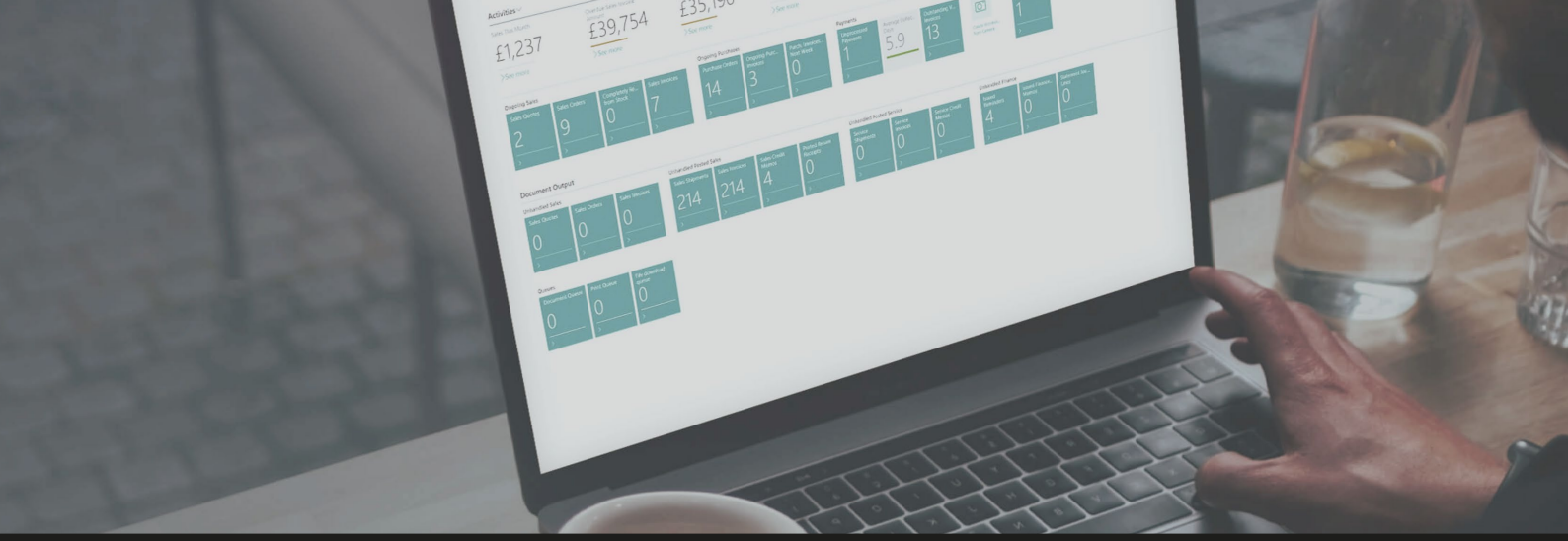


Continia Software

Continia won back a fifth of its IT capacity by removing local admin rights.

Continia Software is the leading provider of fully embedded finance automation solutions for Microsoft Dynamics 365 Business Central. With over 30 years dedicated exclusively to the Dynamics ecosystem, Continia helps organizations transform their daily financial operations, and today more than 32,000 organizations trust it to run their finance processes accurately and efficiently. Much of that work involves sensitive financial data for customers who demand robust, compliant security, many of them under NIS2.

Industry:
Software / Financial Automation

Number of Employees:
~200

Operating System:
Windows 95% / Mac 5%

Endpoints on ABR:
300

The Challenge

Before Admin By Request, every user at Continia was a local administrator, and in the team's own words, had far too much power over their own machines. Employees could install whatever they wanted: browser extensions, meeting-recording tools that captured internal meetings, image and video editing software. More seriously, someone had installed betting apps on a company machine, and someone else had installed old spyware they were "testing," software that logged everything happening on the PC.

The company relied on a single endpoint protection tool that only flagged something when it happened to catch it. Otherwise, unwanted software surfaced only when someone from IT walked past a screen or opened up a machine for repair, and for a long time that detection rested on one administrator.

The manual review was a significant, recurring drain. René, the IT administrator, spent around six hours a week (often the first hour or so of every morning) working through a long list of Defender alerts and sorting the important from the unimportant. If he was ill, travelling, or on another project, the backlog simply grew.

The Solution

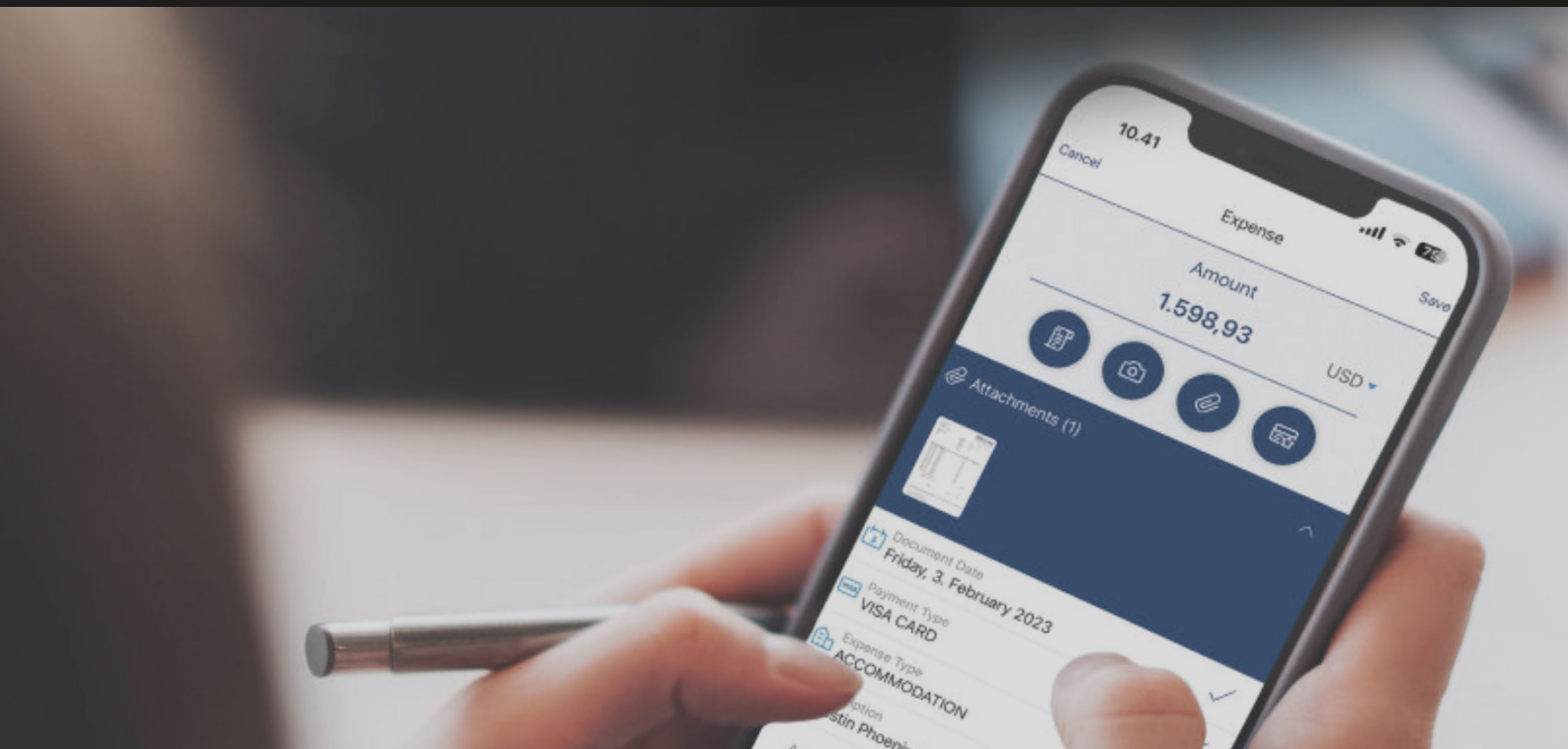
Continia had a concrete goal that made removing local admin rights unavoidable: achieving ISO 27001 certification, which the company did not yet hold. It helped that René already knew Admin By Request from his previous role at Mariagerfjord Kommune, so when the ISO need became pressing, he turned to a product he already trusted.
The team configured Admin By Request around how their people actually work. For most office users, requests go through an approval workflow with the reason logged. For developers, who make up a large part of a software company and who initially loved the freedom of local admin, the team found a balanced model: they can self-approve their own elevation sessions, secured with MFA, so a full log exists without slowing them down. Since most development happens in Docker or source control, very little needs to run locally in the first place.

One deliberate security decision illustrates the team's approach. Several developers argued that PowerShell should be whitelisted for automatic elevation, and René pushed back: if anyone who gained access could freely run PowerShell, the security benefit would evaporate. It stayed off the self-approval list.
Change management came down to listening and explaining. The team heard people out, then made clear why local admin rights had to go and why every elevation needed a logged reason. For office users accustomed to a sandbox playground there was an adjustment period, but it faded quickly once the rules were understood.

> I hear almost nothing from them now. They've learned to think before they act. What comes in to us as a request is considered and written down. That's exactly what we wanted to hear.

René Yde Haggren, IT Administrator, Continia Software

Admin By Request
ZERO TRUST PLATFORM



The Impact

The six hours a week René spent manually sorting alerts has almost disappeared. Incident review is now a quick daily check, with deeper investigation only when something is genuinely serious, because threats are stopped before they become incidents. It also put an end to the "sour email" from René or his boss whenever unsanctioned software turned up, since those installations simply can't happen anymore.
For a two-person team supporting 200 people across 45+ locations, the capacity freed up has been substantial, and it went somewhere specific: the work required to achieve ISO 27001 certification. Instead of running from one burning house to the next, the team could finally move forward. The security gains came alongside it, with staff now having to think about what they install and integrated malware scans drawing on more than 35 antivirus engines. Fewer accidents, fewer bad days when something goes wrong, and, in the words of Mark (who joined René a year ago), more peace of mind.

> Before, I only ran from one burning house to the next. Now, going through these problems is a very small part of my week. I'd say we've won back 15 to 20% of our IT capacity. That's the equivalent of rescuing an entire position, and it's the time we needed to work toward our ISO 27001 certification. And if I had to highlight one thing beyond the software itself, it's the support: you get an answer immediately, an answer you can actually use. Ten out of ten.

René Yde Haggren, IT Administrator, Continia Software

Moving Forward

The team continues to lean on pre-approved applications wherever it makes sense, automatically clearing trusted software so neither users nor IT has to handle a request each time an update appears.

> I'd say we've become 20 to 25% more secure. Half an hour before this meeting, a colleague tried to install adware, and Admin By Request caught it and flagged it as malware before it ever reached the machine. That's exactly the point: it stops threats before they get installed, instead of us finding out afterwards.

Mark Bøge, Cloud Administrator, Continia Software

Admin By Request
ZERO TRUST PLATFORM

