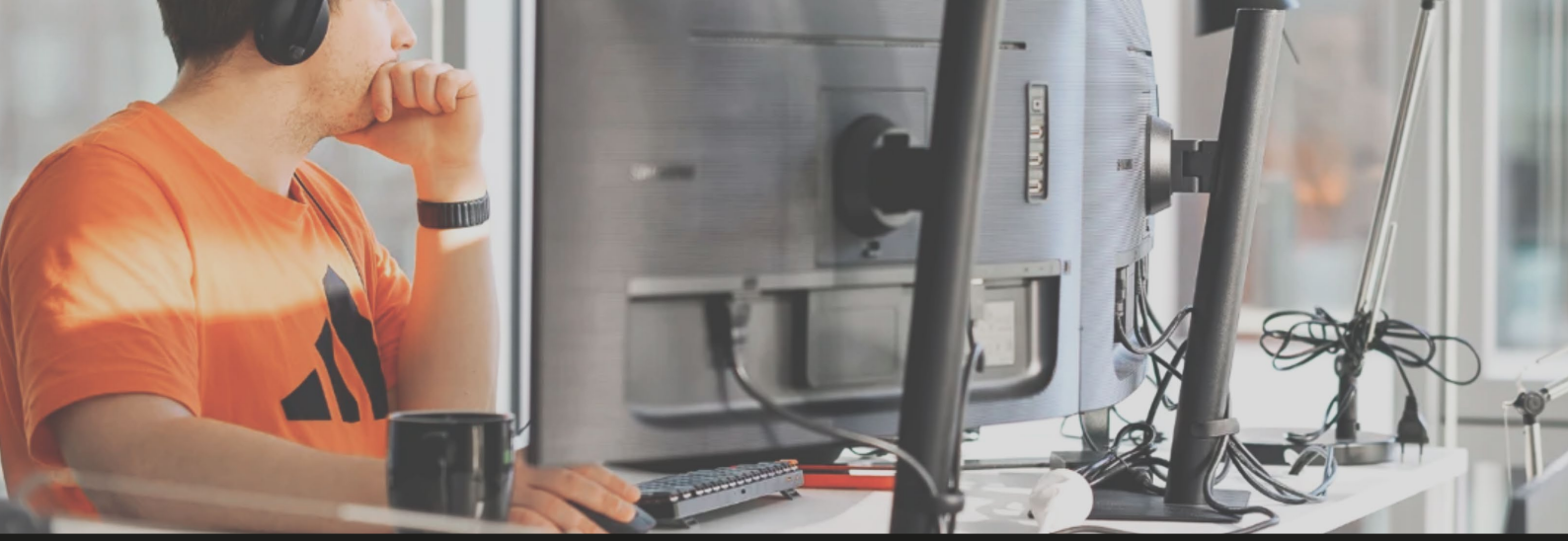


KMD

How KMD secured 3,000 endpoints and cut permanent local admins from 1,500 to zero

KMD is one of Denmark's largest IT companies, building software and services for public and private sector organizations whose systems process around 10% of Denmark's GDP each year.

Industry:

IT Services & Consulting

Number of Employees:

~3,000

Operating System:

Windows 90% / Mac 10%

Endpoints on ABR:

~3,000

KMD

The Challenge

By 2019, KMD identified that standing admin access created unnecessary security exposure and looked to modernize its approach. For a company serving critical infrastructure operators across Denmark, ensuring tight administrator access with a seamless workflow was exactly the kind of work its security standards called for. A LAPS solution had previously served as admin privilege control, but elevation was session-based and the process friction was worse: developers copy-pasted credentials for every tool they installed, roughly forty seconds a day, which across 1,000 developers came to over 2,200 hours a year.

The Solution

When the team saw a demo of Admin By Request's EPM solution, it mapped directly onto the Zero Trust principles they had already committed to: just-in-time elevation, layered defense, least privilege, assumed breach. The decision came around two and a half years ago, timed to a migration from hybrid-joined to Azure-joined devices, and with a carefully planned phased approach quickly scaling to 800 users within a single month. The decisive factor was treating different users differently while keeping the experience invisible to most of them. For the

60% in non-technical roles, pre-approval policies covered nearly everything from day one. For developers, just-in-time elevation replaced the semi-manual workflow, with app whitelisting handling around 95% of use cases before a request is ever needed. The audit trail generated by the platform supports KMD's ongoing compliance program, reducing the manual review burden significantly.

The Impact

The outcome Dion Kær Andersen hadn't expected was taking admin rights from thousands of users without a spike in support load. Volume stayed flat, and a month or more can now pass before a single local-admin case appears in the queue. After the elevation window was adjusted based on feedback to better fit how developers work, complaints stopped entirely. The 2,200-plus hours once lost to semi-manual credential generation now flow back into KMD's mandate to digitalize Denmark, spent building the software its clients depend on. In an organization whose systems process around 10% of the country's GDP, every hour freed from friction is an hour returned to that work. Combined with the move to Azure-joined devices, the rollout pushed KMD's compliance posture forward sharply. The Admin By Request audit log, a timestamped record of every elevation and install, underpins KMD's ISO audits and feeds its Cyber Defence Centre, removing 90 to 95% of what would otherwise need manual review.

Moving Forward

KMD continues to strengthen its Zero Trust posture across its infrastructure, investigating deeper integration and automations between the audit data and the Cyber Defence Centre's alerting, moving from post-mortem analysis toward catching anomalies before damage is done.

> 40 seconds per day for 1,000 developers, across every working day of the year: that time accumulates into an enormous business case. And if people start their day frustrated, you will never get tailwind in IT. Admin By Request made it possible to implement real security control in a way that people can actually live with
>
> Dion Kær Andersen, Head of Modern Workplace

Admin By Request
ZERO TRUST PLATFORM

