Συχνές Ερωτήσεις

(FAQs)

Lookout Mobile Endpoint Security

1. Τι είναι το Lookout Mobile Endpoint Security;

Το Lookout Mobile Endpoint Security (MES) προστατεύει συσκευές με λογισμικό iOS, Android, και Chrome OS ενάντια σε κακόβουλο λογισμικό, ηλεκτρονικό «ψάρεμα» (phishing), μη ασφαλή δίκτυα, ευπάθειες συσκευών, και άλλες μορφές κυβερνοεπιθέσεων που στοχεύουν σε κινητές συσκευές. Το Lookout MES αποτελείται από 3 βασικά στοιχεία:

Εφαρμογή Lookout for Work: Μια iOS και Android εφαρμογή για εταιρικές και BYOD συσκευές που προσφέρει συνδεσιμότητα στο Lookout Security Cloud, επιβλέπει τα σημεία εισόδου των απειλών στις κινητές συσκευές και τις προστατεύει βάσει των καθορισμένων πολιτικών ασφαλείας.

Lookout Security Graph: Το Lookout Security Cloud χρησιμοποιεί συσχετιστική ανάλυση cloud για τον εντοπισμό απειλών στις συσκευές. Βασίζεται σε ένα θεμέλιο πληροφοριών σχετικά με τις απειλές των κινητών συσκευών, δεδομένα εφαρμογών, και ανάλυση κακόβουλων λογισμικών, συμπεριλαμβανομένου ενός συνόλου περισσότερων από 180 εκατομμυρίων εφαρμογών κινητής τηλεφωνίας που εκτελούνται, αξιολογούνται, συγκρίνονται και αναλύονται σε συνεχή βάση. Το Lookout Security Cloud υποστηρίζεται επίσης από δεδομένα τηλεμετρίας πλήθους που συλλέγονται από περισσότερες από 200 εκατομμύρια κινητές συσκευές, με δεκάδες εκατομμύρια συσκευές να συνεισφέρουν με νέα δεδομένα ασφαλείας, κάθε μήνα, από όλο τον κόσμο.

Κονσόλα Διαχείρισης: Η Κονσόλα Διαχείρισης είναι η κεντρική τοποθεσία όπου οι διαχειριστές μπορούν να διευκολύνουν την εγγραφή συσκευών, να λαμβάνουν δεδομένα σχετικά με τις απειλές και τις επικίνδυνες εφαρμογές στο δίκτυό τους και να ορίζουν πολιτικές ασφαλείας.

2. Η Lookout έχει πρόσβαση στα προσωπικά μου δεδομένα και πληροφορίες;

Προστασία Δεδομένων: Η Lookout πιστεύει ακράδαντα ότι το απόρρητο είναι εξίσου σημαντικό με την ασφάλειά σας, γι' αυτό και θέλουμε να είμαστε απόλυτα διαφανείς σχετικά με τα δεδομένα που συλλέγουμε για να συμβάλλουμε στη διασφάλιση των συσκευών σας και της ασφάλειας κάθε εργαζομένου. Μπορείτε να διαβάσετε σχετικά με την πολιτική απορρήτου της Lookout εδώ.

Οι τελικοί χρήστες μπορούν να έχουν πρόσβαση στη πολιτική προσωπικών δεδομένων μέσα από την εφαρμογή Lookout for Work, που έχουν εγκαταστήσει.

Συλλογή Δεδομένων: Για την ασφάλεια των κινητών συσκευών, το Lookout for Work MES πρέπει να συλλέγει και να αναλύει ορισμένα δεδομένα για τον εντοπισμό και την αντιμετώπιση των απειλών. Γενικά, το Lookout MES συλλέγει 4 κατηγορίες δεδομένων από τις εγγεγραμμένες συσκευές:

- Δεδομένα εφαρμογών για τον εντοπισμό απειλών ασφαλείας που βασίζονται σε εφαρμογές.
- Δεδομένα Firmware ή λειτουργικού συστήματος για τον εντοπισμό παραβιασμένου Firmware ή λειτουργικών συστημάτων.
- Δεδομένα διαμόρφωσης για τον εντοπισμό επικίνδυνων ή κακόβουλων ρυθμίσεων και παραμετροποιήσεων.
- Δεδομένα αναγνώρισης συσκευής για τον εντοπισμό και την αποκατάσταση συσκευών που έχουν ρίσκο ασφαλείας για τον

οργανισμό σας και την επικοινωνία με τους χρήστες της συσκευής σε περίπτωση προβλήματος ασφάλειας.

Η Lookout δεν συλλέγει προσωπικά δεδομένα και πληροφορίες, όπως εικόνες, ήχο, βίντεο ή μηνύματα και κείμενα, ούτε δεδομένα που παράγονται από τις εφαρμογές που χρησιμοποιούν οι εργαζόμενοι της εταιρείας.

Έλεγχος των Δεδομένων που προβάλλει η Lookout στους Διαχειριστές: Ορισμένοι οργανισμοί θέλουν να διασφαλίσουν ότι οι διαχειριστές δεν μπορούν να βλέπουν τα ονόματα των εφαρμογών στις συσκευές ή τα δίκτυα στα οποία συνδέονται οι συσκευές, καθώς ενδέχεται να αποκαλύψουν ορισμένα στοιχεία σχετικά με τον υπάλληλο. Για παράδειγμα, μια εφαρμογή γνωριμιών μπορεί να περιέχει κακόβουλο λογισμικό, αλλά το όνομα της εφαρμογής θα μπορούσε να αποκαλύψει προσωπικά στοιχεία για τον υπάλληλο.

Για να αντιμετωπιστεί αυτή η ανησυχία, μπορούμε να επιτρέψουμε στον κάτοχο του Lookout tenant να διαγράψει το όνομα της απειλής. Μόλις ενεργοποιηθεί αυτή η λειτουργία, η Κονσόλα θα εμφανίζει μόνο τις υψηλού επιπέδου πληροφορίες για την απειλή, οι οποίες είναι απαραίτητες για τη λήψη απόφασης αποκατάστασης, ενώ δεν θα εμφανίζονται λεπτομέρειες όπως η συγκεκριμένη διεύθυνση URL, το όνομα της εφαρμογής, τα δεδομένα δυαδικής ανάλυσης της εφαρμογής, το όνομα του δικτύου και τα δεδομένα ανάλυσης δικτύου. Επικοινωνήστε με τον εσωτερικό διαχειριστή σας για να διαπιστώσετε αν αυτή η λειτουργία είναι ενεργοποιημένη στο περιβάλλον σας.

3. Πώς μπορώ να ενεργοποιήσω το Lookout for Work σε μια iOS συσκευή;

Ο διαχειριστής της Υπηρεσίας Lookout από την εταιρεία σας, θα πρέπει να αποστείλει μια πρόσκληση ηλεκτρονικού ταχυδρομείου που εξηγεί σε κάθε χρήστη πώς να εγκαταστήσει την εφαρμογή **Lookout for Work**, μέσω της κονσόλας Διαχειριστή.

Ο χρήστης στη συνέχεια, θα πρέπει να:

1. Πατήσει Install (Εγκατάσταση) και να ολοκληρώσει την εγκατάσταση.
2. Να ανοίξει την εφαρμογή - Οι χρήστες ΠΡΕΠΕΙ να ανοίξουν την εφαρμογή τουλάχιστον μία φορά για να την ενεργοποιήσουν.
3. Επιτρέψει στο Lookout να στέλνει ειδοποιήσεις και προαιρετικά να έχει πρόσβαση στην τοποθεσία τους.
4. Μόλις ολοκληρωθεί η ενεργοποίηση, το Lookout for Work θα πραγματοποιήσει πλήρη σάρωση της συσκευής και θα εντοπίσει αν υπάρχουν προβλήματα/απειλές. Εάν δεν υπάρχουν προβλήματα, ο χρήστης θα δει το μήνυμα «Δεν βρέθηκαν προβλήματα».

4. Πως να ενεργοποιήσω το Lookout for Work σε μια συσκευή Android;

Ο διαχειριστής της Υπηρεσίας Lookout από την εταιρεία σας, θα πρέπει να αποστείλει μια πρόσκληση ηλεκτρονικού ταχυδρομείου που εξηγεί σε κάθε χρήστη πώς να εγκαταστήσει την εφαρμογή **Lookout for Work**, μέσω της κονσόλας Διαχειριστή.

Ο χρήστης στη συνέχεια, θα πρέπει να:

1. Πατήσει «Εγκατάσταση»
2. Πατήσει «Αποδοχή» (επιτρέποντας τη λήψη της εφαρμογής)
3. Ανοίξει την εφαρμογή (οι χρήστες ΠΡΕΠΕΙ να ανοίξουν την εφαρμογή τουλάχιστον μία φορά για να ενεργοποιήσουν την εφαρμογή).
4. Μόλις ολοκληρωθεί η ενεργοποίηση, το Lookout for Work θα πραγματοποιήσει πλήρη σάρωση της συσκευής και θα εντοπίσει αν

υπάρχουν προβλήματα/απειλές. Εάν δεν υπάρχουν προβλήματα, ο χρήστης θα δει το μήνυμα «Δεν βρέθηκαν προβλήματα».

5. Γιατί η εφαρμογή Lookout for Work μου ζητάει κωδικό ενεργοποίησης;

Κατά τη λήψη της εφαρμογής Lookout for Work από το App Store ή το Google Play Store, οι χρήστες ενδέχεται να κληθούν να εισάγουν έναν κωδικό ενεργοποίησης ή μια διεύθυνση ηλεκτρονικού ταχυδρομείου. Αυτός ο κωδικός ενεργοποίησης επιτρέπει τη συσκευή του τελικού χρήστη στο Lookout tenant του οργανισμού.

6. Γιατί η εφαρμογή Lookout for Work μου ζητάει να δώσω άδεια πρόσβασης στα δεδομένα τοποθεσίας μου; Είναι απαραίτητο να δώσω πρόσβαση;

Κατά την ενεργοποίηση της εφαρμογής Lookout for Work, ζητάμε από τους χρήστες να επιτρέψουν τις ειδοποιήσεις και τις υπηρεσίες τοποθεσίας.

Αυτή είναι απλώς μία από τις διάφορες μεθόδους που χρησιμοποιεί το λογισμικό, ως μηχανισμό διατήρησης/ελέγχου για την εφαρμογή.
Σημείωση: Η Lookout δεν συλλέγει ποτέ δεδομένα τοποθεσίας ούτε τα μοιράζεται με τον εργοδότη/διαχειριστή της εταιρείας. Η Lookout δεν παρακολουθεί τη συσκευή ή τον χρήστη.

Δεν απαιτείται να δώσετε πρόσβαση σε δεδομένα τοποθεσίας. Οι χρήστες μπορούν να εξαιρεθούν από την πρόσβαση της Lookout for Work στην τοποθεσία τους.

7. Γιατί η εφαρμογή Lookout for Work μου ζητάει να επιτρέψω τη λήψη ειδοποιήσεων; Είναι απαραίτητο;

Όταν ένας χρήστης ανοίγει την εφαρμογή Lookout for Work για πρώτη φορά, τον παροτρύνουμε να επιτρέψει τις ειδοποιήσεις και τις υπηρεσίες τοποθεσίας.

Συνιστούμε στους χρήστες να επιτρέπουν τις ειδοποιήσεις, ώστε η Lookout να μπορεί να στέλνει ενημερώσεις σε πραγματικό χρόνο όταν εντοπίζεται κάποιο πρόβλημα ή απειλή. Η ειδοποίηση δίνει τη δυνατότητα στον τελικό χρήστη να διορθώνει και εξαλείφει το πρόβλημα ή την απειλή.

8. Η εφαρμογή Lookout for Work λειτουργεί στο background; Μπορώ να κλείσω την εφαρμογή;

Ναι, η εφαρμογή Lookout for Work λειτουργεί στο background.

Ναι, οι χρήστες μπορούν να κλείσουν με ασφάλεια την εφαρμογή, η οποία θα ενημερώνει περιοδικά τη Κονσόλα και θα συνεχίζει να προστατεύει τη συσκευή. Η εφαρμογή Lookout for Work θα ειδοποιεί τον χρήστη και τον διαχειριστή κάθε φορά που ανακαλύπτει κάποιο πρόβλημα ή απειλή.
Σημείωση: Όταν οι χρήστες σύρουν την εφαρμογή στο iOS (κάνουν swipe-up), το Lookout θα επικοινωνεί και πάλι περιοδικά με την εφαρμογή χωρίς καμία ένδειξη προς τον χρήστη. Ο χρήστης δεν θα μπορεί να δει την εφαρμογή όταν πατήσει το κουμπί Home. Ωστόσο, η εφαρμογή συνεχίζει να επικοινωνεί με το backend σύστημα και να προστατεύει τη συσκευή.

9. Ποια είναι η επίπτωση στη κατάσταση της μπαταρίας;

Οι δοκιμές της Lookout και η εμπειρία των χρηστών δείχνουν ότι η κατανάλωση της μπαταρίας θα είναι κατά μέσο όρο 3%-5% σε μια περίοδο 24 ωρών. Οι χρήστες ενδέχεται να παρατηρήσουν μεγαλύτερη κατανάλωση κατά την αρχική εγκατάσταση και τη πλήρη σάρωση της συσκευής.

10. Η εφαρμογή Lookout for Work εντόπισε μια εφαρμογή που πραγματοποιεί παράλληλη φόρτωση (side-loading) και μου συνέστησε να την απεγκαταστήσω. Χρειάζομαι αυτή την εφαρμογή για επαγγελματικούς λόγους. Τι πρέπει να κάνω;

Αυτός ο τύπος ειδοποίησης ενεργοποιείται όταν μια εφαρμογή εγκαταστάθηκε στη συσκευή μέσω μιας πηγής εκτός των εγκεκριμένων app stores και δεν έχει υπογραφεί από ένα Enterprise Provisioning Profile, εγκεκριμένο από τον οργανισμό σας. Αυτό σημαίνει ότι η εφαρμογή παράκαμψε τη διαδικασία έγκρισης του app store και ενδέχεται να είναι επιβλαβής. Μπορεί επίσης να πρόκειται για μια εφαρμογή υπό ανάπτυξη ή προς δοκιμή από τον χρήστη. Εάν πιστεύετε ότι η εφαρμογή δεν ενέχει κίνδυνο, μπορείτε να επιτρέψετε τη λειτουργία της side-loaded εφαρμογής.

11. Η εφαρμογή Lookout for Work εντόπισε έναν μη διαπιστευμένο προγραμματιστή (app developer) και πρότεινε τη διαγραφή της εφαρμογής. Χρειάζομαι αυτή την εφαρμογή για επαγγελματικούς λόγους. Τι πρέπει να κάνω;

Εγκαθιστώντας μια τέτοια εφαρμογή, η συσκευή αποδέχτηκε έναν προγραμματιστή με τρόπο που του επιτρέπει να εγκαταστήσει οποιονδήποτε αριθμό εφαρμογών στη συσκευή χωρίς να περάσει από την τυπική διαδικασία έγκρισης του Apple App Store ή της beta έκδοσης. Οι εφαρμογές που εγκαθίστανται με αυτόν τον τρόπο μπορεί ενδεχομένως να είναι επιβλαβείς. Ωστόσο, με αυτό τον τρόπο, είναι πιθανό, να γίνεται δοκιμή μιας εφαρμογής υπό ανάπτυξη, στη συσκευή του χρήστη. Εάν πιστεύετε ότι ο προγραμματιστής δεν αποτελεί κίνδυνο, μπορείτε να επιτρέψετε την εγκατάσταση και χρήση της εφαρμογής του.

12. Πως μπορώ να αποκτήσω την εφαρμογή Lookout for Work;

Ο ευκολότερος τρόπος για να ενεργοποιήσετε την εφαρμογή Lookout for Work, είναι να ζητήσετε από τον διαχειριστή της Υπηρεσίας Lookout από την εταιρεία σας, να σας στείλει μια πρόσκληση μέσω της οποίας μπορείτε να κατεβάσετε και να ενεργοποιήσετε την εφαρμογή.

Μπορείτε επίσης να κατεβάσετε το Lookout for Work από το App Store ή το Google Play Store κάνοντας αναζήτηση για την εφαρμογή «Lookout for Work». Εάν ένας χρήστης κατεβάσει την εφαρμογή Lookout for Work από οποιοδήποτε από τα δύο app stores, θα χρειαστεί να συμπληρώσει τα απαραίτητα διαπιστευτήρια: διεύθυνση email ή κωδικό ενεργοποίησης.

Apple App Store

Google Play Store

13. Πώς μπορώ να ενημερώσω την εφαρμογή Lookout for Work;

Η εφαρμογή Lookout for Work θα ενημερώνεται αυτόματα όταν προστίθενται νέες εκδόσεις στο App Store ή στο Google Play Store.

14. Τι θα βλέπει ο τελικός χρήστης όταν εμφανίζεται ένα πρόβλημα ή μια απειλή;

Όταν η λειτουργία Απόκρισης, στην ενότητα «Πολιτικές» έχει οριστεί σε «Ειδοποίηση Συσκευής» και η εφαρμογή Lookout for Work εντοπίσει ένα πρόβλημα, ο χρήστης λαμβάνει μια ειδοποίηση στη συσκευή του και βλέπει ένα σύμβολο στο εικονίδιο της εφαρμογής. Ο χρήστης μπορεί να πατήσει την ειδοποίηση για περισσότερες πληροφορίες. Αυτό

ανοίγει την εφαρμογή Lookout for Work και εμφανίζει την περιγραφή του προβλήματος ή της απειλής, τις συστάσεις και τα βήματα για την επίλυση του προβλήματος.

Όταν η λειτουργία Απόκρισης έχει οριστεί σε «Να μην ειδοποιηθεί η συσκευή», ο χρήστης δεν θα ειδοποιηθεί και μόνο ο διαχειριστής θα λάβει ειδοποίηση.

15. Τι είδους ζητήματα ή απειλές μπορεί να ανιχνεύσει το Lookout;

Οι κινητές απειλές κατηγοριοποιούνται σε τέσσερις φορείς κινδύνου:

- Web and Περιεχόμενο (Ασφαλής Περιήγηση)
- Εφαρμογές
- Δίκτυο
- Ευπάθειες & Ρίσκα Συσκευών

Από προεπιλογή, το Lookout αναθέτει πολιτικές σε διαφορετικούς τύπους ζητημάτων με βάση την εκτίμησή μας για τη σοβαρότητα ή τον αντίκτυπο της πιθανής απειλής. Οι διαχειριστές μπορούν να προσαρμόσουν τις προεπιλεγμένες πολιτικές ώστε να αντικατοπτρίζουν καλύτερα τις ανάγκες της εταιρείας τους. Οι πολιτικές κατηγοριοποιούνται ως υψηλού, μεσαίου ή χαμηλού κινδύνου αντικατοπτρίζοντας ένα αντίστοιχο επίπεδο κινδύνου για κάθε τύπο απειλής.