

• כיצד ספק שירותי ענן מגן על המידע הארגוני? מהו זמן שחזור המידע אליו הספק מתחייב? האם הספק מבצע בדיקות שחזורים תקופתיות? מהי תדירות הגיבוי? האם המידע נפרס במתקנים שונים? האם ישנה אופציה לקבלת העתק של המידע באופן קבוע במתקן הלקוח?  
• האם התשתית כוללת גנרטורים בגיבוי, מערכות גיבוי לחשמל, התראה על כשלים, המערכת החשמל, מיזוג, כיבוי אש והאם המתקן מאובטח כראוי?

בתעשייה? האם כלקוח אוכל לראות את הרמת הביצועים של המערכות בכל רגע נתון?  
• על בסיס איזה תשתית חומרה ותוכנה מפעיל ספק הענן את המערכות? האם מדובר במערכות של היצרנים המובילים בעולם? מהי רמת השרידות וזמינות המערכות שמציע הספק?  
• כיצד הספק מפריד בין לקוחות? כיצד הוא מאבטח את המידע? האם ניתן להצפין נתונים? האם הלקוח נדרש לאפשר לספק גישה למערכות המחשוב?

שיטות עבודה קיימות?  
• האם הספק מתחייב לסייע במידה והלקוח רוצה להוציא את המערכות מפתרון הענן? מהו תהליך היציאה מהענן והאם ישנה התחייבות של הספק ללוחות זמנים ליציאה מהענן.  
• מהו הרמת השירות שספק הענן מציע? האם הספק מתחייב לזמינות המערכות? מהו מנגנון הפיצוי שמציע הספק במקרה של תקלה בתשתית?  
• האם הספק מתחייב לרמת ביצועים בהתאם לזמני התגובה המקובלים

## מיתוסים בנוגע למחשוב ענן

גם אם ספק מחשוב הענן נדרש על ידי הנהלת החברה לספק פתרון מלא שכולל את האמור לעיל, נדרשת אותה מצבת כוח אדם על מנת לבצע תחזוקה ראויה למערכות.

### המידע בענן לא מאובטח

רוב הלקוחות חושבים שהמידע בענן אינו מאובטח וכיון שמדובר בתשתית משותפת, שירותי הענן חשופים יותר מתשתית מקומית לאירועי אבטחת מידע.

ספק ענן רציני משקיע הרבה זמן וכסף בהקמת מערכות אבטחת מידע מתאימות עבור מחשוב ענן. אלו מערכות יקרות מאוד, כאלה שלקוח לא היה מוכן או מסוגל להקים ברשת המקומית.

אבטחת המידע מתחלקת לשני תחומים חשובים:

אבטחת המידע - כיצד ספק הענן מאבטח את המידע ומפריד בין לקוח ללקוח. לרוב מדובר בהפרדה פיזית בתשתית התקשורת בגישה למתקן, הצפנת תשתית התקשורת, הצפנת נתונים והפעלה של מערכות בקרת אירועי אבטחת מידע, שמאפשרת לספק שירותי הענן וללקוח לקבל התראות בזמן אמת. כאשר מתבצע משהו שאינו תואם את מדיניות אבטחת המידע של הספק או הלקוח. למשל, חשיפה של דיסק של שרת וירטואלי אחד לאחר.

זמינות מידע - היבט לא פחות חשוב מאבטחת המידע היא זמינות המידע הארגוני בענן. לרוב הענן נתפס כתשתית ברמת זמינות נמוכה יותר. ההפך הוא הנכון. פתרון מחשוב ענן מתאים מספק רמת זמינות גבוהה יותר ע"י שכפול המידע למספר מתקנים שונים. ספק שירותי ענן מאפשר שחזור מהיר של נתונים ללא מגבלת נפח השחזור, ומספק עשרות נקודות זמן של המידע לשחזור. ספק שירותי ענן מבצע בדיקת גיבויים מקיפה יותר ובתדירות גבוהה יותר מכל מערכת מידע ברשת מקומית.

חשוב לזכור שספק הענן חשוף לתביעות ולכן משקיע מאמץ וזמן רב ביישום פתרון המגן על המידע ומאבטח אותו כראוי.

### חסכון כספי

רוב הלקוחות סבורים שמטרת הענן היא לחסוך כסף לארגון או לחילופין, שהמעבר לענן יקר יותר מהפעלה של מערכות המידע בתוך הארגון.

ברור שיש לבדוק כל מקרה לגופו, אך ברוב המקרים ספק שירותי ענן מודע להיבט העלויות ועושה מאמצים רבים על מנת להוזיל את עלות הפתרון ללקוח.

פתרון מחשוב ענן לא צריך להיות זול יותר, ויתכן שעלויותיו זהות. אך פתרון הענן מספק תועלות נוספות כגון תשלום חודשי קבוע לאורך התקופה במקום מדרגות השקעה משמעותיות. כל מנהל כספים מעדיף תשלום חודשי קבוע ויודע.

שירותי ענן מספקים רמת זמינות גבוהה יותר של המערכות והמידע הארגוני ותועלות נוספות שאינן מדידות באופן ישיר אך חשובות לכל חברה.

### ביצועים

כשחושבים על מחשוב ענן, לרוב עולה תמונה של קו תקשורת איטי וחווית משתמש גרועה. ההפך הוא הנכון: שירותי ענן מסתמכים על קו תקשורת מהיר שמספק חווית משתמש ברמה של רשת מקומית. ספקי הענן מבינים כי חווית המשתמש היא פרמטר קריטי בהצלחת הפתרון, ולכן משקיעים משאבים רבים בהפעלת מנגנונים להבטחת ביצועים, איזון עומסים, ואינם משתפים מערכות באופן שפוגע במשתמשי המערכת.

### הולכים לפטר אותי

אחד החסמים במעבר לענן הוא מנהל הרשת או מנהל מערכות המידע החושש למשלתו. פתרון הענן אינו מוביל לפיטורים, הרי מישהו עדיין צריך לנהל את הפעילות מול ספק הענן (מנהל מערכות המידע), לתפעל את מערכות ההפעלה והאפליקציות (מנהל הרשת) ולספק תמיכה למשתמשי הקצה (אנשי תמיכה).