come into play, and they vary considerably depending on industry and geography — companies handling payment data need to think about PCI DSS, healthcare-adjacent businesses need to consider HIPAA, and companies with customers or operations in Europe need to think through GDPR obligations regardless of where the company itself

is headquartered. A platform like Fusion Cloud provides the tools to meet these requirements — audit logging, data residency options, access controls — but configuring them correctly for a specific company's actual regulatory exposure is a project in its own right, not something that happens automatically the day the system goes live.

The gap between "the software is secure" and "we're actually secure"

This is precisely where a lot of smaller companies get a false sense of security. IT leadership sees that the ERP vendor has strong certifications and assumes that translates directly into organizational safety, without validating that the specific configuration — user roles, integration security, data access policies — was actually implemented correctly for their business. It's a bit like assuming a house is secure because it has a good lock, without checking whether anyone actually locked the door.

An increasing number of CFOs and boards have started insisting on independent verification of exactly this gap before signing off on a go-live — not because they distrust the platform, but because they've learned that "secure software, configured carelessly" is a common and expensive failure mode. This is one of the areas firms like Orpington Technologies specifically assess as part of an ERP readiness review: not whether Oracle Fusion Cloud is secure in the abstract, but whether the specific implementation a company is about to depend on was actually configured the way it should have been.

Looking ahead

Security is fundamentally about protecting what a company has already invested in building. The next article in this series turns to a related but distinct question that every CFO eventually has to answer with real numbers: what does an Oracle Fusion Cloud ERP implementation actually cost, all in, and what kind of return can a small or mid-sized business realistically expect for that investment?

Sources

1. Small Business Cybersecurity Statistics and Trends [2026], StationX — https://app.stationx.net/articles/small-business-cybersecurity-statistics