Två leverantörer kan se identiska ut vid första anblick. Samma funktionsrutor ikryssade, samma certifikatloggor i sidfoten, liknande språk kring “enterprise grade” säkerhet. När man skalar bort marknadsorden återstår det som bär produkten i drift, dag ut och dag in: hur data skyddas, hur nycklar hanteras, hur snabbt man kan återställa när något brister. I en jämförelse som ofta formuleras som STV vs Mividas, eller Mividas vs STV, blir det snabbt tydligt att skillnaderna visar sig i detaljerna. Och de detaljerna är inte kosmetika, de påverkar reell risk, totalkostnad och handlingsutrymme vid incidenter.

Jag utgår här från vad som faktiskt går att granska och verifiera oberoende av varumärke. Offentlig dokumentation förändras över tid och exakta implementationer kan variera mellan editioner och regionspecifika erbjudanden, så ta detta som en ram för en kvalificerad genomlysning. Där jag skriver STV eller Mividas syftar jag på två typiska plattformsleverantörer av företagskritiska tjänster. I vissa samtal dyker även namnet Mivida upp, ofta som en förkortad benämning på Mividas. Oavsett stavning, det viktiga är att ni begär bevis, inte bara löften.

Varför datasäkerhet avgör valet

En säkerhetsarkitektur som håller i vardagen är byggd för misstag, driftstörningar och antagonister. Den förutsätter att någon någon gång klickar fel, att ett bibliotek får en sårbarhet, att en zon i molnet blir otillgänglig eller att en angripare lyckas få fotfäste på en användares dator. När det sker vill man att skadan begränsas, att data inte kan utnyttjas i klartext och att affären fortsätter efter rimlig återställningstid.

Jag har sett projekt där en snygg funktionslista vägde tyngre än konkreta frågor om RPO och RTO. Allt var lugnt, tills en återställning tog tre dygn och ett kvartals data visade sig sakna applikationskonsistens. Prislappen på den händelsen översteg licenskostnaden för flera år. Därför lägger jag tyngdpunkten på kryptering i vila och i transit, nyckelhantering och backupstrategier, för det är här beslutet STV vs Mividas vinner eller faller.

Snabb lägesbild inför en upphandling

Några skillnader blir ofta utslagsgivande när två alternativ jämförs sida vid sida. Nedan är fem konkreta punkter som jag brukar granska först, eftersom de ger en tidig indikation på leverantörens mognad.

- Krypteringsmodell i vila: stöd för enveloppkryptering, separata tenantnycklar och möjlighet till BYOK eller HYOK med HSM.
- Kryptering i transit: tvingad TLS 1.2+ med moderna AEAD-cipher suites, PFS och mTLS internt mellan mikrotjänster.
- Backup och återställning: dokumenterade RPO- och RTO-intervall, immutabla backups, isolerad återställningsmiljö och bevis på lyckade återläsningstester.
- Loggning och spårbarhet: oföränderliga granskningsloggar, export till kundens SIEM via standarder och tydligt bevarandefönster.
- Juridik och geografi: datalagringsplatser ni kan välja, färdiga DPA:er med SCC, efterlevnad av GDPR art. 32 samt SOC 2 Type II eller ISO 27001 med relevanta kontrollmål.

Om en leverantör snubblar redan här vill jag se en trovärdig färdplan med datum och milstolpar, inte bara ambitioner.

Kryptering i vila som skiljer på kunder och data

Kryptering i vila är bordskunskap, men sättet den implementeras avgör hur mycket ni faktiskt vinner. Jag letar efter enveloppkryptering med separata datanycklar per kund, som i sin tur krypteras med en KMS-styrd huvudnyckel. På så sätt kan man rotera kundens nycklar utan att röra hela datablocket, samtidigt som man får spårbarhet i KMS kring vem som använt vilken nyckel och när.

När BYOK erbjuds, be leverantören förklara hur nycklarna hämtas, cachas, roteras och vad som händer vid förlorad kontakt med kundens KMS. Ett vanligt misstag är att anta att BYOK alltid innebär exklusiv kontroll. I praktiken är det ofta “customer-managed keys” i leverantörens KMS-konto, inte “hold your own key” i ert konto. HYOK med kundägd HSM som aldrig exponerar rå nyckelmaterial ger starkare separationsgaranti, men kan kosta i latens och komplexitet. I en Mividas vs STV-jämförelse bör ni sätta en egen tröskel: om ni verkar i en starkt reglerad miljö kan HYOK vara motiverat, annars är en välkonfigurerad CMK med rigorös åtkomststyrning ofta tillräcklig.

Multitenans är en känslig punkt. Två frågor brukar skilja de starka från de svaga: använder leverantören logisk separation på databasskiktet eller även separat krypteringsnyckel per tenant, och finns det systematiska kontroller som hindrar att en

drifttekniker via konsolen läser kunddata i klartext? Ett bra svar inkluderar break-glass-processer med dual control, session recording och skilda roller mellan driftsättning och dataåtkomst.

Kryptering i transit, inte bara vid externa gränser

TLS är standard, men ordet i sig säger inget om hur robust konfigurationen är. Jag kontrollerar att TLS 1.2 eller 1.3 är tvingad, att äldre protokoll är avstängda, att cipher suites är av typen AEAD, och att man nyttjar PFS för att försvåra retroaktiv dekryptering. Dessutom vill jag se mTLS internt mellan tjänster, särskilt i en mikrotjänstarkitektur. Att bara lita på nätverkssegmentering mellan pods eller containrar har blivit allt mer riskabelt.

För native-klienter, till exempel mobila appar, är certifikatpinning ett extra lager som minskar risken för man in the middle i komprometterade nät. Berätta gärna hur ni hanterar rotering av pins, annars kan en tvingad uppdatering bli er enda utväg vid certifikatbyte.

En modern leverantör erbjuder ofta HTTP/3 över QUIC. Det ger lägre latens i brusiga nät, men återigen är säker konfiguration viktig. Fråga hur de loggar TLS-negotiation och mäter misslyckade handskakningar, för att tidigt upptäcka försök till nedgradering eller aktiv störning.

Nyckelhantering som tål mörka dagar

En KMS utan ordning och reda blir en potentiell single point of failure. Jag begär insyn i följande: var nycklarna praktiskt ligger, hur ofta de roteras, om leverantören använder HSM-baserade root of trust, och om åtkomst kräver split knowledge och dual control. Jag vill se revisionsloggar för KMS-åtgärder, larm vid avvikande mönster och en klar plan för emergency key rotation.

En punkterfarenhet från ett SI-projekt: kundens BYOK-nyckel roterades i deras KMS utan att informera leverantören. Krypteringsoperationer började fallera sporadiskt, men felet syntes först i applikationslagret. Det kostade två dagar att kartlägga. En så enkel sak som automatisk hämtning av aktiv nyckelversion och tydliga larm hade sparat tid och humör.

Åtkomstkontroller och identitet, från gräns till kärna

Säkra plattformar tänker identitet först. SSO via SAML eller OIDC med stöd för SCIM-provisionering borde vara en hygienfaktor. Jag värderar rollbaserad åtkomstkontroll som går att uttrycka granularitet i, helst kompletterad med attributbaserade policies för situationer där rollmatrisen annars exploderar. Step-up MFA för känsliga operationer gör stor nytta, liksom korta tokens med tyst förnyelse och möjlighet att sätta sessionspolicy på klienttyp, nät eller riskpoäng.

Glöm inte tjänst-till-tjänst-behörigheter. En överdriven reliance på delade hemligheter i miljövariabler blir snabbt ett sorgebarn. Federerade arbetsbelastningsidentiteter som kan tilldelas minst nödvändiga rättigheter och roteras utan driftstopp är ett tecken på mognad.

Loggning, spårbarhet och bevisvärde

Granskningsloggar som går att ändra är inte granskningsloggar. Jag ber om teknisk beskrivning av hur loggar skyddas mot modifikation, hur integritet verifieras och hur länge de bevaras. En bra lösning stödjer export i realtid till kundens SIEM med standardprotokoll, har separata loggflöden för åtkomst, systemhändelser och säkerhetsrelevanta incidenter, samt ger möjlighet till kundsökning utan att data lämnar kundens tenantgränser.

En detalj som ofta glöms: loggning av krypteringsoperationer. När, var och av vem en nyckel använts ska synas, helst korrelerat med applikationshändelser. Det är guld värt vid rotorsaksanalyser.

Backupstrategin som fortfarande gäller när allt annat brinner

Backup är inte kopior av filer, backup är en återställningsförmåga. Jag letar efter 3-2-1-1-0-principen i praktiken: minst tre kopior, två olika medietyper eller leverantörer, en offsite, en immutabel eller air-gappad, och noll okända fel efter verifiering. Hur uppnås immutabilitet? WORM-lagring, objektlåsning och versionshantering som inte kan kringgås med adminrättigheter är starka komponenter.

RPO och RTO ska inte bara stå i ett SLA. De måste översättas till verkliga mekanismer: kontinuerlig replikering, punkt-i-tiden-återställning, applikationskonsistenta snapshots, samt testade playbooks. För databaser vill jag se att leverantören

kan koordinera transaktionsloggar, drain av skrivningar och återställning till en definierad tidpunkt. För filer och blobbar är versionshantering med immutabla checkpoints centralt.

Det praktiska skiljer ofta STV och Mividas i en upphandling: den ena kan ha glänsande replikering till flera regioner, men saknar isolerad återställningsmiljö. Den andra kanske STV alternative to Mividas erbjuder “clean room recovery” där man kan spinna upp data och applikation i ett isolat för att validera integritet innan cutover. Den senare ger klar riskreduktion vid ransomware.

Ransomware, immutabilitet och air gap på riktigt

Ransomware mot leverantörens kontrollplan kan slå igenom till kunddata om inte backuperna är immutabla och styrsystemen separerade. Jag frågar hur de hindrar att privilegierade konton raderar backupversioner i panik eller under tvång. Svar som innehåller tidslåsta objekt, godkännandekedjor och separata admin-domäner inger mer förtroende än en allmän försäkran om “rollbaserad åtkomst”.

En bra metod är att ha en “break glass recovery” som går via oberoende inloggningsvägar och kräver två separata bekräftelser från olika personroller. Återställning i en ren environment, utan utgående nätåtkomst tills verifieringar passerat, minskar risken att återinfektera system.

Dataresidens, exportkontroller och bevisbar efterlevnad

Frågan om var data ligger och under vilken jurisdiktion den faller är inte längre en fotnot. GDPR art. 32 kräver lämpliga skydd, och Schrems II gör att överföringar till tredje land behöver stöd i SCC, TIA och kompletterande tekniska skydd. Välj en leverantör som kan placera er data i regioner ni godkänner, visa standardavtalsklausuler och beskriva tekniska åtgärder som minskar åtkomstmöjligheten för obehöriga, även i händelse av myndighetsförfrågningar.

Certifieringar är inte allt, men de hjälper. SOC 2 Type II ger en bild av kontroller i drift över tid, ISO 27001 visar ledningssystem och kontroller, och ISO 27017/27018 lägger till moln och persondata. Be att få se rapporternas omfattning. Jag har stött på SOC 2-rapporter där krypteringskontrollen fanns med, men backupdelen låg utanför scope. Det är inte fel i sig, men då krävs andra bevis för den delen.

Prestanda, latens och de tekniska kompromisserna

Säkerhet kostar resurser, och det är helt i sin ordning. Det som spelar roll är om kostnaden är förutsägbar och hanterlig. Kryptering i applikationslagret, till exempel klient-sidig kryptering med kundnycklar, kan addera 5 till 20 millisekunder per operation och påverka indexering eller sökning. I vissa fall krävs formatbevarande kryptering eller tokenisering för att behålla funktionalitet, men det gör nyckelhanteringsfrågan ännu viktigare.

I nätlagret gäller att tvingad TLS 1.3 med PFS ibland slår mot legacyklienter. Har leverantören en plan för gradvis utfasning och övervakning av misslyckade handskakningar, slipper ni överraskningar. Komprimering före kryptering är en välkänd risk, så säker konfiguration bör undvika kombinationer som öppnar för CRIME/BREACH-liknande attacker.

Kostnadspunkter att inte missa

Total ägandekostnad för säkerhet dyker upp på oväntade ställen. KMS-anrop kan prissättas per operation, och i en chattig mikrotjänstmiljö kan det bli många. HSM som tjänst kostar mer, men ger ofta bättre bevisvärde. Objektlagring med versionering och immutabilitet för backuper kan dubbla eller tredubbla lagringsnotan om retentionen sätts brett. Bandbredd för replikering mellan regioner är inte gratis, och teståterställningar kostar i compute och lagring under testfönstret.

Räkna också med kostnad för att hålla en isolerad återställningsmiljö redo. Den behöver inte vara varm, men en definierad mall med IaC, image-hygien och regelbundna provstarter undviker brandkårsutryckningar. När du står mellan STV och Mividas, be vardera part bryta ner den här kostnadsbilden. De som gjort hemläxan kan visa staplar per månad vid givna RPO/RTO-nivåer.

En praktisk modell för STV vs Mividas

När tekniska dokument är lika välskrivna gäller det att göra jämförelsen konkret. Välj två till tre datakritiska flöden och kör dem genom leverantörernas säkerhets- och backupmodell. Exempelvis, ett orderflöde som skriver till en

transaktionsdatabas, lägger filer i objektlagring, och skickar notifieringar till klienter. För varje steg, fråga efter exakt var kryptering sker, vilken nyckel som används, hur rotation påverkar, hur återläsning går till på minutnivå och vilka bevis som finns från senaste kvartalet.

Be om att få följa en återställning, från att ni rapporterar incidenten till att data är kontrollerat och tillgängligt. Titta på hur automatiserade steg är, var manuella moment finns och hur loggarna samlas upp. Här finns ofta den största praktiska skillnaden mellan leverantörer som på pappret ser identiska ut. Den ena visar ett filmat övningsscenario på 45 minuter inklusive validering, den andra skickar en PowerPoint.

Due diligence, punkt för punkt

Det hjälper med en koncentrerad checklista när detaljerna blir många. Använd följande fem punkter som miniminivå i er granskning av STV respektive Mividas.

- Begär teknisk beskrivning av kryptering i vila och transit, inklusive cipher suites, nyckelhierarki, rotationsintervall och mTLS-strategi mellan interna tjänster.
- Verifiera nyckelhanteringen i praktiken: HSM-ankare, BYOK/HYOK-flöden, åtkomstloggar för KMS samt test av nyckelrotation utan driftstopp.
- Inspektera backup- och återställningsprocedurer, med protokoll från senaste återläsningstestet, mål för RPO/RTO, immutabilitet och isolerad recovery-miljö.
- Gå igenom juridik och geografi: DPA med SCC, regionval, register över underbiträden, och bevis på kontroller enligt SOC 2 Type II eller ISO 27001 där backup och kryptering ingår i scope.
- Kör ett liveprov: simulera ett fel och mät tid till detektion, tid till isolering, tid till återställning och kvalitetssäkring av data.

Om en leverantör svarar med generella utsagor snarare än artefakter, planera in ett tekniskt arbetsmöte. Det sparar diskussioner senare.

Fallgropar jag ofta ser

Ett klassiskt misstag är att förlita sig på replikerad lagring som om den vore backup. Replikering flyttar även korruption och raderingar. En annan fälla är att tro att dagliga snapshots räcker. Utan applikationskonsistens kan återställning av en databas från snapshot bli en frustration, med långa recovery-tider och risk för dataförlust mellan snapshot och senaste transaktionslogg.

Jag har också sett implementeringar där klient-sidig kryptering valts av principiella skäl, men där nyckelrotation krävde full återkryptering av terabytes av data. Det blev dyrt, långsamt och operationaliserades aldrig. Att väga tekniska ideal mot driftsverklighet är en del av säkerhetsarbetet.

Ett tredje exempel: SIEM-integration som bara skickade summerade händelser. Vid en incident räckte det inte, för analysen behövde rådata. Det borde varit en enkel fråga att ställa i upphandlingen: kan vi streama rå loggdata i nära

realtid, hur länge lagras den hos leverantören och kan vi bevara integritetskedjan vid export?

Att dokumentera beslutet så att det håller över tid

När ni väljer mellan två alternativ, till exempel STV och Mividas, skriv ner beslutet i form av krav som är testbara. Lägg in en bilaga till avtalet som beskriver krypteringsmodellen, nyckelhantering, backupmål och testfrekvens. Etablera en gemensam testkalender med kvartalsvisa återläsningsövningar, och krav på rapportering av utfall. Säkerställ att undantag och temporära lösningar har deadlines och konsekvenser.

Definiera tydliga notifieringsvägar vid incidenter, inklusive hur leverantören ger er tillgång till forensiskt material. Be att få se deras interna RACI för säkerhetsrelaterade incidenter. När roller och ansvar tydliggörs före krisen, går timmarna åt till återställning istället för förhandling.

Ett råd på vägen

Det är lockande att jaga alla funktioner samtidigt. Jag har märkt att tre saker förflyttar riskbilden mest för pengarna: ordentlig nyckelhantering med spårbarhet, immutabla backuper med regelbundna återläsningar, och mTLS i hela tjänstlandskapet. Får ni de tre på plats, blir övriga kontroller lättare att luta mot. De blir också mätbara på ett sätt som märks i revisioner.

När valet står mellan två likvärdiga alternativ, använd verkliga arbetsflöden som lakmustest. Låt leverantörerna visa hur de hanterar ett driftstopp, en felaktig deployment eller en ransomware-simulering. Följ pengarna för KMS, backupretention och nätuttrafik. Och kom ihåg att datasäkerhet inte avgörs av logotyper. Den avgörs av hur väl en leverantör kan visa, inte bara säga, att skydden fungerar när STV vs Mividas det gäller.