Infor M3 – The Challenge of API Security

From internet connected toasters to integrated social media platforms, our world is becoming ever more interconnected.

This increase in connectivity has the potential to greatly boost collaboration and productivity (as well as guaranteeing your toast is ready 5 minutes after your alarm goes off in the morning). But from a cyber security standpoint, it brings with it a whole new set of challenges, because increased integration means more potential vulnerabilities. This general trend will affect most enterprise applications, Infor M3 included.

In the past, many Infor M3 customers based their API security on the simple fact that setting up access via API was technically complex and therefore difficult to exploit. But maturing API technology that allows APIs to run through a web browser and the introduction of REST APIs (among other things) has made this process far less technical.

On the one hand, this is great for Infor M3 users, making it easier than ever to integrate Infor M3 with other systems. But less technically complex APIs also make Infor M3 easier to exploit, meaning robust API security is absolutely vital.

And herein lies the problem, because managing API security in Infor M3 can be extremely challenging.

There are several reasons for this, but perhaps the most important is that API security is managed completely separately from functional security in Infor M3 (something we've found many Infor M3 customers aren't even aware of!). Now, there are good reasons for doing this, but the upshot is that setting up and maintaining API security in Infor M3 is extremely time-consuming.

API security is binary: it's either switched 'off', and everyone can run APIs, or 'on', and no one can. For businesses already using Infor M3, simply turning API security on, then, is not an option, as it would restrict Infor M3 users from running APIs altogether, grinding workflows across the business to a halt. Instead, the relevant permissions must be setup individually for each member of staff using Infor M3, which is in itself a huge task.

Let's take the Smart Office APIs as an example. There are 5 in total, and each API has 5 corresponding transactions. That's 25 permissions to configure per employee just to successfully integrate Smart Office. Scale this up for a medium-sized company of 300 people, and we're talking 7000 individual permissions to configure—all of which must be done manually—to integrate just one of the many programs users need access to.

For most companies, the manpower required to administer this process is simply unsustainable, particularly when factoring in the ever-changing landscape of joiners, movers, and leavers, and the fact that Infor are constantly striving to develop and implement new APIs on a regular basis—again, great for Infor M3 customers, but a real headache for the security admin who's trying to keep up.

This has led to some companies forgoing API security altogether, but the consequences of doing so can be severe, opening up your ERP and data to exploitation both from internal and external attacks.

At Vince, we believe the security of your ERP solution is non-negotiable, which is why we created VSE — Vince Security. With VSE, we've dramatically simplified security for Infor M3, allowing you to quickly and comprehensively protect your ERP solution.

API security comes as standard with VSE, and we've mapped every single Infor M3 API against its relevant functions, meaning API security is taken care of automatically in line with your Infor M3 settings. This means granting an employee access to a function automatically gives them the relevant API permissions at the transactional level, turning what was once an extremely time-consuming and manual task into something that takes just a couple of clicks.

If you'd like to learn more about VSE, click here to view our product page.

VINCE AS
Inkognitogata 34, 0256 Oslo
Telephone: +47 951 01 321
E-Mail: peder.floer@vince.no