Komunikace suverénně

Jak přemýšlet o komunikační infrastruktuře státu, veřejného sektoru a velkých českých organizací v době dat, AI a geopolitické nejistoty

Lukáš Přibyl – Head of Presales in IceWarp

VÝZNAM TÉMATU

IceWarp

Komunikace je provozní nervová soustava organizace

E-mail, chat, kalendáře, schůzky, dokumenty, identita a AI dnes tvoří jeden propojený systém.

Výpadek nebo ztráta kontroly neznamená jen nepohodlí — může zastavit rozhodování, koordinaci i reakci na krizové situace.

Komunikační systém obsahuje obsah, metadata, provozní stopy, bezpečnostní logy i historii rozhodování.

Čím důležitější je organizace, tím méně by měla spoléhat pouze na zvyklost nebo tržní dominanci dodavatele.

Která komunikace je pro nás opravdu kritická?

IceWarp

Data jako hodnota: čím skutečně platíme?

Data nejsou vedlejší produkt provozu; jsou ekonomická, bezpečnostní a strategická hodnota.

Hodnotná nejsou jen samotná sdělení, ale také metadata: kdo, kdy, odkud, s kým a nad čím pracuje.

Pokud někdo data využívá, zpracovává nebo z nich odvozuje hodnotu, musí být jasné proč, kde a podle jakých pravidel.

Když jsou data platidlo, musíme vědět, komu a za co platíme.

Kdo z našich dat získává hodnotu — a víme to přesně?

IceWarp

Nemáme povinnost jít s davem

To, že většina organizací používá určitou platformu, neznamená, že je vhodná pro každou agendu.

Standardizace může být výhodná, ale nesmí nahradit bezpečnostní, právní a provozní posouzení.

Pro stát a velké organizace je důležitá schopnost samostatně rozhodnout, ne pouze převzít tržní default.

Správná otázka nezní „co používají ostatní“, ale „co odpovídá našim datům, rizikům a odpovědnosti“.

Nemáme povinnost jít s davem.

Co jsme si jako stát nastavili

Česká regulace už sama říká, že některá data a některé služby vyžadují vyšší opatrnost.

IceWarp

Katalog cloud computingu jako praktický signál

Česká veřejná správa nevybírá cloud pouze podle marketingového tvrzení dodavatele.

Katalog cloud computingu a související požadavky řeší bezpečnostní úrovně, lokalitu zákaznických dat a specifických provozních údajů.

To je důležité: stát už má mechanismus, který říká, že u některých služeb je potřeba vyšší opatrnost.

Otázka zní: používáme tato pravidla skutečně jako nástroj rozhodování?

Pravidla existují. Pracujeme s nimi při architektonických rozhodnutích?

IceWarp

Katalog cloud computingu běží přes Power BI

Vyhledávací nástroj nad katalogem cloud computingu Digitální a informační agentury je veřejně dostupný přes doménu app.powerbi.com.

Věděli jste, že Power BI je v katalogu cloud computingu uvedeno mezi službami Microsoftu zapsanými s výjimkou z požadavku na výlučné uložení zákaznických dat i specifických provozních údajů ve stavu neaktivních dat v EU/ESVO?

Působí to symbolicky: i při debatě o suverenitě a cloudových výjimkách používáme globální platformy jako přirozený nástroj.

Není to problém sám o sobě. Je to dobrý důvod k otázce.

Výjimka není nálepka „špatně“

Výjimka neznamená, že služba je zakázaná nebo automaticky nebezpečná.

Znamená, že u konkrétní služby není splněn standardní požadavek na výlučné uložení určité kategorie dat v EU/ESVO.

Orgán veřejné správy má o této skutečnosti vědět a zahrnout ji do posouzení rizik.

Problém nevzniká samotnou výjimkou, ale tím, když se o ní při rozhodování nemluví.

Je konkrétní agenda kompatibilní s konkrétní výjimkou?

IceWarp

Zákaznická data vs. specifické provozní údaje

Zákaznická data

Obsah, dokumenty, e-maily, záznamy, přílohy, pracovní data a další informace vložené zákazníkem do služby.

Specifické provozní údaje

Logy, auditní stopy, diagnostika, identifikátory, provozní informace, bezpečnostní data a metadata o používání služby.

Praktický dopad

Provozní údaje mohou někdy odhalit víc než samotný dokument: strukturu organizace, chování uživatelů, incidenty a vnitřní procesy.

Chráníme metadata stejně vážně jako obsah?

Vybrané veřejně viditelné příklady

Jmenujme konkrétní příklady, ale používejme je jako důvod pro lepší otázky — ne jako útok.

IceWarp

Microsoft 365: nejpalčivější otázky pro veřejný sektor

Entra ID

Identita je centrální bod přístupu. Výjimky a globální provozní model otevírají otázky kolem lokality a provozních údajů.

Teams

Komunikace, schůzky, přepisy, chaty a metadata mohou být pro stát stejně citlivé jako dokumenty.

SharePoint / Purview / Defender

Dokumenty, compliance, bezpečnostní telemetrie a auditní vrstvy vyžadují přesné pochopení datových toků.

NÚKIB na své stránce uvádí tyto služby Microsoft Ireland Operations Limited, které nesplňují požadavek řádku 1.3 Zákaznická data i řádku 1.4 Specifické provozní údaje

Nestačí vědět, že služba funguje. Víme, kde a jak pracuje s každým typem dat?

Microsoft 365 Copilot: AI jako nová datová vrstva

Copilot-like nástroje nepracují jen s jedním dokumentem, ale s kontextem uživatele, oprávněními a daty z celého prostředí.

Prompty mohou obsahovat interní, osobní, úřední nebo bezpečnostně citlivé informace.

Odpovědi, sumarizace, přepisy, indexy, auditní záznamy a provozní data vytvářejí nové datové vrstvy.

Největším rizikem nemusí být jen přenos mimo EU, ale i to, že AI rychle zviditelní špatně nastavená interní oprávnění.

Máme před zapnutím AI jasno v datech, oprávněních, retenci a odpovědnosti?

GORDIC / GINIS SaaS: otázky pro agendové systémy

Veřejný fakt

NÚKIB uvádí GINIS Standard SaaS a GINIS Enterprise+ SaaS u výjimek řádků 1.3 a 1.4.

Citlivost agend

Agendové systémy mohou obsahovat spisy, dokumenty, workflow, ekonomické údaje a vazby na občany, organizace i úřední procesy.

Správná otázka

Ne zda je služba „špatně“, ale zda konkrétní agenda odpovídá riziku spojenému s výjimkou.

Které agendy si mohou dovolit výjimku — a které už ne?

ALVAO: otázky pro service desk a asset management

Veřejný fakt

NÚKIB uvádí ALVAO Service Desk a ALVAO Asset Management u výjimek řádků 1.3 a 1.4.

Service desk

Tickety mohou obsahovat incidenty, přílohy, screenshoty, popisy chyb, jména uživatelů a citlivé provozní informace.

Asset management

Evidence aktiv může odhalovat zařízení, software, odpovědné osoby, provozní vazby a slabá místa organizace.

Je IT provozní dokumentace méně citlivá než obchodní nebo úřední dokument?

Od datové suverenity k provozní odolnosti

Co když se globální služba, konektivita nebo dodavatelský model naruší?

KRIZOVÝ SCÉNÁŘ

IceWarp

Co když globální služby přestanou fungovat?

Nejde o předpověď. Jde o otázku provozní připravenosti.

Co se stane, když není dostupný e-mail, Teams/Meet, SharePoint/Drive, identita, MFA, AI asistent nebo administrace tenantu?

Má organizace lokální komunikační kanál pro krizové řízení?

Které procesy se zastaví okamžitě a které vydrží několik hodin nebo dní?

Jak dlouho jsme po výpadku „v pohodě“?

IceWarp

Co když se poškodí podmořský kabel?

Moderní cloud stojí na globální konektivitě, směrování, DNS, CDN, identitě a datových tocích mezi regiony.

Poškození významné konektivity nemusí znamenat úplný kolaps internetu, ale může přinést latenci, nedostupnost služeb, omezení kapacity nebo regionální dopady.

Kritická komunikace by měla mít architekturu, která počítá i s degradovaným provozem.

Některé klíčové služby může být vhodné držet lokálně, on-premise nebo alespoň na kontinentu s jasnějším provozním modelem.

Máme plán pro stav, kdy globální konektivita není samozřejmost?

IceWarp

Co se stane s předplatným, když služba není dostupná?

U globálních SaaS platforem platíme za službu, ale v krizi potřebujeme hlavně provozní kontinuitu.

Jak bude řešen výpadek? Jaké SLA platí? Jaké jsou kompenzace — a pomohou nám v reálném provozu?

Máme offline nebo lokální režim pro kritické dokumenty, kontakty, krizové postupy a komunikaci?

Známe RTO/RPO pro komunikaci stejně dobře jako pro datové systémy?

Je finanční kompenzace za výpadek totéž jako schopnost pokračovat?

IceWarp

Neměla by být nejdůležitější data skutečně u nás?

Pro běžnou agendu může být globální cloud rozumný a efektivní.

Pro krizovou komunikaci, bezpečnostní agendy, vedení organizace, právní komunikaci nebo citlivé spisy může být vhodný jiný model.

On-premise, kontrolovaný hosting nebo evropský/lokální dodavatel může snížit závislost na globálním provozním řetězci.

Nejde o ideologii, ale o klasifikaci dat a dopadů.

Která data a komunikace mají být opravdu pod naší kontrolou?

Praktické otázky pro zadavatele

Ne více strachu. Více přesnosti, důkazů a architektonické disciplíny.

CHECKLIST

IceWarp

Otázky, které mají zaznít při výběru řešení

Jaké typy dat služba zpracovává: obsah, metadata, telemetry, support data, AI data?

Kde jsou data uložena at rest a kde jsou reálně zpracovávána?

Kdo k nim může přistupovat — včetně supportu, SOC, subdodavatelů a mateřské struktury?

Je služba zapsaná v katalogu cloud computingu? Je zapsaná s výjimkou?

Jaký je exit plán a kolik dní bychom zvládli bez služby?

Nechceme víc slibů. Chceme lepší otázky.

IceWarp

Co musí být rozhodnuto před zapnutím AI

Které aplikace, týmy a datové typy smí AI používat?

Kde se ukládají prompty, odpovědi, přepisy, sumarizace, auditní logy a případné indexy?

Je smluvně zajištěno, že data nebudou použita k trénování obecného modelu?

Kdo odpovídá za chybné výstupy AI a jejich použití při rozhodování?

Lze AI vypnout, omezit, auditovat a řídit podle citlivosti dat?

AI nezmenšuje potřebu suverenity. AI ji zvyšuje.

EXIT STRATEGIE

IceWarp

Dokážeme odejít?

Suverenita není jen schopnost službu koupit. Je to i schopnost ji nahradit.

Export dat musí být praktický, úplný, čitelný a časově zvládnutelný.

Je potřeba myslet na e-maily, dokumenty, chaty, schůzky, oprávnění, archivy, logy a automatizace.

Bez exit plánu se pohodlná služba může stát dlouhodobou závislostí.

Máme plán B, nebo jen smlouvu A?

ODOLNOST

IceWarp

Jak dlouho jsme po výpadku v pohodě?

Máme definované RTO/RPO pro komunikaci, ne jen pro databáze?

Kdo rozhoduje při výpadku globální služby a jak se k sobě krizový tým dostane?

Jsou kontakty, krizové postupy a klíčové dokumenty dostupné i mimo primární globální platformu?

Máme pravidelně testovaný scénář „bez cloudu“?

Komunikace je často první systém, který v krizi potřebujeme — ne poslední.

Návrat k volbě dodavatele

Volba dodavatele komunikační platformy je strategické rozhodnutí o tom, kdo má skutečnou kontrolu nad našimi daty, metadaty, provozem a schopností zůstat nezávislí i v době nejistoty.

STRATEGICKÁ VOLBA

IceWarp

Globální, evropský, český: vědomá volba podle rizika

Globální platforma může být správná volba pro některé scénáře.

Evropský nebo český dodavatel může být vhodnější tam, kde je důležitá jurisdikce, dostupnost supportu a menší řetězec subdodavatelů.

On-premise nebo kontrolovaný hosting může být lepší volba pro kritickou komunikaci a citlivá data.

Správná architektura může kombinovat různé modely podle rizika agendy.

Nemusíme zvolit jeden model pro všechno.

IceWarp jako možnost: úroveň suverenity podle potřeby

On-premise

Maximální kontrola nad infrastrukturou, lokalitou, backupem, sítí, přístupem a provozními pravidly.

IceWarp Cloud

Cloudová varianta s důrazem na konkrétní lokalitu uložení dat a jednodušší komunikační model.

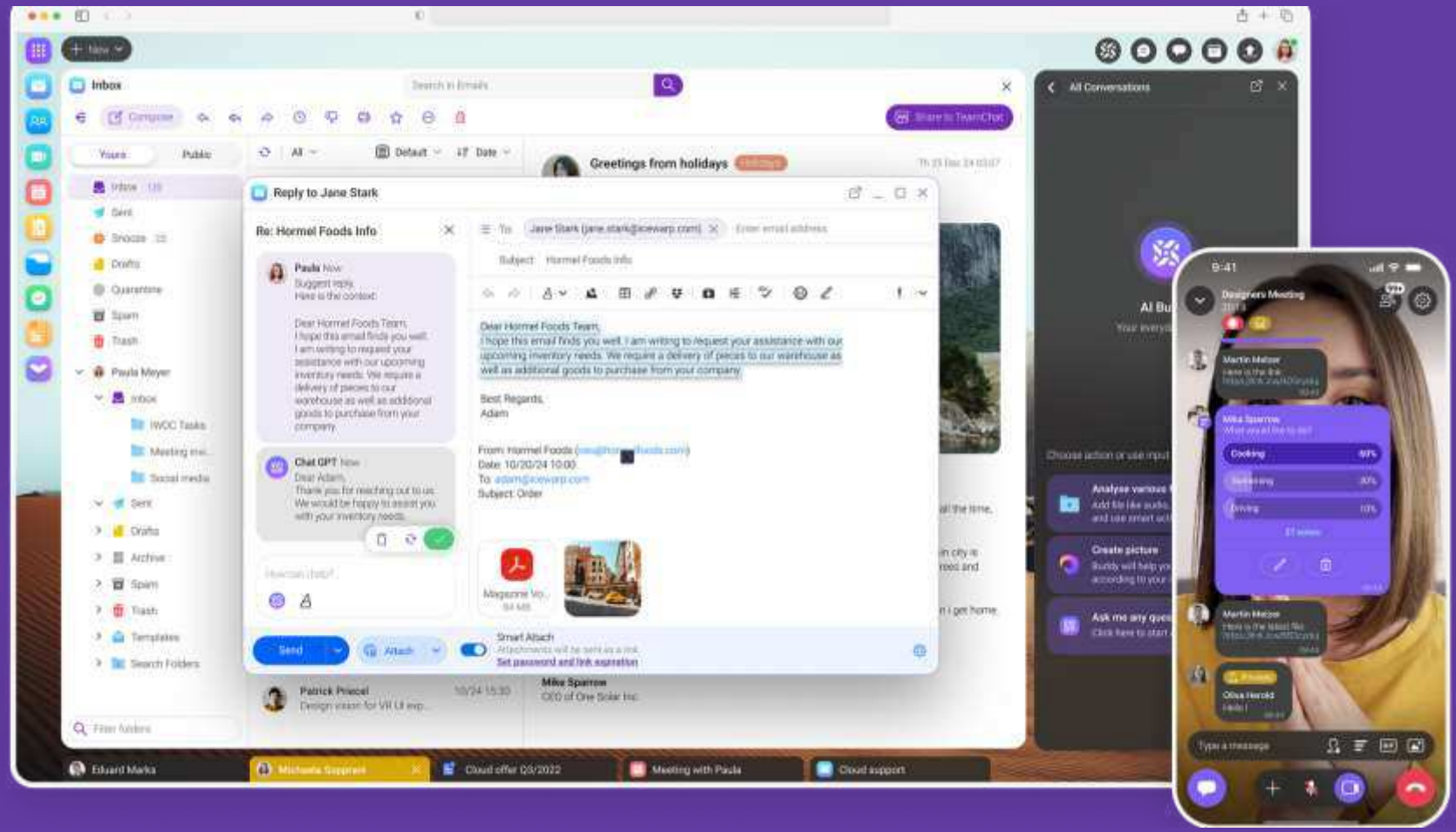
Hybridní přístup

Moderní funkce s možností držet primární data v prostředí zákazníka a cloud používat pro vybrané runtime služby.

Kde je nejvyšší riziko, tam má být nejvyšší kontrola.

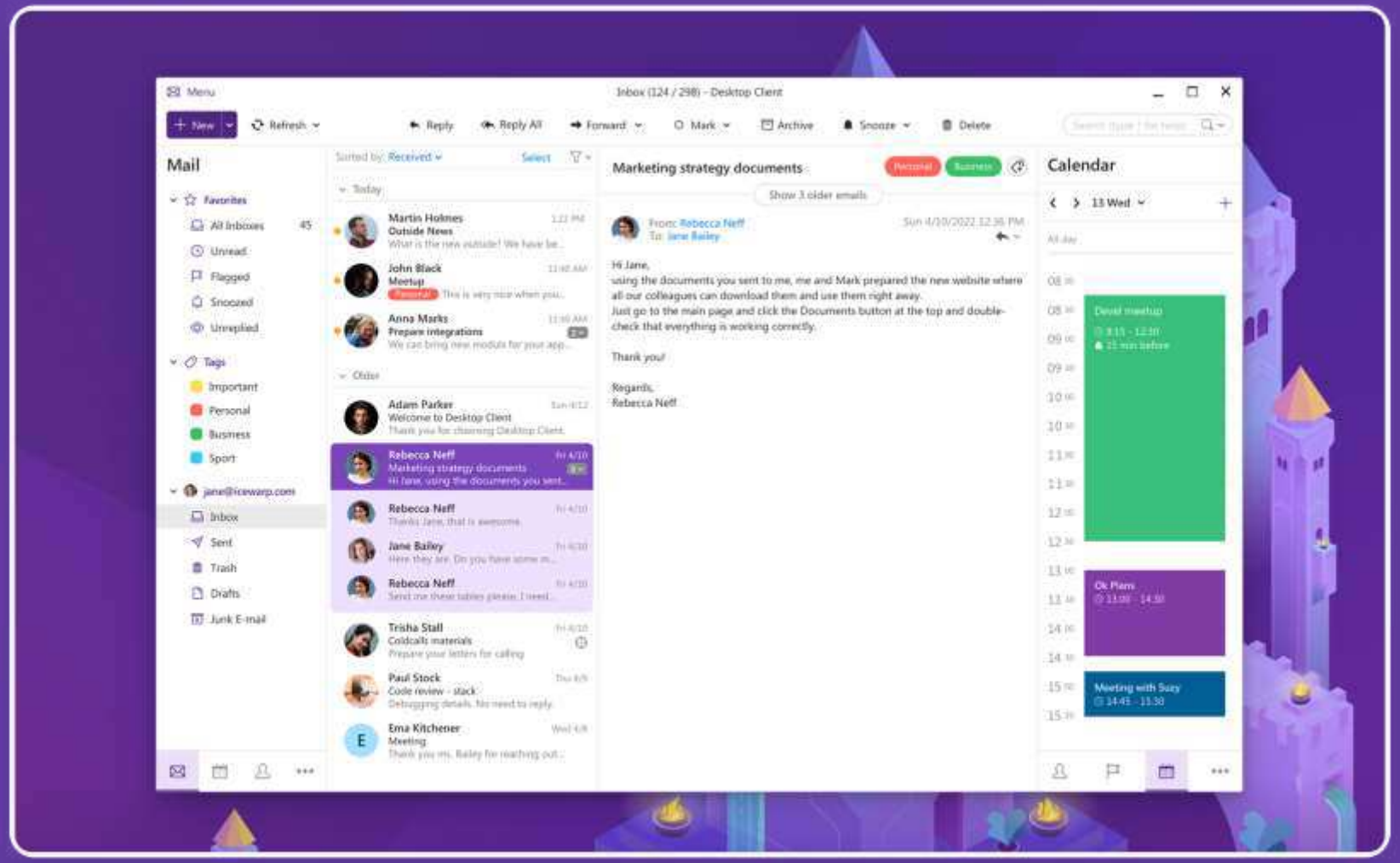
IceWarp

Web Client



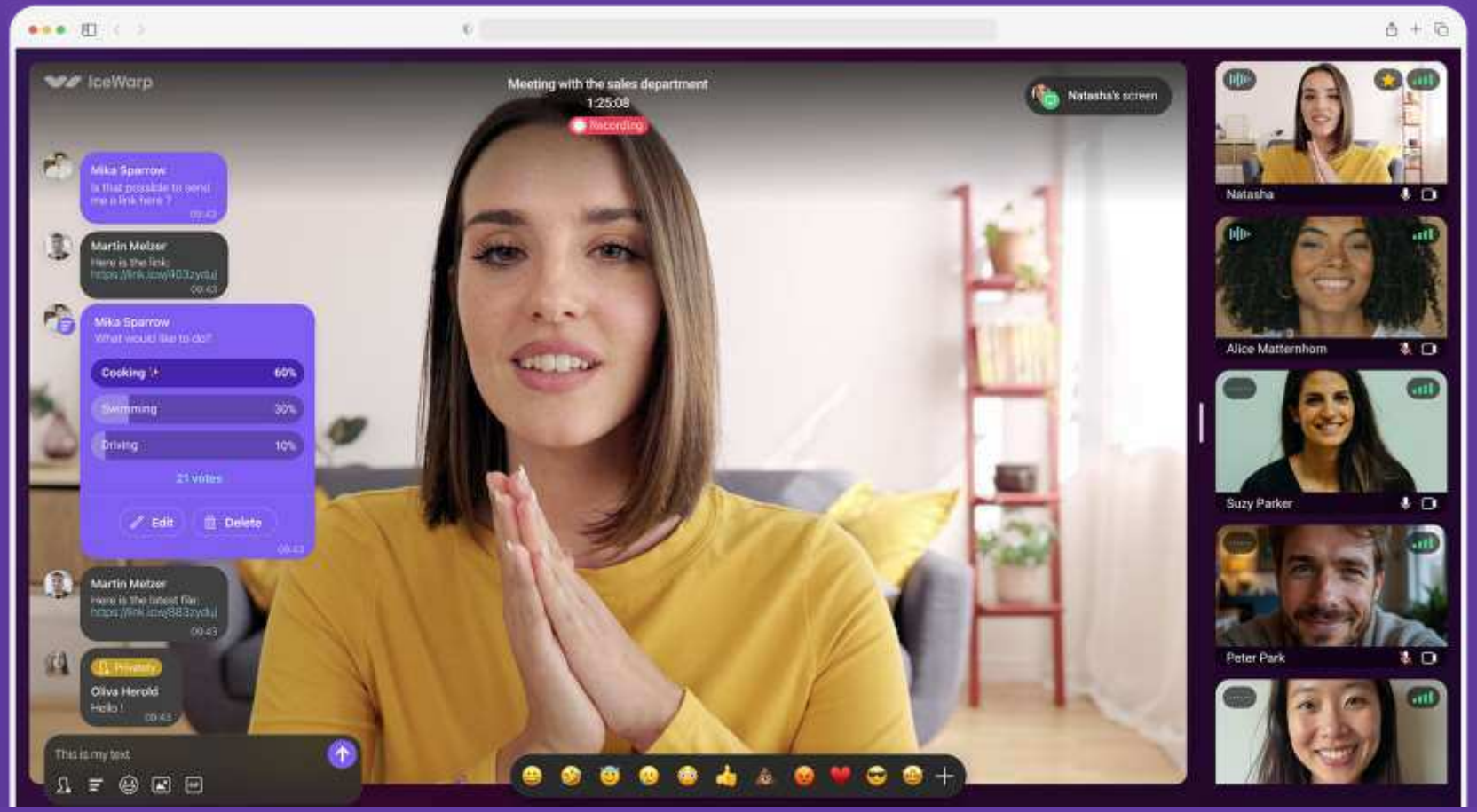
IceWarp

Desktop Client



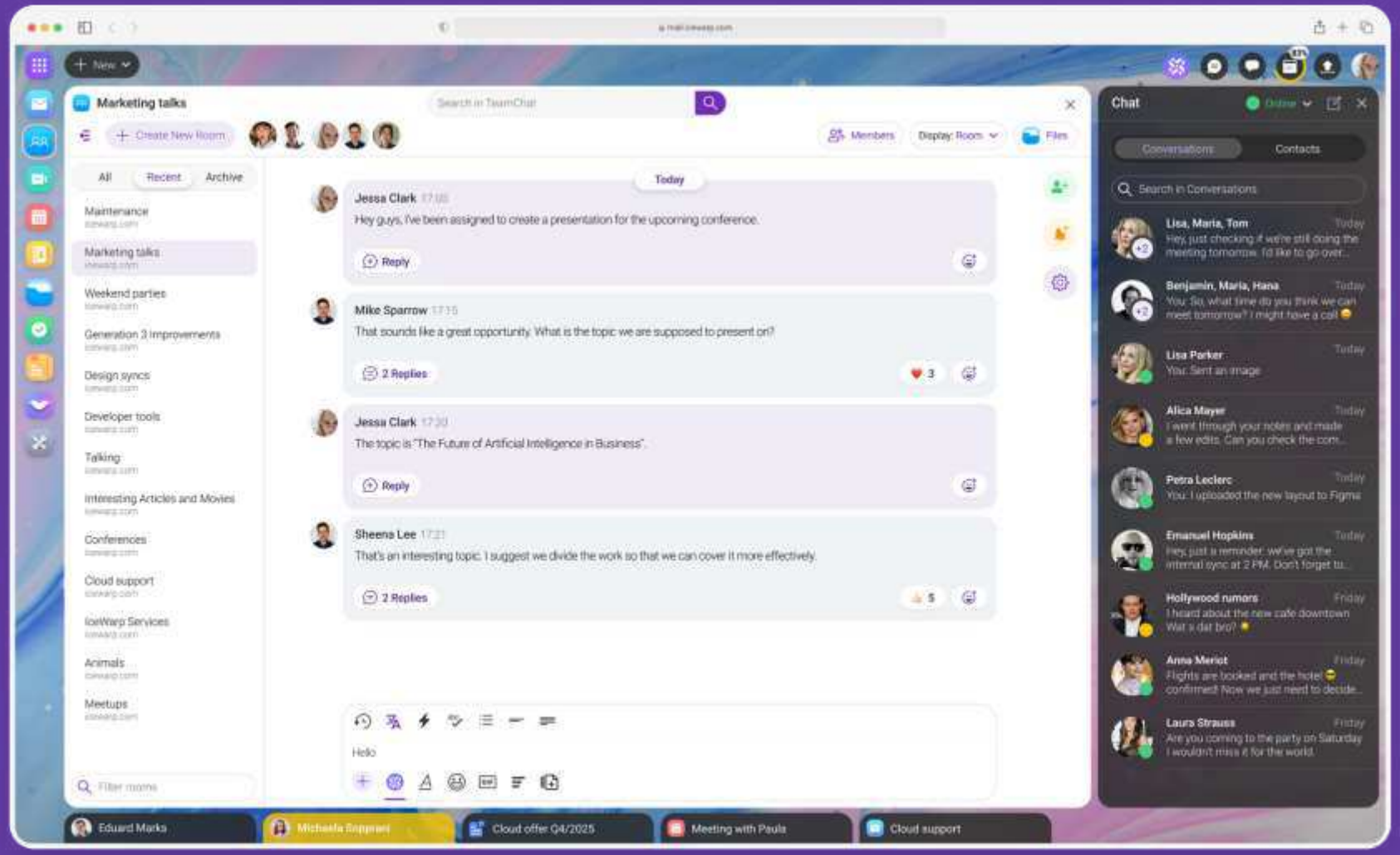
IceWarp

Konference



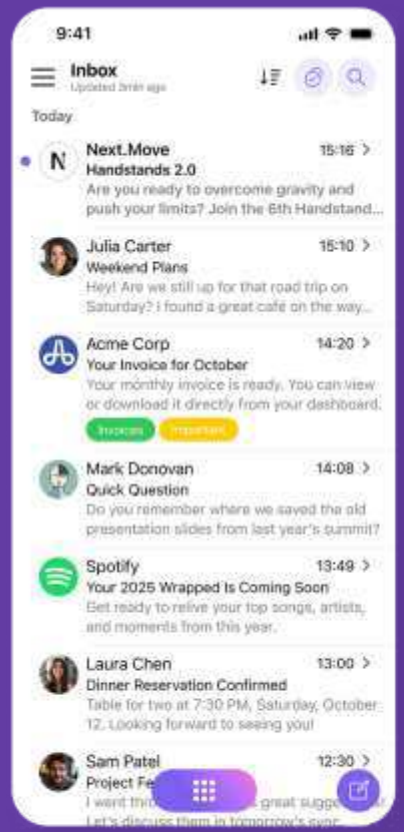
IceWarp

TeamChat



IceWarp

Mobilní aplikace



Email

TeamChat

Konference

Poznámky

STRATEGICKÁ VOLBA

IceWarp

IceWarp v kontextu suverénní komunikace

Prověřená cesta pro veřejný sektor
IceWarp Cloud je zapsán v českém katalogu cloud computingu a IceWarp Cloud je uveden také v katalogu služeb Vládního cloudu SR.

Volba způsobu nasazení podle potřeb zákazníka
Cloud, on-premise, hybridní model i cloudové mikroslužby — od pohodlí cloudu až po maximální kontrolu nad daty v prostředí zákazníka.

Moderní kancelářská a komunikační platforma
E-mail, kalendáře, kontakty, TeamChat, konference, dokumenty, mobilní a desktopové aplikace, včetně práce s dokumenty kompatibilními s Microsoft Office.

Nemusíme zvolit jeden model pro všechno.

Děkuji za pozornost!