

## IBM Security Verify

Στην παρούσα Περιγραφή Υπηρεσιών παρέχεται μια περιγραφή της Υπηρεσίας Cloud. Στα αντίστοιχα έγγραφα παραγγελίας παρέχονται πληροφορίες τιμολόγησης και πρόσθετες λεπτομέρειες σχετικά με την παραγγελία του Πελάτη.

### 1. Υπηρεσία Cloud

Το IBM Cloud Identity παρέχει ενιαία σύνδεση (Single Sign-On - SSO), ταυτοποίηση πολλαπλών παραγόντων και στοιχεία ελέγχου κύκλου ζωής για τους διάφορους τύπους εσωτερικών (υπάλληλοι) και εξωτερικών χρηστών.

#### 1.1 Προσφορές

Ο Πελάτης μπορεί να επιλέξει από τις ακόλουθες διαθέσιμες προσφορές.

##### 1.1.1 IBM Security Verify

Το IBM Security Verify βοηθά τον Πελάτη να διασφαλίσει την παραγωγικότητα των χρηστών συνδυάζοντας σε μια κοινή προσφορά παρεχόμενες σε περιβάλλον νέφους (cloud) λειτουργίες ενιαίας σύνδεσης, ταυτοποίησης πολλαπλών παραγόντων, διαχείρισης κύκλου ζωής, προσαρμοζόμενης πρόσβασης, ανάλυσης δεδομένων ταυτοτήτων και διακυβέρνησης ταυτοτήτων. Αυτή η Υπηρεσία Cloud υποστηρίζει επίσης χιλιάδες έτοιμες λειτουργίες σύνδεσης και πρότυπα που επιτρέπουν την πρόσβαση σε δημοφιλείς εφαρμογές υπηρεσιών cloud και την ενοποίηση εσωτερικών εφαρμογών.

- **Ενιαία Σύνδεση (Single Sign-On)**

Αυτή η Υπηρεσία Cloud παρέχει Ενιαία Σύνδεση (SSO) και Open ID Connect (OIDC), Ταυτοποίηση ως Υπηρεσία για εξουσιοδότηση βασιζόμενων στο cloud API, μια πλατφόρμα εκκίνησης εφαρμογών, λειτουργίες αναφορών διαχείρισης και ένα χειριστήριο ανάλυσης. Αυτή η Υπηρεσία Cloud συνδέει τους χρήστες στις εφαρμογές χρησιμοποιώντας πρωτόκολλα ταυτοποίησης και ενοποίησης που βασίζονται σε σύγχρονα πρότυπα, συμπεριλαμβανομένων εκατοντάδων λειτουργιών σύνδεσης σε κοινές εφαρμογές. Αυτή η Υπηρεσία Cloud ενοποιείται πλήρως με τα τοπικά εγκαθιστώμενα προγράμματα λογισμικού IBM Security Verify Access και IBM Security Verify Application Gateway, τα οποία συμπεριλαμβάνονται ως λογισμικό ενεργοποίησης, παρέχοντας μια λύση για την υποστήριξη των επιχειρηματικών απαιτήσεων του Πελάτη για τη διαχείριση της πρόσβασης τόσο στις τοπικά εγκατεστημένες εφαρμογές όσο και στις εφαρμογές στο cloud.

- **Ταυτοποίηση Πολλαπλών Παραγόντων (Multi-Factor Authentication)**

Αυτή η Υπηρεσία Cloud παρέχει ταυτοποίηση πολλαπλών παραγόντων για εφαρμογές που προστατεύονται από το Cloud Identity Connect ή μέσω της άμεσης κλίσης API καθώς και για άλλα σημεία επιβεβλημένης εφαρμογής, συμπεριλαμβανομένων πελατών RADIUS, εξυπηρετητών Unix/Linux PAM και εξυπηρετητών Windows, με σκοπό την επαλήθευση της ταυτότητας τους κατά την πρόσβαση σε μια ψηφιακή υπηρεσία. Περιλαμβάνει μηχανισμούς όπως e-mail, SMS και κωδικούς πρόσβασης μίας χρήσης περιορισμένης χρονικής ισχύος (διακριτικά λογισμικού) και ταυτοποίηση βιομετρικών στοιχείων μέσω κινητών συσκευών που βασίζονται στο IBM Verify. Αυτή η Υπηρεσία Cloud ενοποιείται με το τοπικά εγκαθιστώμενο πρόγραμμα λογισμικού IBM Security Verify Access παρέχοντας μια λύση για την υποστήριξη των επιχειρηματικών απαιτήσεων του Πελάτη για τη διαχείριση της πρόσβασης τόσο στις τοπικά εγκατεστημένες εφαρμογές όσο και στις εφαρμογές στο cloud.

- **Προσαρμοζόμενη Πρόσβαση (Adaptive Access)**

Αυτή η Υπηρεσία Cloud χρησιμοποιεί έναν συνδυασμό εργαλείων ανάλυσης απειλών και τεχνητής νοημοσύνης που βοηθά τους οργανισμούς να διαχωρίζουν τους κακόβουλους από τους πραγματικούς χρήστες κατά την προσπάθεια πρόσβασης των χρηστών στις εφαρμογές που προστατεύονται από την υπηρεσία. Αυτή η υπηρεσία επεξεργάζεται πληροφορίες για τους χρήστες, τις συσκευές τους και τα μοτίβα συμπεριφοράς με σκοπό την επιλογή σε πραγματικό χρόνο της κατάλληλης ενέργειας περιορισμού κινδύνου (άδεια πρόσβασης, επιβολή ταυτοποίησης ή αποκλεισμός πρόσβασης). Η υπηρεσία χρησιμοποιεί εκατοντάδες σημεία δεδομένων και περιρρέουσες πληροφορίες από τη συσκευή ενός τελικού χρήστη για να προσδιορίσει τη συσκευή και να υπολογίσει ένα ολιστικό επίπεδο κινδύνου για τη συνεδρία. Οι οριζόμενοι στην πολιτική

πρόσβασης κανόνες πρόσβασης βάσει κινδύνου χρησιμοποιούνται στη συνέχεια για τον καθορισμό της ενέργειας του συστήματος. Αυτή η υπηρεσία συνδέεται στενά με τις αναφορές διαχείρισης του Security Verify, τον επεξεργαστή κανόνων πολιτικής πρόσβασης και την υπηρεσία ταυτοποίησης πολλαπλών παραγόντων.

- Διαχείριση Κύκλου Ζωής και Διακυβέρνηση (Lifecycle Management and Governance)

Αυτή η Υπηρεσία Cloud ενοποιείται πλήρως με τα τοπικά εγκαθιστώμενα προγράμματα λογισμικού IBM Security Identity Governance and Intelligence (IGI) και IBM Security Identity Manager (ISIM), τα οποία συμπεριλαμβάνονται ως λογισμικό ενεργοποίησης, παρέχοντας μια λύση για την υποστήριξη των επιχειρηματικών απαιτήσεων του Πελάτη για τη διακυβέρνηση ταυτοτήτων τόσο στις τοπικά εγκατεστημένες εφαρμογές όσο και στις εφαρμογές στο cloud. Αυτή η Υπηρεσία Cloud παρέχει στους οργανισμούς προηγμένες λειτουργίες διαχείρισης κύκλου ζωής ταυτοτήτων στο cloud. Στις παρεχόμενες λειτουργίες περιλαμβάνονται ο συγχρονισμός λογαριασμών, η ροή εργασιών αίτησης πρόσβασης σε εφαρμογές, η πιστοποίηση πρόσβασης και η παροχή πληροφοριών στις εφαρμογές στο τοπικό περιβάλλον και στο cloud. Οι πελάτες μπορούν να συμπεριλάβουν το IBM Security Verify Account Synchronization ως πρόσθετη υπηρεσία.

- Ανάλυση (Analytics)

Αυτή η Υπηρεσία Cloud ενισχύει υπάρχουσες λύσεις της IBM, όπως οι IBM Security Identity Governance and Intelligence (IGI) και IBM Security Identity Manager (ISIM), για να παρέχει ένα ολιστικό προφίλ κινδύνου των διαχειριζόμενων χρηστών. Αυτή η Υπηρεσία Cloud περιλαμβάνει έναν τοπικό μηχανισμό ανάλυσης πολλαπλών χρήσεων που επεξεργάζεται δεδομένα δραστηριοτήτων και δικαιωμάτων χρήσης από διάφορες πηγές, οι οποίες παρέχουν προβολή 360 μοιρών των κινδύνων πρόσβασης και δυνατότητα ανάληψης ενεργειών με βάση αυτές τις τεκμηριωμένες πληροφορίες κινδύνου.

### 1.1.2 IBM Cloud Identity Connect

Αυτή η Υπηρεσία Cloud παρέχει Ενιαία Σύνδεση (SSO) και Open ID Connect (OIDC), Ταυτοποίηση ως Υπηρεσία για εξουσιοδότηση βασιζόμενων στο cloud API, μια πλατφόρμα εκκίνησης εφαρμογών, λειτουργίες αναφορών διαχείρισης και ένα χειριστήριο ανάλυσης. Αυτή η Υπηρεσία Cloud συνδέει τους χρήστες στις εφαρμογές χρησιμοποιώντας πρωτόκολλα ταυτοποίησης και ενοποίησης που βασίζονται σε σύγχρονα πρότυπα, συμπεριλαμβανομένων εκατοντάδων λειτουργιών σύνδεσης σε κοινές εφαρμογές. Αυτή η Υπηρεσία Cloud αποτελεί ένα ενιαίο περιβάλλον με το τοπικά εγκαθιστώμενο πρόγραμμα λογισμικού IBM Security Access Management (ISAM), το οποίο περιλαμβάνεται ως λογισμικό ενεργοποίησης, και παρέχει μια λύση για την υποστήριξη των επιχειρηματικών απαιτήσεων του Πελάτη για τη διαχείριση της πρόσβασης τόσο στις τοπικά εγκατεστημένες εφαρμογές όσο και στις εφαρμογές στο cloud.

### 1.1.3 IBM Cloud Identity Connect for ISAM

Αυτή η Υπηρεσία Cloud αποτελεί ένα ενιαίο περιβάλλον με το τοπικά εγκαθιστώμενο πρόγραμμα λογισμικού IBM Security Access Management (ISAM) και παρέχει μια λύση για την υποστήριξη των επιχειρηματικών απαιτήσεων του Πελάτη για τη διαχείριση της πρόσβασης τόσο στις τοπικά εγκατεστημένες εφαρμογές όσο και στις εφαρμογές στο cloud. Για τη χρήση αυτής της Υπηρεσίας Cloud, ο Πελάτης πρέπει να διαθέτει ένα ενεργό δικαίωμα Συνδρομής και Υποστήριξης Λογισμικού (S&S) για το πρόγραμμα IBM Security Access Management (ISAM) και η συνδρομή S&S πρέπει να παραμείνει ενεργή καθ' όλη τη διάρκεια της περιόδου συνδρομής του Πελάτη για την Υπηρεσία Cloud. Το δικαίωμα χρήσης του Πελάτη για αυτή την Υπηρεσία Cloud πρέπει να είναι ισοδύναμο με το δικαίωμα άδειας χρήσης του ISAM στο τοπικό περιβάλλον του Πελάτη. Η διακοπή της συνδρομής S&S του Πελάτη θα έχει ως αποτέλεσμα τη διακοπή της Υπηρεσίας Cloud. Σε αυτή την Υπηρεσία Cloud δεν περιλαμβάνεται πρόσβαση στο λογισμικό ενεργοποίησης που ορίζεται στο Άρθρο 5.2.

### 1.1.4 IBM Cloud Identity Essentials

Αυτή η Υπηρεσία Cloud παρέχει στον Πελάτη τη δυνατότητα ενιαίας σύνδεσης (SSO) στις εφαρμογές cloud της IBM και στις δημόσιες εφαρμογές cloud που χρησιμοποιεί. Αυτή η Υπηρεσία Cloud μπορεί να συνδυαστεί με το IBM MaaS360 για την παροχή πρόσθετων επιπέδων ελέγχου ασφάλειας, όπως π.χ. η πρόσβαση υπό όρους (conditional access).

### 1.1.5 IBM Cloud Identity Verify

Αυτή η Υπηρεσία Cloud παρέχει ταυτοποίηση πολλαπλών παραγόντων για εφαρμογές που προστατεύονται από το Cloud Identity Connect ή μέσω της άμεσης κλίσης API καθώς και για άλλα σημεία επιβεβλημένης εφαρμογής, συμπεριλαμβανομένων πελατών RADIUS, εξυπηρετητών Unix/Linux PAM και εξυπηρετητών Windows, με σκοπό την επαλήθευση της ταυτότητας τους κατά την πρόσβαση σε μια ψηφιακή υπηρεσία. Περιλαμβάνει μηχανισμούς όπως e-mail, SMS και κωδικούς πρόσβασης μίας χρήσης περιορισμένης χρονικής ισχύος (διακριτικά λογισμικού) και ταυτοποίηση βιομετρικών στοιχείων μέσω κινητών συσκευών που βασίζονται στο IBM Verify. Αυτή η Υπηρεσία Cloud αποτελεί ένα ενιαίο περιβάλλον με το τοπικά εγκαθιστώμενο πρόγραμμα λογισμικού IBM Security Access Management (ISAM) και παρέχει μια λύση για την υποστήριξη των επιχειρηματικών απαιτήσεων του Πελάτη για τη διαχείριση της πρόσβασης τόσο στις τοπικά εγκατεστημένες εφαρμογές όσο και στις εφαρμογές στο cloud. Παρέχεται ανεξάρτητα ή συμπληρωματικά με το Cloud Identity Connect, το Cloud Identity Connect for ISAM και το Cloud Identity Essentials.

### 1.1.6 IBM Cloud Identity Govern

Αυτή η Υπηρεσία Cloud ενοποιείται πλήρως με τα τοπικά εγκαθιστώμενα προγράμματα λογισμικού IBM Security Identity Governance and Intelligence (IGI) και IBM Security Identity Manager (ISIM), τα οποία συμπεριλαμβάνονται ως λογισμικό ενεργοποίησης, παρέχοντας μια λύση για την υποστήριξη των επιχειρηματικών απαιτήσεων του Πελάτη για τη διαχείριση πρόσβασης τόσο στις τοπικά εγκατεστημένες εφαρμογές όσο και στις εφαρμογές στο cloud. Αυτή η Υπηρεσία Cloud παρέχει στους οργανισμούς προηγμένες λειτουργίες διαχείρισης κύκλου ζωής στοιχείων ταυτότητας στο cloud, συμπεριλαμβανομένης της διαχείρισης ροής εργασιών αίτησης πρόσβασης σε εφαρμογές.

### 1.1.7 IBM Cloud Identity Connect and Verify

Αυτή η Υπηρεσία Cloud παρέχει στον Πελάτη τις λειτουργίες του IBM Cloud Identity Connect και του IBM Cloud Identity Verify συνδυασμένες σε μία προσφορά.

### 1.1.8 IBM Cloud Identity Analyze

Αυτή η Υπηρεσία Cloud ενισχύει υπάρχουσες λύσεις της IBM, όπως οι IBM Security Identity Governance and Intelligence (IGI) και IBM Security Identity Manager (ISIM), για να παρέχει ένα ολιστικό προφίλ κινδύνου των διαχειριζόμενων χρηστών. Αυτή η Υπηρεσία Cloud περιλαμβάνει έναν τοπικό μηχανισμό ανάλυσης πολλαπλών χρήσεων που επεξεργάζεται δεδομένα δραστηριοτήτων και δικαιωμάτων χρήσης από διάφορες πηγές, οι οποίες παρέχουν προβολή 360 μοιρών των κινδύνων πρόσβασης και δυνατότητα ανάληψης ενεργειών με βάση αυτές τις τεκμηριωμένες πληροφορίες κινδύνου.

### 1.1.9 IBM Cloud Identity Adaptive Access

Αυτή η Υπηρεσία Cloud χρησιμοποιεί τεκμηριωμένες συναφείς πληροφορίες τεχνητής νοημοσύνης (AI) σχετικά με τους χρήστες, τις συσκευές και τα μοτίβα συμπεριφοράς τους προκειμένου να βοηθήσει τους οργανισμούς στην εφαρμογή των κατάλληλων πολιτικών ταυτοποίησης.

### 1.1.10 IBM Cloud Identity Connect Verify and Govern

Αυτή η Υπηρεσία Cloud παρέχει στον Πελάτη τις λειτουργίες του IBM Cloud Identity Connect, του IBM Cloud Identity Verify και του IBM Cloud Identity Govern συνδυασμένες σε μία προσφορά.

## 1.2 Προαιρετικές Υπηρεσίες

### 1.2.1 IBM Security Verify Non-Production

Το IBM Security Verify Non-Production Environment on Cloud είναι μια χωριστή περίπτωση χρήσης της πλατφόρμας IBM Security Verify την οποία επιτρέπεται να χρησιμοποιεί ο Πελάτης μόνο για την εκτέλεση εσωτερικών, μη παραγωγικών δραστηριοτήτων, συμπεριλαμβανομένων, ενδεικτικά και όχι / περιοριστικά, δραστηριοτήτων διενέργειας δοκιμών, ρύθμισης απόδοσης, διάγνωσης σφαλμάτων, εσωτερικής συγκριτικής αξιολόγησης απόδοσης (benchmarking), δοκιμαστικής εφαρμογής (staging) και διασφάλισης ποιότητας ή/και για την ανάπτυξη εσωτερικά χρησιμοποιούμενων προσθηκών ή επεκτάσεων της Υπηρεσίας Cloud με τη χρήση δημοσιευμένων API (application programming interfaces). Για αυτή την Υπηρεσία Cloud παρέχεται η δυνατότητα συμπερίληψης μιας σύμβασης επιπέδου παροχής υπηρεσιών (SLA) αναφορικά με τη διαθεσιμότητα, η οποία θα υπόκειται στους όρους που προβλέπονται στο Άρθρο 3, Επίπεδα Παροχής Υπηρεσιών και Τεχνική Υποστήριξη. Αυτή η Υπηρεσία Cloud έχει δυναμικότητα 100 συμβάντων ανά δευτερόλεπτο.

### 1.2.2 IBM Security Verify Vanity Domain

Ο προσαρμοσμένος τομέας (ένας τομέας) επιτρέπει στον Πελάτη να χρησιμοποιεί έναν ιδιόκτητο τομέα που είναι πιο σχετικός με τον οργανισμό του Πελάτη, αντί να χρησιμοποιεί τον προεπιλεγμένο τομέα μισθωτή που παρέχεται έτοιμος από την πλατφόρμα. Ένα πιστοποιητικό SSL θα διατηρείται από την IBM για αυτόν τον τομέα και θα ανανεώνεται σε ετήσια βάση.

### 1.2.3 IBM Security Verify Application Gateway Hosted

Η πύλη εφαρμογών παρέχει μια φιλοξενούμενη και διαχειριζόμενη από την IBM ελαφριά πλατφόρμα για Πελάτες που αναζητούν υποστήριξη μη τυπικών, ή παλαιότερων, μηχανισμών ταυτοποίησης. Σε αυτούς τους μηχανισμούς συμπεριλαμβάνονται η ταυτοποίηση βάσει LTPA και κεφαλίδων HTTP. Η διαχείριση της συνεχούς παρακολούθησης και της συντήρησης γίνεται από την IBM.

### 1.2.4 IBM Security Verify SMS and Email One-time Password

Αυτή η υπηρεσία παρέχει έναν μηχανισμό ταυτοποίησης δεύτερου επιπέδου με τη χρήση κωδικών πρόσβασης μίας χρήσης που παραδίδονται μέσω μηνυμάτων e-mail και SMS.

### 1.2.5 IBM Security Verify Account Synchronization

Ο συγχρονισμός λογαριασμών (account synchronization) είναι μια διαδικασία μέσω της οποίας οι λογαριασμοί από τις εφαρμογές προορισμού που έχουν παραμετροποιηθεί για παροχή δεδομένων εντοπίζονται και μεταβιβάζονται στο Security Verify. Η διαδικασία εκτελεί επαλήθευση των υφιστάμενων λεπτομερειών λογαριασμών και εφαρμόζει πολιτικές υιοθέτησης και διορθωτικών μέτρων με στόχο το σύστημα να διατηρείται συγχρονισμένο με τις εφαρμογές προορισμού.

### 1.2.6 IBM Cloud Identity Non-Production

Το IBM Cloud Identity Non-Production Environment on Cloud είναι μια χωριστή περίπτωση χρήσης της πλατφόρμας IBM Cloud Identity την οποία επιτρέπεται να χρησιμοποιεί ο Πελάτης μόνο για την εκτέλεση εσωτερικών μη παραγωγικών δραστηριοτήτων, συμπεριλαμβανομένων, ενδεικτικά και όχι περιοριστικά, δραστηριοτήτων διενέργειας δοκιμών, ρύθμισης απόδοσης, διάγνωσης σφαλμάτων, εσωτερικής συγκριτικής αξιολόγησης απόδοσης (benchmarking), δοκιμαστικής εφαρμογής (staging) και διασφάλισης ποιότητας ή/και για την ανάπτυξη εσωτερικά χρησιμοποιούμενων προσθηκών ή επεκτάσεων της Υπηρεσίας Cloud με τη χρήση δημοσιευμένων API (application programming interfaces). Για αυτή την Υπηρεσία Cloud παρέχεται η δυνατότητα συμπερίληψης μιας σύμβασης επιπέδου παροχής υπηρεσιών (SLA) αναφορικά με τη διαθεσιμότητα, η οποία θα υπόκειται στους όρους που προβλέπονται στο Άρθρο 3, Επίπεδα Παροχής Υπηρεσιών και Τεχνική Υποστήριξη. Αυτή η Υπηρεσία Cloud έχει δυναμικότητα 100 συμβάντων ανά δευτερόλεπτο.

### 1.2.7 IBM Cloud Identity Vanity Domain

Ο προσαρμοσμένος τομέας (ένας τομέας) επιτρέπει στον Πελάτη να χρησιμοποιεί έναν ιδιόκτητο τομέα που είναι πιο σχετικός με τον οργανισμό του Πελάτη, αντί να χρησιμοποιεί τον προεπιλεγμένο τομέα μισθωτή που παρέχεται έτοιμος από την πλατφόρμα. Ένα πιστοποιητικό SSL θα διατηρείται από την IBM για αυτόν τον τομέα και θα ανανεώνεται σε ετήσια βάση.

### 1.2.8 IBM Cloud Identity Application Gateway Hosted

Η πύλη εφαρμογών παρέχει μια φιλοξενούμενη και διαχειριζόμενη από την IBM ελαφριά πλατφόρμα για Πελάτες που αναζητούν υποστήριξη μη τυπικών, ή παλαιότερων, μηχανισμών ταυτοποίησης. Σε αυτούς τους μηχανισμούς συμπεριλαμβάνεται η ταυτοποίηση βάσει LTPA και κεφαλίδων HTTP. Η διαχείριση της συνεχούς παρακολούθησης και της συντήρησης γίνεται από την IBM.

## 1.3 Υπηρεσίες Επιτάχυνσης

### 1.3.1 IBM Security Verify Solution Planning

Αυτή η υπηρεσία παρέχει επαγγελματικές υπηρεσίες διάρκειας μίας (1) εβδομάδας κατά την οποία η IBM θα εκτελέσει ορισμένες ή όλες τις ακόλουθες δραστηριότητες:

- Διαμόρφωση περιβάλλοντος ενιαίας σύνδεσης (single sign-on) για βασιζόμενες στο cloud εφαρμογές SaaS
- Παραμετροποίηση μιας πλατφόρμας εκκίνησης (launch pad) για τον εύκολο εντοπισμό εφαρμογών
- Διασύνδεση εφαρμογών με έτοιμες λειτουργίες σύνδεσης (connectors)
- Σχεδιασμός και αρχιτεκτονική της λύσης και σχετική καθοδήγηση
- Προτεινόμενες από την IBM προσεγγίσεις και πρακτικές

### 1.3.2 IBM Security Verify Workshop for Multi-Factor Authentication

Αυτή η υπηρεσία παρέχει ένα εργαστήριο επαγγελματικών υπηρεσιών διάρκειας τριών (3) ημερών, το οποίο θα επικεντρώνεται στις προκλήσεις της ταυτοποίησης πολλαπλών παραγόντων και στην προστασία των εφαρμογών του Πελάτη με τη χρήση του IBM Cloud Identify Verify. Το εργαστήριο θα καλύπτει μερικά ή όλα τα ακόλουθα θέματα:

- Ενσωμάτωση γνώριμων μηχανισμών ταυτοποίησης σε όλες τις ψηφιακές και προσωπικές αλληλεπιδράσεις όπου απαιτείται ταυτοποίηση
- Παραμετροποίηση εφαρμογής για την επιβολή ισχυρής ταυτοποίησης (strong authentication) με τη χρήση ενός φιλικού για την προγραμματιστή REST API
- Παροχή προτάσεων για την ασφάλεια ταυτοτήτων σύμφωνα με τις βέλτιστες πρακτικές του κλάδου
- Εναρμονισμένη εμπειρία χρηστών και υιοθέτηση σε όλους τους παράγοντες μορφής - τηλέφωνα, υπολογιστές tablet και φορητούς υπολογιστές

### 1.3.3 IBM Security Verify Strategy and Planning

Αυτή η υπηρεσία παρέχει ένα εργαστήριο επαγγελματικών υπηρεσιών διάρκεια τριών (3) εβδομάδων σχετικά με τον τρόπο εφαρμογής βέλτιστων πρακτικών ασφάλειας για το cloud. Το εργαστήριο επικεντρώνεται κυρίως στην ασφάλεια υποδομής και εφαρμογών. Το εργαστήριο θα καλύπτει μερικά ή όλα τα ακόλουθα θέματα:

- Διαμόρφωση περιβάλλοντος ενιαίας σύνδεσης (single sign-on) για βασιζόμενες στο cloud εφαρμογές SaaS
- Παραμετροποίηση μιας πλατφόρμας εκκίνησης (launch pad) για τον εύκολο εντοπισμό εφαρμογών
- Διασύνδεση εφαρμογών με έτοιμες λειτουργίες σύνδεσης (connectors)
- Σχεδιασμός και αρχιτεκτονική της λύσης και σχετική καθοδήγηση
- Πληροφόρηση για τις αναδυόμενες τάσεις στην ασφάλεια του κυβερνοχώρου
- Προτεινόμενες από την IBM προσεγγίσεις και πρακτικές

### 1.3.4 IBM Security Verify Expert On Demand

Αυτή η υπηρεσία παρέχει επαγγελματικές υπηρεσίες διάρκειας είκοσι (20) ωρών, οι οποίες παραδίδονται με τη μορφή δώρων συνεδριών κατά τη διάρκεια μιας χρονικής περιόδου τριάντα (30) ημερών από την ημερομηνία έναρξης. Στο πλαίσιο των υπηρεσιών θα διατίθεται ένας αρχιτέκτονας λύσεων IBM Security Verify ο οποίος θα απαντά σε ερωτήσεις και θα παρέχει καθοδήγηση και προτάσεις, ενδεικτικά και όχι περιοριστικά, για τα ακόλουθα θέματα:

- Τεχνικές δεξιότητες για την ενίσχυση της υλοποιημένης λύσης του Πελάτη
- Ερωτήσεις σχετικά με την αρχιτεκτονική και την υλοποίηση της λύσης του Πελάτη
- Καθοδήγηση σχετικά με τη λύση ή/και τη στρατηγική του Πελάτη

### 1.3.5 IBM Cloud Identity Connect Solution Planning

Αυτή η υπηρεσία παρέχει επαγγελματικές υπηρεσίες διάρκειας μίας (1) εβδομάδας κατά την οποία η IBM θα εκτελέσει ορισμένες ή όλες τις ακόλουθες δραστηριότητες:

- Διαμόρφωση περιβάλλοντος ενιαίας σύνδεσης (single sign-on) για βασιζόμενες στο cloud εφαρμογές SaaS
- Παραμετροποίηση μιας πλατφόρμας εκκίνησης (launch pad) για τον εύκολο εντοπισμό εφαρμογών
- Διασύνδεση εφαρμογών με έτοιμες λειτουργίες σύνδεσης (connectors)
- Σχεδιασμός και αρχιτεκτονική της λύσης και σχετική καθοδήγηση
- Προτεινόμενες από την IBM προσεγγίσεις και πρακτικές

### 1.3.6 IBM Cloud Identity Verify Workshop for Multi-Factor Authentication

Αυτή η υπηρεσία παρέχει ένα εργαστήριο επαγγελματικών υπηρεσιών διάρκειας τριών (3) ημερών, το οποίο θα επικεντρώνεται στις προκλήσεις της ταυτοποίησης πολλαπλών παραγόντων και στην προστασία των εφαρμογών του Πελάτη με τη χρήση του IBM Cloud Identify Verify. Το εργαστήριο θα καλύπτει μερικά ή όλα τα ακόλουθα θέματα:

- Ενσωμάτωση γνώριμων μηχανισμών ταυτοποίησης σε όλες τις ψηφιακές και προσωπικές αλληλεπιδράσεις όπου απαιτείται ταυτοποίηση

- Παραμετροποίηση εφαρμογής για την επιβολή ισχυρής ταυτοποίησης (strong authentication) με τη χρήση ενός φιλικού για την προγραμματιστή REST API
- Παροχή προτάσεων για την ασφάλεια ταυτοτήτων σύμφωνα με τις βέλτιστες πρακτικές του κλάδου
- Εναρμονισμένη εμπειρία χρηστών και υιοθέτηση σε όλους τους παράγοντες μορφής - τηλέφωνα, υπολογιστές tablet και φορητούς υπολογιστές

### 1.3.7 IBM Cloud Security Strategy and Planning

Αυτή η υπηρεσία παρέχει ένα εργαστήριο επαγγελματικών υπηρεσιών διάρκειας τριών (3) εβδομάδων σχετικά με τον τρόπο εφαρμογής βέλτιστων πρακτικών ασφάλειας για το cloud. Το εργαστήριο επικεντρώνεται κυρίως στην ασφάλεια υποδομής και εφαρμογών. Το εργαστήριο θα καλύπτει μερικά ή όλα τα ακόλουθα θέματα:

- Διαμόρφωση περιβάλλοντος ενιαίας σύνδεσης (single sign-on) για βασιζόμενες στο cloud εφαρμογές SaaS
- Παραμετροποίηση μιας πλατφόρμας εκκίνησης (launch pad) για τον εύκολο εντοπισμό εφαρμογών
- Διασύνδεση εφαρμογών με έτοιμες λειτουργίες σύνδεσης (connectors)
- Σχεδιασμός και αρχιτεκτονική της λύσης και σχετική καθοδήγηση
- Πληροφόρηση για τις αναδυόμενες τάσεις στην ασφάλεια του κυβερνοχώρου
- Προτεινόμενες από την IBM προσεγγίσεις και πρακτικές

### 1.3.8 IBM Cloud Identity Expert On Demand

Αυτή η υπηρεσία παρέχει επαγγελματικές υπηρεσίες διάρκειας είκοσι (20) ωρών, οι οποίες παραδίδονται με τη μορφή δώρων συνεδριών κατά τη διάρκεια μιας χρονικής περιόδου τριάντα (30) ημερών από την ημερομηνία έναρξης. Στο πλαίσιο των υπηρεσιών θα διατεθεί ένας αρχιτέκτονας λύσεων Cloud Identity ο οποίος θα απαντά σε ερωτήσεις και θα παρέχει καθοδήγηση και προτάσεις, ενδεικτικά και όχι περιοριστικά, για τα ακόλουθα θέματα:

- Τεχνικές δεξιότητες για την ενίσχυση της υλοποιημένης λύσης Cloud Identity του Πελάτη
- Ερωτήσεις σχετικά με την αρχιτεκτονική και την υλοποίηση της λύσης Cloud Identity του Πελάτη
- Καθοδήγηση σχετικά με τη λύση ή/και τη στρατηγική Cloud Identity του Πελάτη

## 2. Φύλλα Δεδομένων για την Επεξεργασία και Προστασία Δεδομένων

Η Πρόσθετη Πράξη για την Επεξεργασία Δεδομένων (Data Processing Addendum - Πρόσθετη Πράξη DPA) της IBM, που διατίθεται στην ιστοσελίδα <http://ibm.com/dpa>, και το(-α) Φύλλο(-α) Δεδομένων για την Επεξεργασία και Προστασία Δεδομένων (τα οποία αναφέρονται ως φύλλο(-α) δεδομένων ή Παράρτημα(-τα) DPA), που διατίθενται στις ιστοσελίδες που παραπέμπουν οι παρακάτω διασυνδέσεις, παρέχουν πρόσθετες πληροφορίες για την προστασία δεδομένων στις Υπηρεσίες Cloud και τις επιλογές που παρέχουν οι Υπηρεσίες Cloud για τα είδη Περιεχομένου που μπορεί να υφίστανται επεξεργασία, τις δραστηριότητες επεξεργασίας και τις λειτουργίες προστασίας δεδομένων καθώς και τη διατήρηση και επιστροφή Περιεχομένου. Η Πρόσθετη Πράξη DPA διέπει τα δεδομένα προσωπικού χαρακτήρα που περιλαμβάνονται στο Περιεχόμενο, εάν και στο βαθμό που ισχύουν i) ο Ευρωπαϊκός Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) (ΕΕ/2016/679) ή ii) άλλοι νόμοι περί προστασίας δεδομένων που προσδιορίζονται στην ιστοσελίδα <http://ibm.com/dpa/dpl>.

<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=735E5650E26711E69CCD7F0385C6524D>

## 3. Επίπεδα Παροχής Υπηρεσιών και Τεχνική Υποστήριξη

### 3.1 Σύμβαση Επιπέδου Παροχής Υπηρεσιών

Η IBM παρέχει στον πελάτη την ακόλουθη σύμβαση επιπέδου παροχής υπηρεσιών (SLA). Η IBM θα παρέχει την υψηλότερη ισχύουσα αποζημίωση με βάση τη σωρευτική διαθεσιμότητα της Υπηρεσίας Cloud, όπως αναφέρεται στον παρακάτω πίνακα. Το ποσοστό διαθεσιμότητας υπολογίζεται ως ο συνολικός αριθμός λεπτών σε έναν συμβατικό μήνα, μείον τον συνολικό αριθμό λεπτών του Χρόνου Διακοπής της Υπηρεσίας κατά τη διάρκεια του συμβατικού μήνα, διαιρούμενος διά του συνολικού αριθμού λεπτών στον συμβατικό μήνα, και ισχύει για την επηρεαζόμενη περιοχή και τον αριθμό των εγγεγραμμένων χρηστών στη συγκεκριμένη περιοχή. Ο ορισμός του Χρόνου Διακοπής Υπηρεσίας, η

διαδικασία για την έγερση αξιώσεων πίστωσης και ο τρόπος επικοινωνίας με την IBM για ζητήματα διαθεσιμότητας υπηρεσιών αναφέρονται στην επισκόπηση υποστήριξης των IBM SaaS στην ιστοσελίδα [https://www.ibm.com/software/support/saas\\_support\\_overview.html](https://www.ibm.com/software/support/saas_support_overview.html).

Διαθεσιμότητα	Πίστωση (% της μηνιαίας χρέωσης συνδρομής*)
Χαμηλότερη από 99,9%	10%

\* Η χρέωση συνδρομής είναι η συμβατικά προβλεπόμενη τιμή για το μήνα που αποτελεί το αντικείμενο της αξίωσης.

### 3.1.1 Άλλες Πληροφορίες για αυτή τη Σύμβαση SLA

Κατά τις πρώτες εξήντα (60) ημέρες της περιόδου ισχύος για τον Πελάτη ("Δοκιμαστική Περίοδος"), ο Πελάτης δεν θα δικαιούται καμία πίστωση σε περίπτωση μη επίτευξης από το περιβάλλον της Υπηρεσίας Cloud του ελάχιστου Ποσοστού 99,9% που προβλέπεται στην παρούσα Σύμβαση για τον Χρόνο Αδιάλειπτης Λειτουργίας. Εάν η IBM εντοπίσει πριν ή κατά τη διάρκεια της Δοκιμαστικής Περιόδου υπάρχουσες παραμετροποιήσεις, πολιτικές, δεδομένα ή κώδικα του Πελάτη ("Προϋπάρχοντα Λειτουργικά Τμήματα") που προορίζονται για μεταφορά στην Υπηρεσία Cloud αλλά θα εμπόδιζαν την Υπηρεσία Cloud να επιτύχει το Ποσοστό Αδιάλειπτης Λειτουργίας που προβλέπεται στην παρούσα Σύμβαση, η IBM διατηρεί το δικαίωμα να ειδοποιήσει τον Πελάτη για τα εν λόγω Προϋπάρχοντα Λειτουργικά Τμήματα και να τα εξαιρέσει, κατά την αποκλειστική διακριτική ευχέρεια της IBM, από τις διατάξεις της Σύμβασης SLA. Σε περίπτωση που η IBM ειδοποιήσει τον Πελάτη για εξαιρούμενα Προϋπάρχοντα Λειτουργικά Τμήματα, η IBM θα είναι υπεύθυνη για την παρουσίαση ενός σχεδίου διορθωτικών μέτρων, το οποίο εξασφαλίζει στο βαθμό που αυτό είναι εφικτό την ανταπόκριση των εν λόγω εξαιρούμενων Προϋπαρχόντων Λειτουργικών Τμημάτων στο Ποσοστό Αδιάλειπτης Λειτουργίας που ορίζεται στην παρούσα Σύμβαση. Ο Πελάτης θα είναι αποκλειστικά υπεύθυνος για το κόστος των εν λόγω διορθωτικών μέτρων, εκτός εάν άλλως συμφωνηθεί από τα δύο συμβαλλόμενα μέρη.

## 3.2 Τεχνική Υποστήριξη

Για πληροφορίες σχετικά με την τεχνική υποστήριξη που παρέχεται για την Υπηρεσία Cloud, συμπεριλαμβανομένων στοιχείων επικοινωνίας για τη λήψη υποστήριξης, των βαθμών κρισιμότητας, των χρόνων απόκρισης και άλλων πληροφοριών και διαδικασιών υποστήριξης, επιλέξτε την Υπηρεσία Cloud στον οδηγό υποστήριξης της IBM (IBM support guide) στην ιστοσελίδα <https://www.ibm.com/support/home/pages/support-guide/>.

## 4. Χρέωσεις

### 4.1 Μετρικά Συστήματα Χρέωσης

Τα μετρικά συστήματα χρέωσης για την Υπηρεσία Cloud καθορίζονται στο Έγγραφο Συναλλαγής.

Χρησιμοποιούνται τα ακόλουθα μετρικά συστήματα χρέωσης για αυτή την Υπηρεσία Cloud:

- Περίπτωση Χρήσης (Instance) είναι κάθε πρόσβαση σε μια συγκεκριμένη παραμετροποίηση των Υπηρεσιών Cloud.
- Δέσμευση (Engagement) είναι μια επαγγελματική ή εκπαιδευτική υπηρεσία που σχετίζεται με τις Υπηρεσίες Cloud.
- Συμβάν (Event) είναι μια εμφάνιση ενός συγκεκριμένου συμβάντος που βρίσκεται υπό την επεξεργασία των Υπηρεσιών Cloud ή σχετίζεται με τη χρήση των Υπηρεσιών Cloud.
  - Για το Security Verify SMS and One-Time Password, ένα Συμβάν είναι ένας κωδικός πρόσβασης μίας χρήσης που παραδίδεται μέσω μηνύματος e-mail ή SMS.
  - Για το Cloud Identity Connect, ένα Συμβάν είναι μια αίτηση http προς την Υπηρεσία Cloud.
- Για το Cloud Identity Verify, ένα Συμβάν είναι οποιαδήποτε μέθοδος πολλαπλών παραγόντων καλείται μέσω της Υπηρεσίας Cloud. Εξουσιοδοτημένος Χρήστης (Authorized User) είναι ένας μοναδικός χρήστης που έχει εξουσιοδοτηθεί να αποκτά πρόσβαση στις Υπηρεσίες Cloud με οποιονδήποτε τρόπο, είτε άμεσα είτε έμμεσα (για παράδειγμα, μέσω ενός προγράμματος πολυπλεξίας (multiplexing), μιας συσκευής ή ενός εξυπηρετητή εφαρμογών (application server)), με οποιοδήποτε μέσο.

- Υπάλληλος (Employee) είναι ένα μοναδικό πρόσωπο που εργάζεται στην Επιχείρηση του Πελάτη ή κατά άλλον τρόπο πληρώνεται από αυτήν ή ενεργεί εκ μέρους της, ανεξάρτητα από το εάν του έχει χορηγηθεί άδεια πρόσβασης στις Υπηρεσίες Cloud.
- Δικαιούμενος Συμμετέχων (Eligible Participant) είναι ένα φυσικό ή νομικό πρόσωπο που πληροί τις προϋποθέσεις για συμμετοχή σε οποιοδήποτε πρόγραμμα παράδοσης υπηρεσιών που βρίσκεται υπό τη διαχείριση ή παρακολούθηση των Υπηρεσιών Cloud.
- Μονάδα Πόρου (Resource Unit) είναι μια ανεξάρτητη μέτρηση ενός πόρου τον οποίο διαχειρίζεται ή επεξεργάζεται η Υπηρεσία Cloud ή ο οποίος σχετίζεται με τη χρήση της Υπηρεσίας Cloud.

Η χρήση κάθε λειτουργίας απαιτεί τον αναφερόμενο αριθμό δικαιωμάτων Μονάδων Πόρων για αυτή τη συνδρομή της Υπηρεσίας Cloud:

Αυξανόμενο Επίπεδο	Μέγιστος Μηνιαίος Αριθμός Ενεργών Χρηστών	Λειτουργία σε σταθμισμένο αριθμό απαιτούμενων Μονάδων Πόρων ανά Χρήστη				
		Ενιαία Σύνδεση	Ταυτοποίηση Πολλαπλών Παραγόντων	Προσαρμοζόμενη Πρόσβαση	Διαχείριση Κύκλου Ζωής και Διακυβέρνηση	Ανάλυση
1	500	0,1000	0,1000	0,1000	0,2900	0,1200
2	5.000	0,0800	0,0800	0,0800	0,0750	0,1000
3	10.000	0,0600	0,0600	0,0600	0,0500	0,0750
4	100.000	0,0080	0,0080	0,0080	0,0050	0,0200
5	500.000	0,0025	0,0025	0,0025	0,0020	0,0150
6	1.000.000	0,0020	0,0020	0,0020	0,0010	0,0010
7	5.000.000	0,0015	0,0015	0,0015	0,0005	0,0005
8	10.000.000	0,0015	0,0015	0,0015	0,0002	0,0002
9	50.000.000	0,0010	0,0010	0,0010	0,0001	0,0001
10	999.999.999	0,0005	0,0005	0,0005	0,0001	0,0001

Σημείωση: Όλοι οι υπολογισμοί θα στρογγυλοποιούνται σε ακέραιο αριθμό.

## 5. Πρόσθετοι Όροι

Για τις Συμβάσεις Υπηρεσιών Cloud (ή ισοδύναμες βασικές συμβάσεις cloud) που συνάφθηκαν πριν την 1η Ιανουαρίου 2019, ισχύουν οι όροι που αναφέρονται στον ιστότοπο <https://www.ibm.com/acs>.

### 5.1 Αναφορά του Πελάτη

Ο Πελάτης συμφωνεί ότι η IBM μπορεί να αναφέρει τον Πελάτη δημοσίως ως συνδρομητή των Υπηρεσιών Cloud σε διαφημίσεις και σε δημοσιεύσεις στον τύπο.

### 5.2 Λογισμικό Ενεργοποίησης

Η Υπηρεσία Cloud περιέχει το ακόλουθο Λογισμικό Ενεργοποίησης:

- IBM Security Verify Bridge
- IBM Security Verify
- IBM Security Verify SDK (iOS)
- IBM Security Verify SDK (Android)
- IBM Security Verify SDK for JavaScript
- IBM Security Verify Bridge for Directory Sync
- IBM Application Gateway
- IBM Security Verify Hosted Application Gateway
- IBM Security Verify Gateway for Windows Login



- IBM Security Verify Gateway for PAM (on AIX)
- IBM Security Verify Gateway for PAM
- IBM Security Verify Gateway for RADIUS
- IBM Security Verify Credentials

Το ακόλουθο λογισμικό ενεργοποίησης επιτρέπεται να χρησιμοποιείται μόνο με τις Υπηρεσίες Cloud IBM Cloud Identity Connect, IBM Cloud Identity Connect and Verify και IBM Cloud Identity Connect Verify and Govern:

- IBM Security Access Manager Virtual Enterprise Edition

Το ακόλουθο λογισμικό ενεργοποίησης επιτρέπεται να χρησιμοποιείται μόνο με τις Υπηρεσίες Cloud IBM Security Verify, IBM Cloud Identity Govern και IBM Cloud Identity Connect Verify and Govern:

- IBM Security Identity Governance and Intelligence Enterprise Edition
- IBM Security Identity Manager

**Σημαντικό:** Η παρούσα Περιγραφή Υπηρεσιών συντάχθηκε στην αγγλική γλώσσα. Μπορείτε να βρείτε και να εκτυπώσετε αντίγραφο της παρούσας Περιγραφής Υπηρεσιών στην αγγλική από την εξής ιστοσελίδα:

<http://www-03.ibm.com/software/sla/sladb.nsf/sla/saas>

Η ελληνική μετάφραση παρέχεται μόνο για λόγους διευκόλυνσης. Σε περίπτωση ασυμφωνίας μεταξύ του αγγλικού κειμένου και της ελληνικής του μετάφρασης, το αγγλικό κείμενο υπερισχύει. Εάν για οποιονδήποτε λόγο δεν έχετε πρόσβαση στο αγγλικό κείμενο, παρακαλούμε όπως επικοινωνήσετε με τον τοπικό εκπρόσωπο της IBM προκειμένου να σας το αποστείλουμε άμεσα.