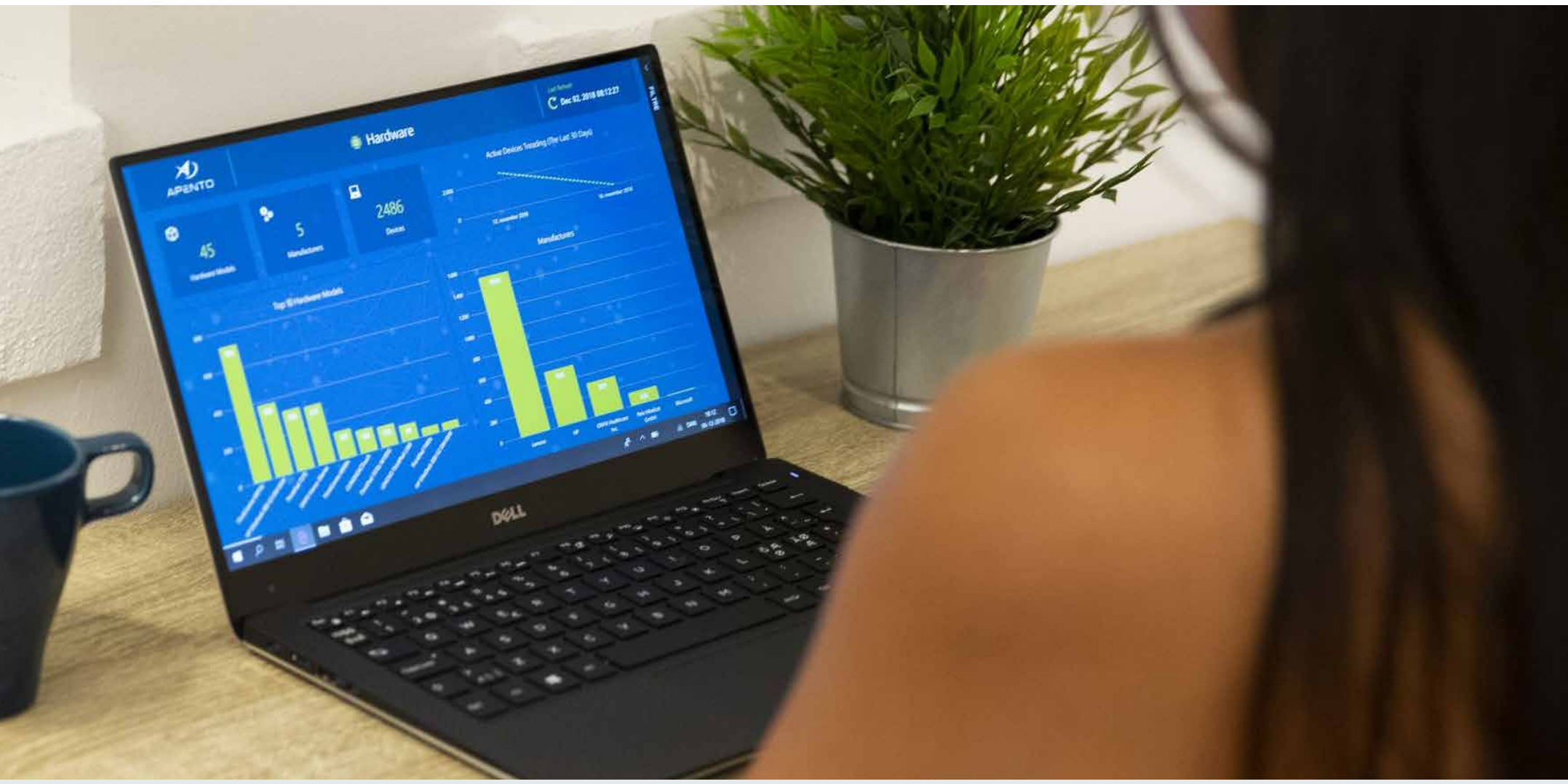
Fra blinde vinkler til proaktiv indsats

Unikt analyseværktøj samler indsigt om alle Windows-klienter på et sted

APENTO

APENTO Device Analytics gør det muligt at

- ✓ **Eliminere de blinde vinkler**
- ✓ **Prioritere IT-afdelingens indsatser**
- ✓ **Handle proaktivt**



Med APENTO Device Analytics kan I overvåge samtlige Windows-klienter i én løsning

På alle væsentlige områder tager APENTO Device Analytics temperaturen på jeres Windows-klienter og viser jer status på overskuelige dashboards.

Få for eksempel indsigt i reelle start-op tider og klart svar på, hvor mange og hvilke Windows-klienter, der ikke er krypterede eller sikkerhedsopdaterede. Pinpoint de mest upålidelige maskiner, og eliminer tidsspilde som følge af blå skærm.

Power BI dashboards giver dig overblikket

Med APENTO Device Analytics får I samlet al info på et sted om, hvordan Windows-klienter kører, hvilke funktioner, der er slået til, og hvordan de er opdateret.

Data opbevares i Microsoft Azure og tilgås via APENTO Device Analytics Power BI-rapporter i form af dashboards.

Herfra kan I dykke ned i de underliggende data, belyse udfordringerne yderligere og identificere den enkelte maskine med problemer.

Fire årlige statusmøder med konsulent

På statusmøder hver tredje måned gennemgår I dashboards sammen med en konsulent fra APENTO, og I modtager anbefalinger på basis af de indsamlede data.

Ny æra med APENTO Device Analytics

Løsningen giver jer nogle kæmpestore fordele i IT-afdelingen. Når en bruger henvender sig, kan I langt nemmere sætte problemet ind i en sammenhæng. For APENTO Device Analytics har allerede gjort forarbejdet gennem tilbundsgående analyser.

Løsningen hjælper jer også til at prioritere indsatserne i en travl hverdag, fordi I konstant har klarhed over, hvor skoen trykker mest.

Og I kan melde ud og handle mere proaktivt, fordi I har en viden om, hvor det er nødvendigt at sætte ind.

Brug også analyserne i budgetmæssig sammenhæng til at dokumentere behov.

Fordele med APENTO Device Analytics

Overblik over:

- ✓ Compliance
- ✓ Sikkerhed
- ✓ Slutbrugeroplevelse

Værdi:

- ✓ Hjælper med at finde forbedringsmuligheder
- ✓ Du kan følge med i, om igangsatte projekter har den ønskede effekt
- ✓ Indikerer, hvornår det er på tide at udskifte maskiner

Få indsigt i alle Windows-klienter på et sted

Analyserne i APENTO Device Analytics samler data fra alle jeres enheder og præsenterer dem som overskuelige søjlediagrammer, grafer og lagkagediagrammer i Power BI dashboards. Hvis I ønsker det, er der naturligvis også mulighed for at vise analyserne i PDF-format og regneark.

Disse indsigter vil du ikke undvære

På de følgende sider får du indtryk af, hvordan APENTO Device Analytics kan hjælpe jer.

Vi har samlet et udsnit af de dashboards, der er med i løsningen, under temaoverskrifterne **Performance**, **Security** og **End User Experience**.

Her får I indsigt i nogle områder, som I formentlig bokser med en gang imellem.

Fra IT-chefer, der allerede bruger løsningen, ved vi, at de nødigt vil undvære disse indsigter. Fordi de giver værdi i en daglige IT-drift.

Performance

Startup Time:
Afslør uacceptabelt lange start-op tider

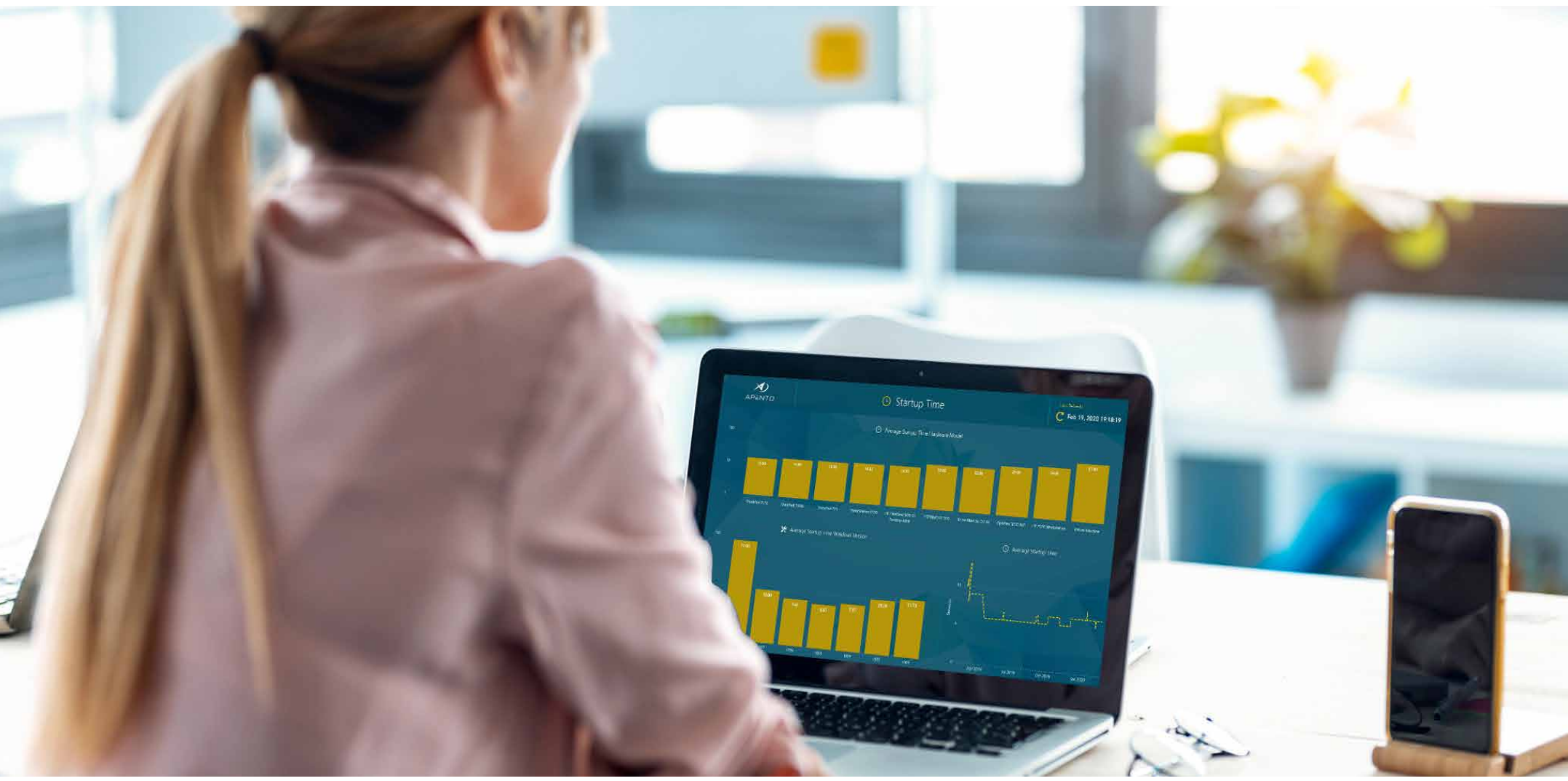
De fleste medarbejdere finder sig i lange start-op tider. Nogle af dem har måske vænnet sig til at indlægge en længere kaffepause fra dagens start, mens deres maskine bliver klar.

Du hører nok ikke om det. Men sagen er, at det koster arbejdstid, og det kan blive til store tab, hvis I har mange PC'er.

Med APENTO Device Analytics bliver disse mørketal krystalklare. Du kan se, hvor mange sekunder de enkelte PC-modeller bruger på at starte op.

Ved du i øvrigt, hvor lang tid Windows tager om at starte? APENTO Device Analytics giver dig svaret og viser den gennemsnitlige starttid på de enkelte Windows-versioner.

Brug data til at højne både effektiviteten og brugeroplevelsen.



Login time:

Få styr på hvor lang tid login reelt tager

Klager dine brugere over, at det tager for langt tid af logge på deres maskiner? Umiddelbart kan det være lidt svært at forholde sig til disse klager, som naturligvis er både individuelle og subjektive.

Derfor kunne det være rart at få nogle facts på bordet.

Login Time dashboard'et i APENTO Device Analytics leverer netop det. Du får overblik over, hvor lang tid det gennemsnitligt tager, før en enhed er klar til brug. Og hvor lang tid, det tager at logge på Windows.

Du kan også se, hvordan udviklingen i login tid har været over tid – og fordelt på Windows-versioner.

På den baggrund kan du nemmere afgøre, hvad det er for et problem, du står overfor.

Security

BitLocker:
Opklar om alle Windows-klienter er krypterede

Hvor stort er problemet, hvis en medarbejder får stjålet sin maskine ved et indbrud i bilen? Som bekendt er det til at overse, hvis BitLocker er slået til, og maskinen krypteret. I modsat fald kan det være yderst kritisk.

APENTO Device Analytics giver dig det enkle svar: Er BitLocker slået til eller ej på jeres Windows-klienter.

På BitLocker dashboard'et kan du se, hvor mange maskiner, der ikke er compliant - fordelt på Windows versioner. Og du får indsigt i, hvordan I performer på dette område over tid.

Dermed får du fikset problemet nu og her – og kan løbende følge med.

Virus Protection:
Tjek hvor mange maskiner, der er uden virusbeskyttelse

APENTO Device Analytics henter data i Microsoft Security Center. Så det, du ser på dit Virus Protection dashboard i APENTO Device Analytics, er ganske enkelt alle jeres Windows-klienter på en gang.

På få sekunder har du svar på, om I har et problem på dette område eller ej, og hvor stort det i givet fald er.

Tjek hvor mange Windows-klienter, der har en virusbeskyttelse, som er compliant, og hvilke maskiner der kræver opmærksomhed. Se, hvor mange der er uden virusbeskyttelse på de enkelte Windows-versioner.

Der er også en graf, som viser den historiske udvikling.

Firewall:

Opdag om Firewall er slået fra på nogle af jeres Windows-klienter

Ingen kæde er stærkere end det svageste led. Så i dette dashboard i APENTO Device Analytics ønsker du bestemt ikke at se for høje tal i det røde felt.

Men det er jo væsentligt at vide, om Firewall'en er disabled på en maskine. Og det er præcis den indsigt, du får her.

Dashboard'et henter data om Windows' indbyggede Firewall og afslører, om alt er, som det skal være. Hvor mange maskiner er ikke compliant? Hvilke Windows-versioner har disse maskiner?

Som på andre dashboards i APENTO Device Analytics kan du også se udviklingen i Firewall compliant maskiner over tid.

Secure Boot:
Hold skadelig software på lang afstand

APENTO Device Analytics hjælper jer også med at identificere problemer med Secure Boot.

I det daglige er det unægtelig noget af en opgave at tjekke det. Men også her får du hjælp fra APENTO Device Analytics.

På Secure Boot dashboard'et kan du på sekunder se det, der ellers ville koste timers og dages arbejde at finde frem til. Du får indsigt i, hvor mange maskiner der ikke har Secure Boot slået til.

Følg også udviklingen over tid.

BIOS Information:
Spot de sårbare maskiner uden opdateret BIOS

Hvordan ser det ud hos jer? Er BIOS opdateret – eller kunne der være maskiner, som ikke har været opdateret i en årrække og derfor er sårbare?

Med BIOS Information i APENTO Device Analytics kan du grave ned i denne udfordring, og som på andre felter får du et samlet overblik som udgangspunkt for prioritering og løsning.

Se typen af BIOS, og hvor mange maskiner, der er legacy eller kører EUFI.

Tjek, hvornår BIOS er opdateret, og hvordan disse opdateringer fordeler sig på antallet af maskiner.

End User Experience

Network Reset Event:
Få overblik over, hvor ofte medarbejderne oplever “frysninger”

Det er både irriterende og tidkrævende for dine brugere at miste forbindelsen til netværket. Hvis du løser det, vil det helt klart højne brugeroplevelsen.

Nu får du mulighed for at angribe problemet, idet APENTO Device Analytics giver dig overblik over det.

Frysninger som følge af Network Reset Events rammer ikke alle PC-modeller lige ofte. Og med den indsigt, du får på dit Network Reset Event dashboard, kan du igangsætte initiativer til at nedsætte antallet af events.

Se for eksempel, hvilke Windows-klienter, der har flere end 10 events, som jo nok må siges at være uacceptabelt mange.

Reliability Index:

Pinpoint de mest upålidelige maskiner

Med APENTO Device Analytics får du mulighed for at identificere upålidelige Windows-klienter, som er årsag til forringet brugeroplevelse.

Løsningen præsenter et samlet overblik over maskinernes pålidelighed - baseret på Windows' egen udregning.

Jeres Windows-klienter grupperes efter den score, de opnår, og det fremgår umiddelbart, om der er problemer, og hvor store de er.

Hvis den gennemsnitlige score er omkring 8 og nogle maskiner opnår under 4, er det oplagt at kigge nærmere på disse maskiner.

I nogle virksomheder anvendes Average Reliability Score Index som en KPI.

Application Reliability:

Få bedre styr på applikationer der crasher

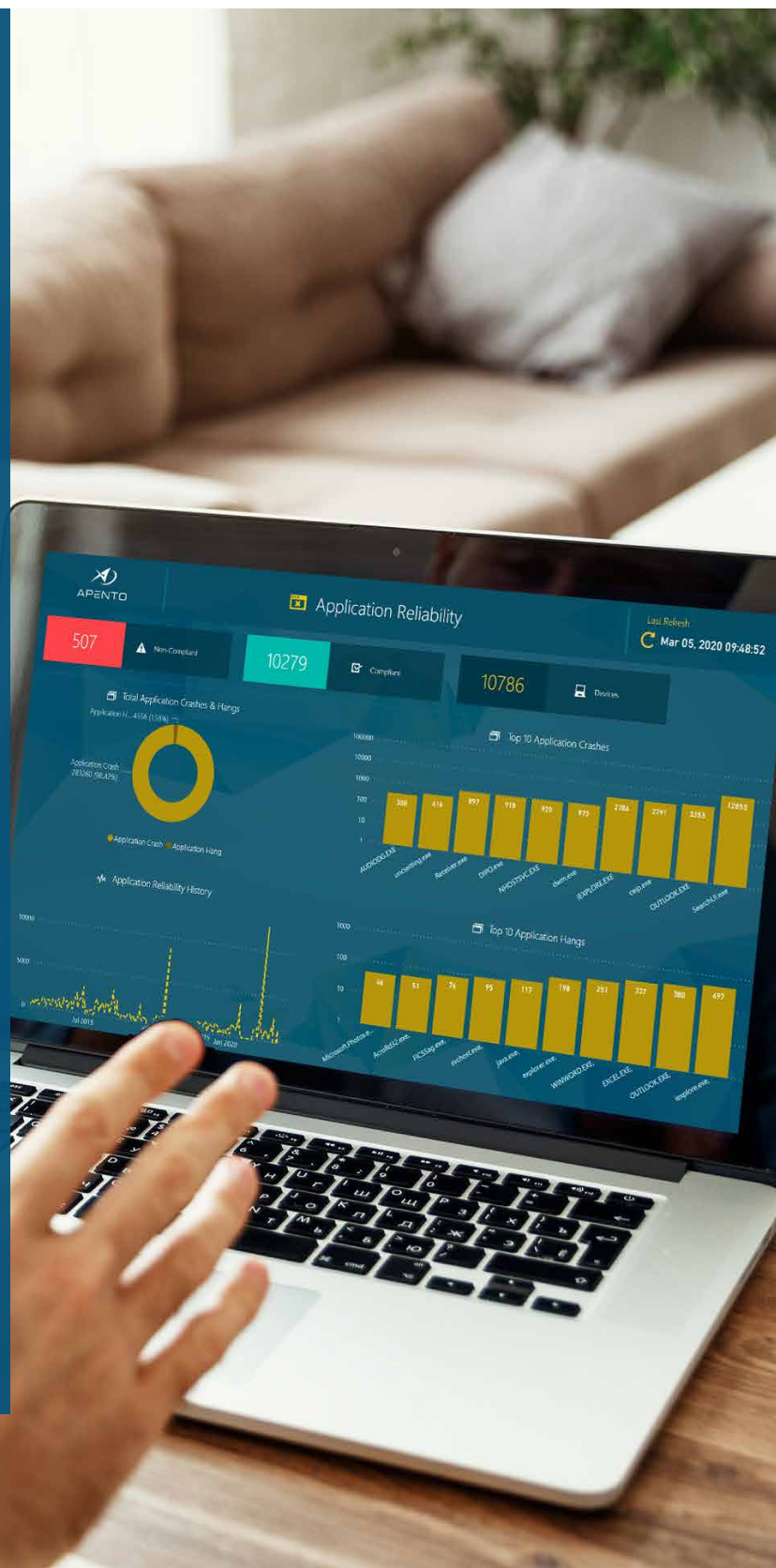
Applikationer, der crasher - for eksempel i forbindelse med opdateringer - giver skår i brugeroplevelsen og koster arbejdstid.

APENTO Device Analytics giver indsigt i årsagen til problemet, og hvad det skyldes.

I Top 10 Application Crashes på Application Reliability dashboard kan du se, hvilke applikationer, der crasher mest. Og en graf viser, hvor pålidelige applikationerne er over tid.

Der er også en oversigt over, hvor mange maskiner, der er compliant på dette område, og hvor mange der ikke er.

Brug indsigten til at levere så meget værdi som muligt til den enkelte bruger.



Blue Screen of Death:

Stop tidsspilde på grund af blå skærm

Problemet er blevet mindre over årene, ja. Men det er der stadig og giver fortsat anledning til tabt arbejde og tidsspilde.

Når Windows beslutter sig for at lukke ned midt i et Word dokument eller bogføring i Dynamics, kommer det som lyn fra en klar himmel. Og den blå skærm kan nemt koste 15-20 minutter pr. gang.

Kom problemet i forkøbet og minimer antallet af blå skærme. Med APENTO Device Analytics får du indsigt til at gøre noget ved problemet.

Få vist historikken inden for en afgrænset periode. Hvor stort er problemet? Hvilke PC-modeller og versioner er mest sårbare? Hvad er årsagerne?

Vil du vide mere og se løsningen?

Er du interesseret i at høre mere om APENTO Device Analytics, og vil du gerne have en gennemgang af løsningen, er du meget velkommen til at kontakte Endpoint Management Expert Ronni Pedersen.

Udfyld formularen, så vender vi tilbage hurtigst muligt.

Udfyld formular

APENTO ApS
Lyoevej 28
7400 Herning
info@apento.com

APENTO

APENTO er:

- ✓ Microsoft Cloud Solution Partner
- ✓ Microsoft Gold Autorized Education Partner
- ✓ Microsoft Elite Partner (Enterprise Mobility + Identity)

Hos APENTO er vi specialister i Microsoft 365 og Microsoft Azure. Vi har rådgivet om, designet og implementeret løsninger hos nogle af Danmarks største virksomheder.

Vi har nogle af landets dygtigste Microsoft 365 og Azure eksperter - og over 300 Microsoft certificeringer.

En kunde fortæller:

"I en urolig tid med store hackerangreb er det betryggende at vide, at alle sikkerhedsindstillinger er opdateret og konfigureret rigtigt. APENTO Device Analytics giver os konstant indblik i, hvilke maskiner der udgør en sikkerhedsrisiko."

IT-kontorchef Haim Atar,
Koncern IT,
Københavns Kommune

APENTO ApS
Lyoevej 28
7400 Herning
info@apento.com