ZeroFOX integreren met paraplu

Inhoud

Inleiding

In dit document wordt beschreven hoe u ZeroFOX Enterprise kunt integreren met Umbrella, zodat de beveiligingsgebeurtenissen kunnen worden toegepast op clients die worden beschermd door Umbrella.

ZeroFOX Enterprise en Cisco Umbrella Integration - Overzicht

Door ZeroFOX Enterprise te integreren met Cisco Umbrella kunnen beveiligingsmedewerkers en beheerders bescherming bieden tegen de huidige op sociale media gebaseerde bedreigingen voor roaming-laptops, tablets of telefoons, terwijl ze ook een andere handhavingslaag bieden aan een gedistribueerd bedrijfsnetwerk.

Cisco Umbrella en ZeroFox Integration: hoe werkt het?

ZeroFOX Enterprise duwt alle bedreigingen die het vindt, zoals cyberbedreigingen op sociale media, waaronder gerichte malware, phishing, social engineering, imitaties en andere frauduleuze of schadelijke activiteiten, naar Cisco Umbrella voor wereldwijde handhaving.

Umbrella valideert vervolgens de dreiging om ervoor te zorgen dat deze kan worden toegevoegd aan een beleid. Als wordt bevestigd dat de informatie van ZeroFOX een bedreiging vormt, wordt het domeinadres toegevoegd aan de bestemmingslijst van ZeroFOX als onderdeel van een beveiligingsinstelling die kan worden toegepast op elk overkoepelend beleid. Dat beleid wordt onmiddellijk toegepast op alle verzoeken die worden ingediend vanaf apparaten die aan dat beleid zijn toegewezen.

In de toekomst parseert Cisco Umbrella automatisch ZeroFOX-waarschuwingen en voegt het schadelijke sites toe aan de ZeroFOX-bestemmingslijst, waardoor ZeroFOX-intelligentie wordt uitgebreid naar alle externe gebruikers en apparaten en een andere laag van handhaving wordt geboden aan uw bedrijfsnetwerk.

Dit wordt bereikt door middel van deze eenvoudige installatiestappen:

1. Schakel de integratie in Umbrella in om een API-token te genereren.
2. Plak die API-token in uw ZeroFOX-account.
3. Stel ZeroFOX in om te blokkeren onder beveiligingsinstellingen voor uw gewenste beleid(en)

Voorwaarden

- ZeroFOX Enterprise-beheerdersrechten
- Administratieve rechten overkoepelend dashboard
- Het Umbrella-dashboard moet de ZeroFOX-integratie hebben ingeschakeld

Opmerking: de ZeroFOX-integratie is alleen inbegrepen in het pakket voor het Umbrella Platform. Als u niet over het Platform-pakket beschikt en ZeroFOX-integratie wilt, neemt u contact op met uw Cisco Umbrella-vertegenwoordiger. Als u het Platform-pakket hebt, maar ZeroFOX niet ziet als een integratie voor uw dashboard, neem dan contact op met Umbrella Support.

Belangrijk: terwijl Umbrella zijn best doet om domeinen waarvan bekend is dat ze over het algemeen veilig zijn (bijvoorbeeld Google en Salesforce) te valideren en toe te staan, om ongewenste onderbrekingen te voorkomen, raden we aan om domeinen die u niet wilt blokkeren toe te voegen aan de Global Allow List of andere bestemmingslijsten volgens uw beleid.

Voorbeelden zijn:

- De homepage voor uw organisatie. Bijvoorbeeld mydomain.com.
- Domeinen die diensten vertegenwoordigen die u levert en die zowel interne als externe records kunnen hebben. Bijvoorbeeld mail.myservicedomain.com en portal.myotherservicedomain.com.

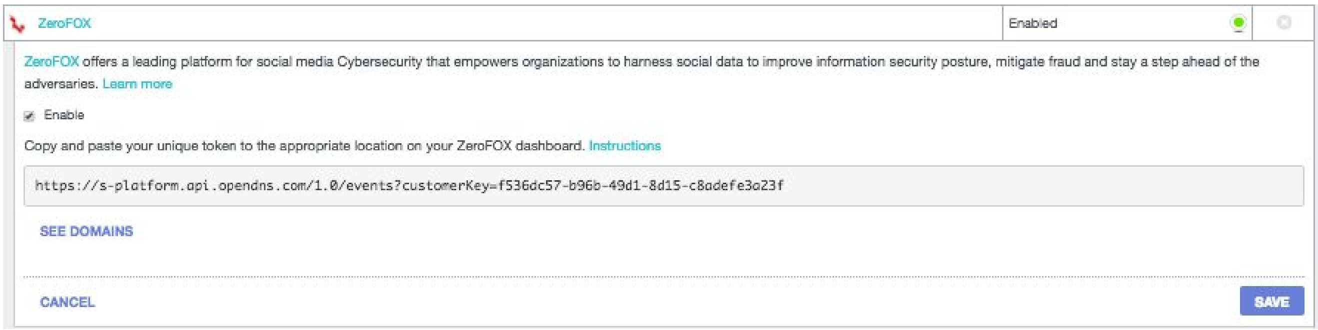
- Minder bekende cloudapplicaties waar u sterk afhankelijk van bent, kunnen niet door Umbrella worden opgemerkt of opgenomen in hun automatische domeinvalidatie. Bijvoorbeeld localcloudservice.com.

De globale lijst met toegestane items is te vinden op Beleid > Bestemmingslijsten in Paraplu. Zie onze documentatie voor meer informatie: Bestemmingslijsten beheren

Stap 1: Umbrella Script en API Token Generation

Begin met het vinden van uw unieke URL in Umbrella voor het ThreatQ-apparaat om mee te communiceren.

1. Meld u aan bij uw Umbrella-dashboard als beheerder, navigeer naar Instellingen > Integraties en klik op "ZeroFOX" in de tabel om het uit te vouwen.
2. Selecteer Inschakelen en klik op Opslaan. Dit genereert een unieke URL met uw klantsleutel.

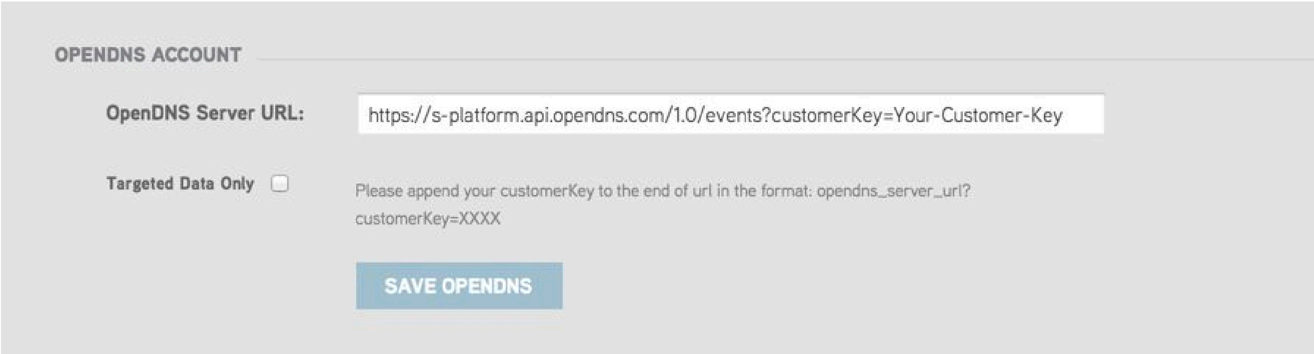


U hebt de URL later nodig wanneer u ZeroFOX configureert, dus kopieer de URL en ga naar uw ThreatQ-dashboard.

Stap 2: Stel uw ZeroFOX Enterprise Dashboard in om informatie naar de paraplu te sturen

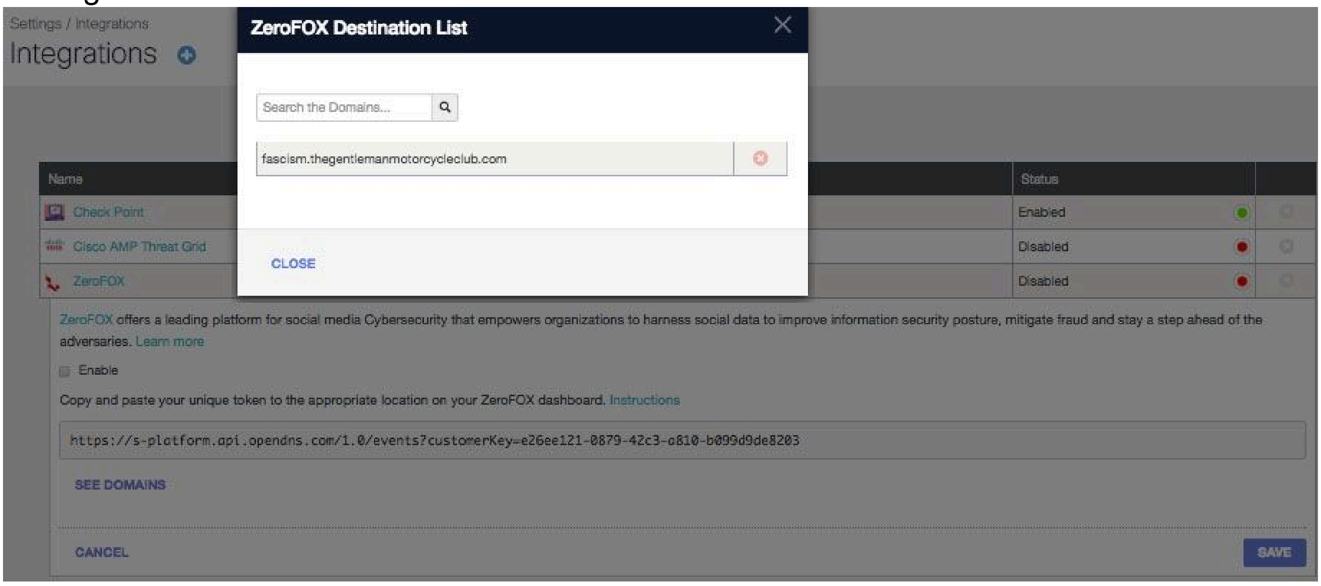
De volgende stap is om de URL die u in stap één hebt gekopieerd toe te voegen aan het ZeroFOX-dashboard.

1. Klik op het tandwielpictogram in het Zerofox-dashboard en selecteer vervolgens Accountinstellingen.
2. Blader omlaag in de integratielijst totdat u de OpenDNS-accountgegevens ziet en plak de URL van Umbrella in het OpenDNS Server URL-veld.
3. Als de integratie voor het eerst is ingeschakeld, raden we u aan Alleen gerichte gegevens te controleren.



Stap 3: ZeroFOX-evenementen instellen om te worden geblokkeerd binnen de paraplu

1. Meld u als beheerder weer aan bij uw Umbrella-dashboard.
2. Navigeer naar Instellingen > Integraties en klik op "ZeroFOX" in de tabel om het uit te vouwen.
3. Klik op Zie domeinen.
   Dit breidt een lijst met domeinen uit die de laatste paar uur van evenementen van uw ZeroFOX-account bevat. Vanaf dat moment begint een doorzoekbare lijst te worden gevuld en te groeien.



De volgende stap is het observeren en controleren van de gebeurtenissen die zijn toegevoegd aan uw nieuwe ZeroFOX-beveiligingscategorie.

Waarnemen van gebeurtenissen toegevoegd aan de ZeroFOX-beveiligingscategorie in de controlemodus

De gebeurtenissen van ZeroFOX Enterprise beginnen een specifieke bestemmingslijst te vullen die kan worden toegepast op beleid als een ZeroFOX-beveiligingscategorie. De doellijst en de beveiligingscategorie bevinden zich standaard in de controlemodus en worden niet toegepast op beleidsregels en leiden niet tot wijzigingen in uw bestaande overkoepelende beleidsregels.

Opmerking: de controlemodus kan worden ingeschakeld zolang dit nodig is op basis van uw implementatieprofiel en netwerkconfiguratie.

Bestemmingslijst bekijken

U kunt de ZeroFox-bestemmingslijst op elk gewenst moment bekijken.

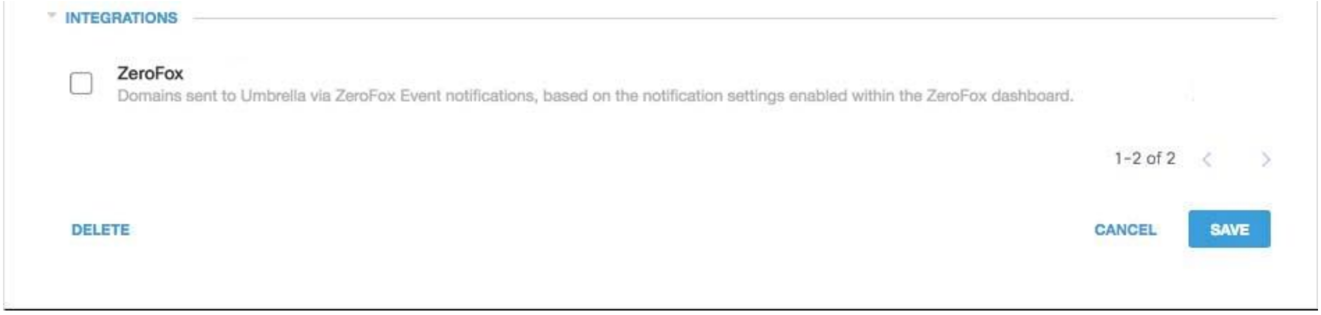
1. Ga naar Instellingen > Integraties.
2. Vouw "ZeroFOX" in de tabel uit en klik op Zie domeinen.

Beveiligingsinstellingen voor een beleid bekijken

U kunt op elk gewenst moment de beveiligingsinstelling bekijken die voor een beleid kan worden ingeschakeld.

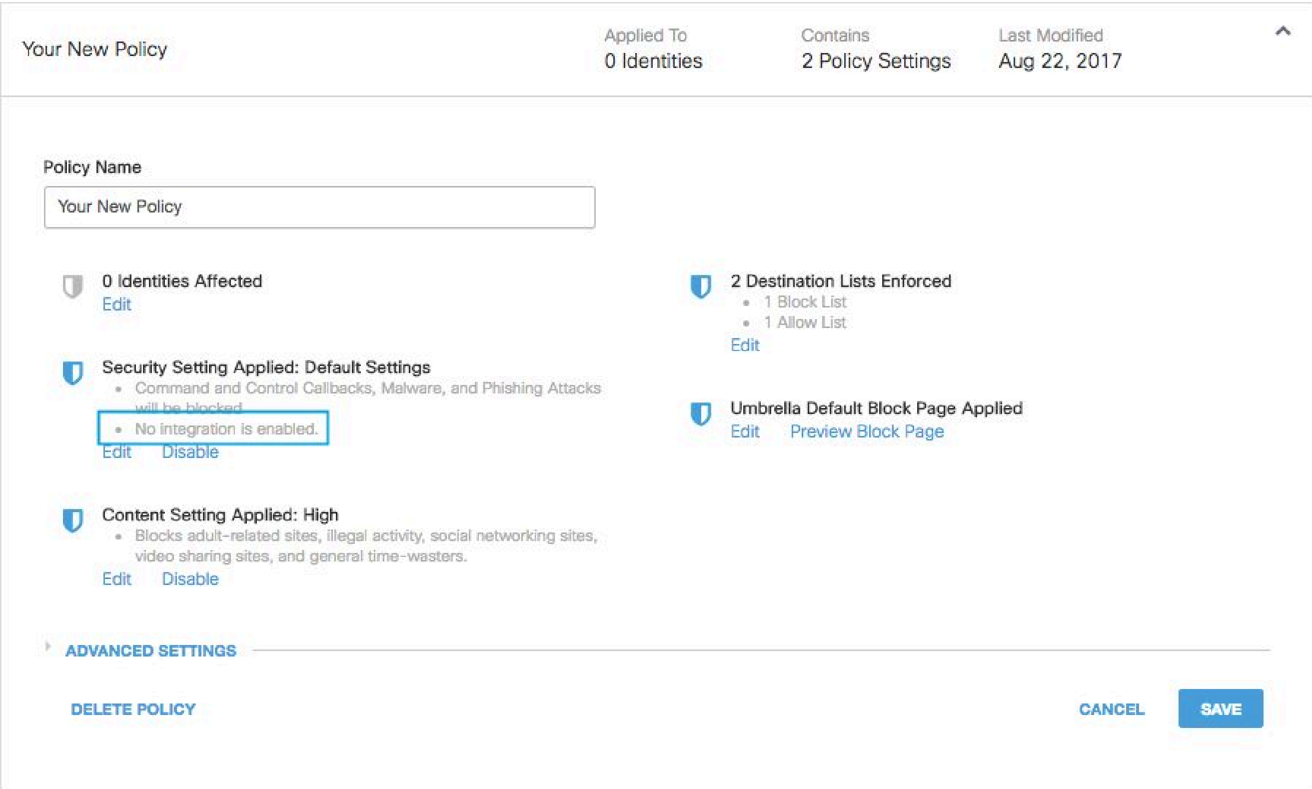
1. Ga naar Beleid > Beveiligingsinstellingen.
2. Klik op een beveiligingsinstelling in de tabel om deze uit te vouwen en blader naar

Integraties om de ZeroFOX-instelling te vinden.



115014041606

U kunt ook integratiegegevens bekijken via de pagina Overzicht van beveiligingsinstellingen.



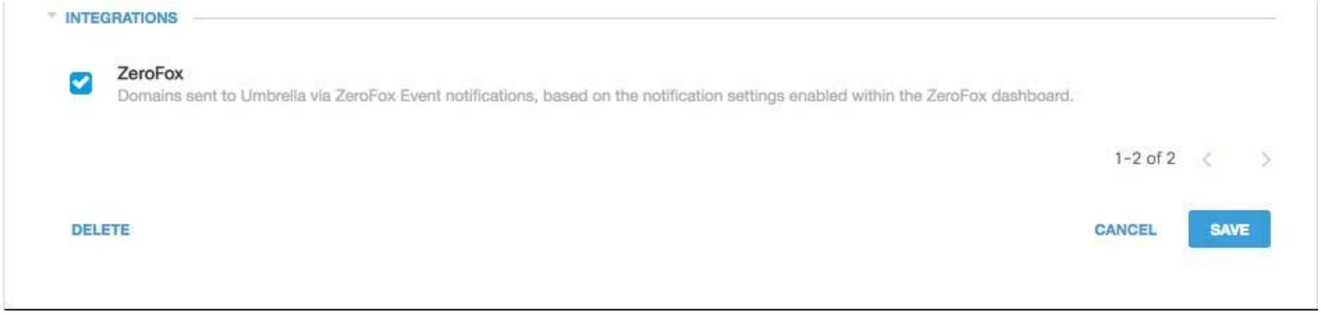
25464154913556

De ZeroFOX-beveiligingsinstellingen in de blokmodus toepassen op een beleid voor beheerde clients

Zodra u klaar bent om deze extra beveiligingsbedreigingen te laten afdwingen door clients die door Umbrella worden beheerd, wijzigt u eenvoudig de beveiligingsinstelling op een bestaand beleid of maakt u een nieuw beleid dat hoger ligt dan uw standaardbeleid om ervoor te zorgen dat het eerst wordt gehandhaafd.

1. Navigeer naar Beleid > Beveiligingsinstellingen en onder Integraties, controleer ZeroFOX en

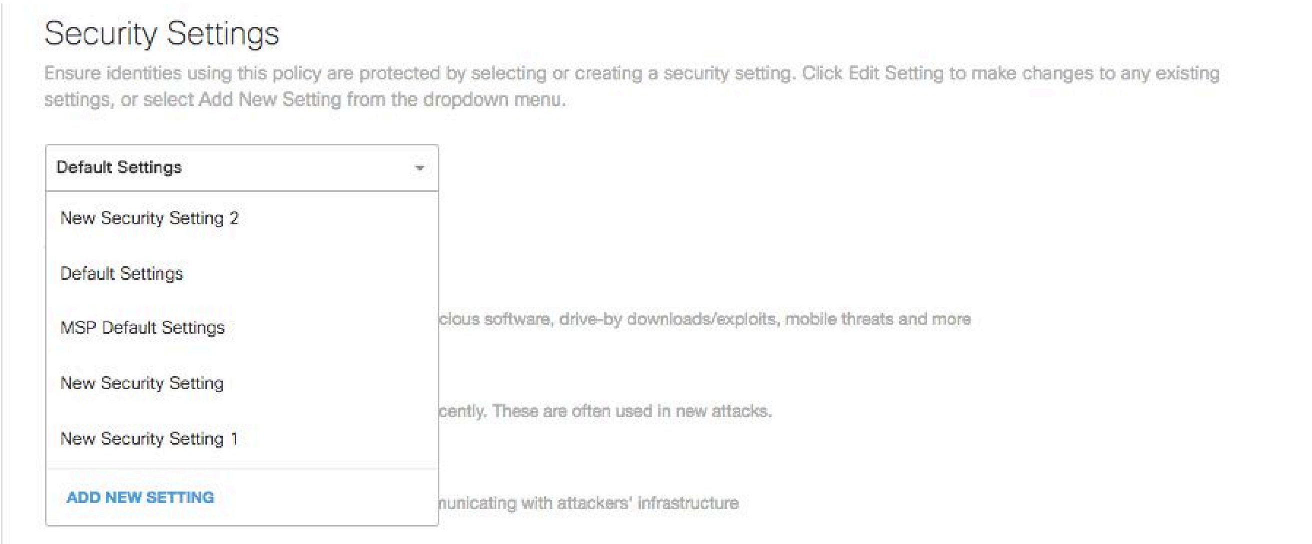
klik op Opslaan.



115014042806

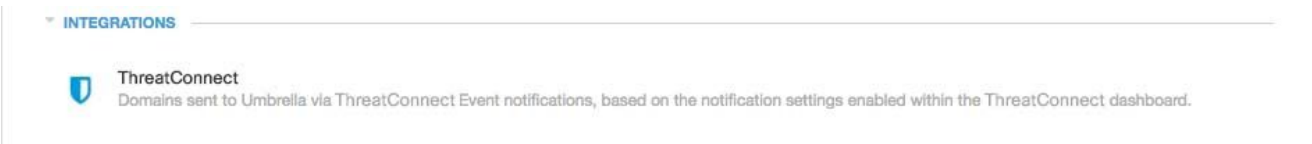
Voeg vervolgens in de wizard Beleid een beveiligingsinstelling toe aan het beleid dat u bewerkt:

1. Navigeer naar Beleid > Beleidslijst.
2. Vouw een beleid uit en klik op Bewerken onder Beveiligingsinstelling toegepast.
3. Selecteer in de vervolgkeuzelijst Beveiligingsinstellingen een beveiligingsinstelling die de instelling ThreatConnect bevat.



25464147943700

Het schildpictogram onder Integraties wordt bijgewerkt naar blauw.



25464147957652

4. Klik op Instellen en retourneren.

ZeroFOX-domeinen in de beveiligingsinstelling voor ZeroFOX worden geblokkeerd voor die identiteiten die dat beleid gebruiken.

Rapportage in Umbrella voor ZeroFOX-evenementen

Rapportage over ZeroFOX-beveiligingsgebeurtenissen

De ZeroFOX-bestemmingslijst is een van de lijsten met beveiligingscategorieën waarover u kunt rapporteren. De meeste of alle rapporten gebruiken de beveiligingscategorieën als filter. U kunt bijvoorbeeld beveiligingscategorieën filteren om alleen ZeroFOX-gerelateerde activiteiten weer te geven.

1. Navigeer naar Rapportage > Activiteit zoeken en selecteer onder Beveiligingscategorieën ZeroFOX om het rapport te filteren zodat alleen de beveiligingscategorie voor ZeroFOX wordt weergegeven.

Opmerking: Als ZeroFOX-integratie is uitgeschakeld, wordt deze niet weergegeven in het filter Beveiligingscategorieën.

115014043046

2. Klik op Apply (Toepassen).

Rapporteren wanneer domeinen zijn toegevoegd aan de ZeroFOX-bestemmingslijst

Het Umbrella Admin Audit-logboek bevat gebeurtenissen uit uw ZeroFOX-account omdat het domeinen aan de bestemmingslijst toevoegt.

Het overkoepelende auditlogboek van de beheerder is te vinden op Rapportage > Controlelogboek van de beheerder. Om te rapporteren wanneer een domein is toegevoegd, filtert u om alleen ZeroFOX-wijzigingen op te nemen door een filter toe te passen op Identiteiten en instellingen voor de ZeroFox-bestemmingslijst.

Nadat u het rapport hebt uitgevoerd, ziet u een lijst met de wijzigingen die zijn aangebracht toen de ZeroFOX-bestemmingslijst werd toegevoegd aan de integratie.

Omgaan met ongewenste detecties of valse positieven

Een lijst met machtigingen voor ongewenste detectie beheren

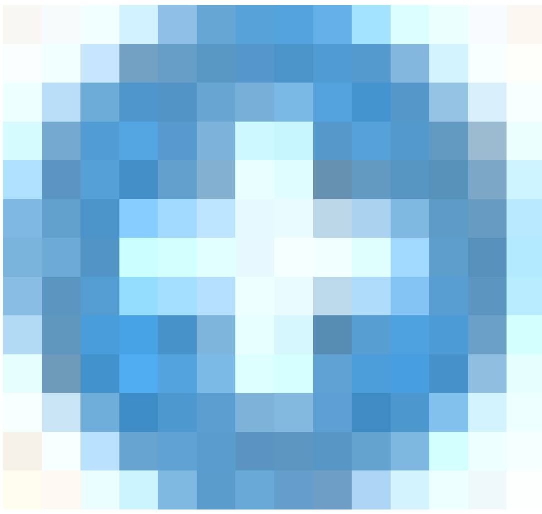
Hoewel onwaarschijnlijk, is het mogelijk dat domeinen die automatisch door ZeroFOX worden toegevoegd, een ongewenste blokkering kunnen veroorzaken die voorkomt dat gebruikers toegang krijgen tot bepaalde websites. In een dergelijke situatie raden we aan om de domeinnamen toe te voegen aan een lijst met machtigingen, die voorrang heeft op alle andere soorten blokkeringslijsten, inclusief beveiligingsinstellingen. Een allow-lijst heeft voorrang op een block-lijst wanneer een domein in beide aanwezig is.

Er zijn twee redenen waarom deze aanpak de voorkeur verdient. Ten eerste, in het geval dat het ZeroFOX-toestel het domein opnieuw zou toevoegen nadat het was verwijderd, staat de lijst beveiligingen toe tegen dit veroorzaken van verdere problemen. Ten tweede toont de allow-lijst een historisch overzicht van problematische domeinen die kunnen worden gebruikt voor forensisch onderzoek of auditrapporten.

Standaard is er een algemene lijst met toegestane items die wordt toegepast op alle beleidsregels. Als u een domein toevoegt aan de algemene machtigingslijst, wordt het domein toegestaan in alle beleidsregels.

Als de ZeroFOX-beveiligingsinstelling in de blokmodus alleen wordt toegepast op een subset van uw beheerde paraplu-identiteiten (deze wordt bijvoorbeeld alleen toegepast op zwervende computers en mobiele apparaten), kunt u een specifieke machtigingslijst maken voor die identiteiten of beleidsregels.

U maakt als volgt een lijst met machtigingen:

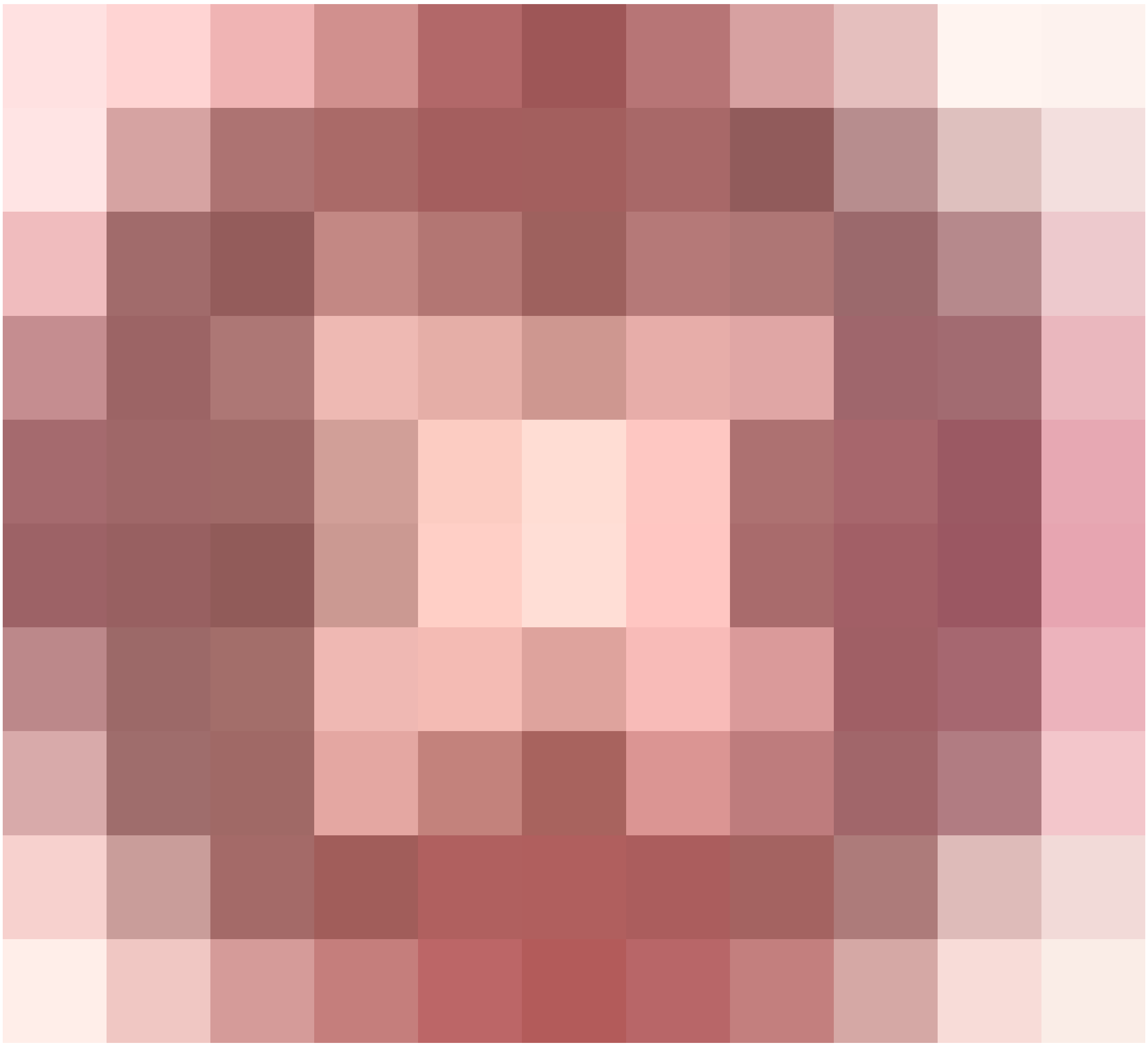
1. Navigeer naar Beleid > Bestemmingslijsten, klik op de 

   25464155856404

   Pictogram toevoegen.
2. Selecteer Toestaan en voeg uw domein toe aan de lijst.
3. Klik op Save (Opslaan).

Zodra de bestemmingslijst is opgeslagen, kunt u deze toevoegen aan een bestaand beleid voor die clients die zijn getroffen door het ongewenste blok.

Domeinen verwijderen uit de bestemmingslijst van ZeroFOX

Er is een  (Verwijderen) pictogram naast elke domeinnaam in de ZeroFOX Bestemmingslijst. Als u domeinen verwijdert, kunt u de ZeroFOX-bestemmingslijst opschonen in het geval van een ongewenste detectie.

Het verwijderen is echter niet permanent als ZeroFOX het domein opnieuw doorstuurt naar Umbrella.

Een domein verwijderen:

1. Navigeer naar Instellingen > Integraties en klik vervolgens op "ZeroFOX" om het uit te vouwen.
2. Klik op Zie domeinen.
3. Zoek naar de domeinnaam die je wilt verwijderen.
4. Klik op het pictogram Verwijderen.

5. Klik op Close (Sluiten).
6. Klik op Save (Opslaan).

In het geval van een ongewenste detectie of vals positief, raden we aan om onmiddellijk een allow-lijst in Umbrella te maken en vervolgens het vals positief binnen ZeroFOX te herstellen. Later kunt u het domein verwijderen uit de ZeroFOX-bestemmingslijst.