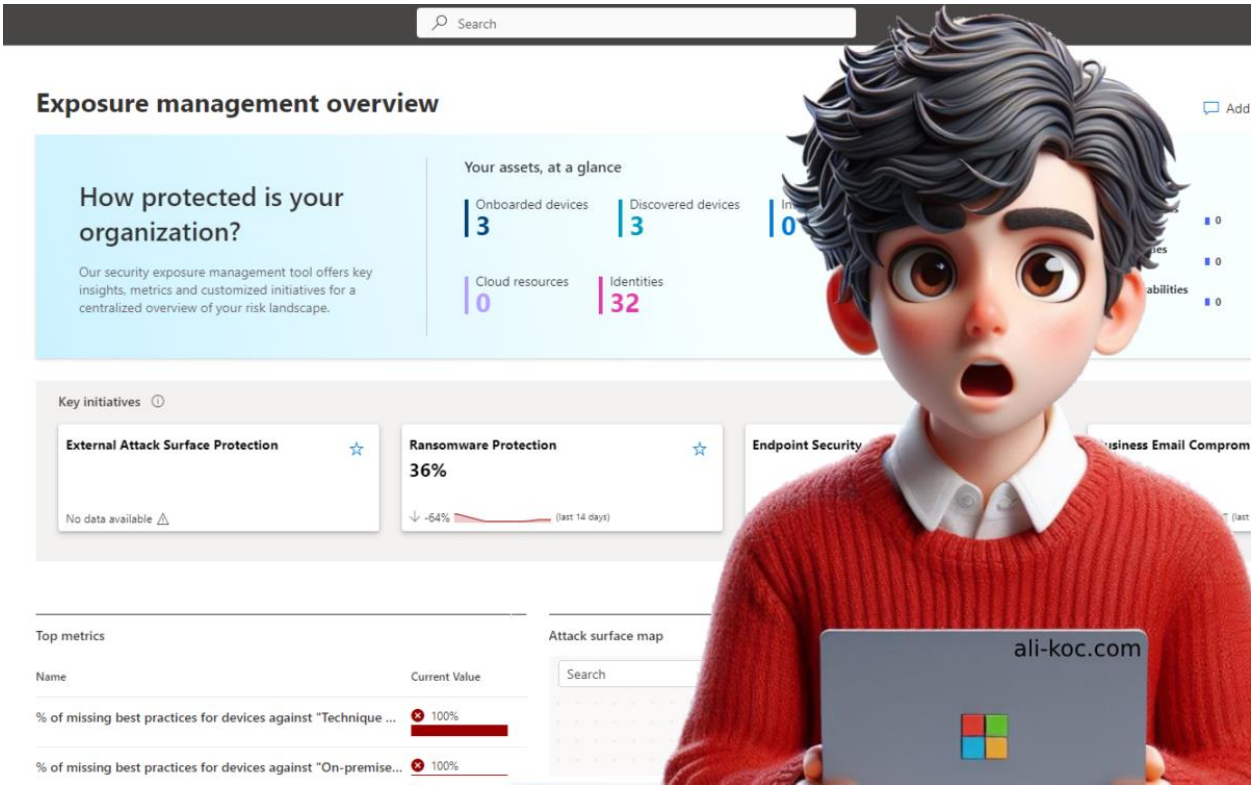
YAYINLANDI ! Exposure Management Genel Kullanıma Sunuldu



Microsoft Security Exposure Management Genel Kullanıma sunuldu. Kullandığınız Security Portalınızda erişebilirsiniz.

Güvenlik ortamınız hakkında bilgiler edinirken, potansiyel tehditleri saldırıya geçmeden önce belirlemenize, önceliklendirmenize ve çözüme kavuşturmanıza yardımcı olacaktır.

Security Customer Connection Program'ın bir üyesi olarak, özel önizlemede geçen uzun bir sürenin ve testlerin ardından Microsoft'un Security Exposure Management'in genel önizlemede kullanabiliyor olmak çok mutlu ediyor!

Security Exposure Management

Exposure Management, Extended Security Posture Management (XSPM), etki alanına özgü ürünlerden gelen güvenlik duruşu bilgilerini ve içgörülerini bir araya getiren iş yükleri arası

maruz kalma ve duruş yönetimi için kullanacağımız alan durumunda. Bu, mevcut Microsoft Güvenlik iş yüklerinizin üzerine inşa edilmiş bir platform genel önizlemeye sunulmuştur.

•Microsoft Defender for Endpoint (MDE)
•Microsoft Defender for Identity (MDI)
•Microsoft Defender for Cloud Apps (MDA)
•Microsoft Defender for Office (MDO)
•Microsoft Defender for IOT (MDIOT)
•Microsoft Secure Score
•Microsoft Defender Vulnerability Management
•Defender Cloud Security Posture Management (CSPM)
•External Attack Surface Management
•Microsoft Entra

Exposure Management , yukarıda bulunan bu iş yüklerinin maruziyet ve duruşla ilgili yönlerinin yerini almayacak. Bunun yerine, bunları birleşik bir görünümde birleştirerek maruz kalma, potansiyel saldırı yolları ve güvenlik programlarının olgunluğu hakkında içgörüler sunarak iş önceliklerini göz önünde bulundururken sürekli güvenlik duruşu iyileştirmesini sağlayacaktır. Bu, ransomware koruması ve Endpoint Security gibi farklı güvenlik alanlarına odaklanan, maruziyeti ve duruşu değerlendirmek için mevcut ürünleri optimize eden Girişimler aracılığıyla proaktif olarak gerçekleştirilebilir. Alternatif olarak, reaktif bir yaklaşım, gelişen tehditler ve güvenlik açıkları nedeniyle dikkat gerektiren güvenlik olaylarının toplu bir görünümünü içermektedir.
Exposure Management ayrıca, kritik kurumsal varlıkların otomatik olarak tanımlanması ve bu varlıklara yönelik tehditleri bir saldırganın bakış açısından anlamak ve ele almak için gelişmiş saldırı yolu yönetimi de dahil olmak üzere gelişmiş çapraz iş yükü analizini dahil ederek iş yüküne özgü deneyimleri yükseltmektedir.

Microsoft Exposure Management'in Faydaları

Comprehensive visibility into exposure: Platform, tüm güvenlik ürünlerinde maruziyete ilişkin tek bir görünüm sağlayarak güvenlik yöneticilerine kuruluşlarının risk profiline ilişkin bütünsel bir anlayış sunmaktadır.

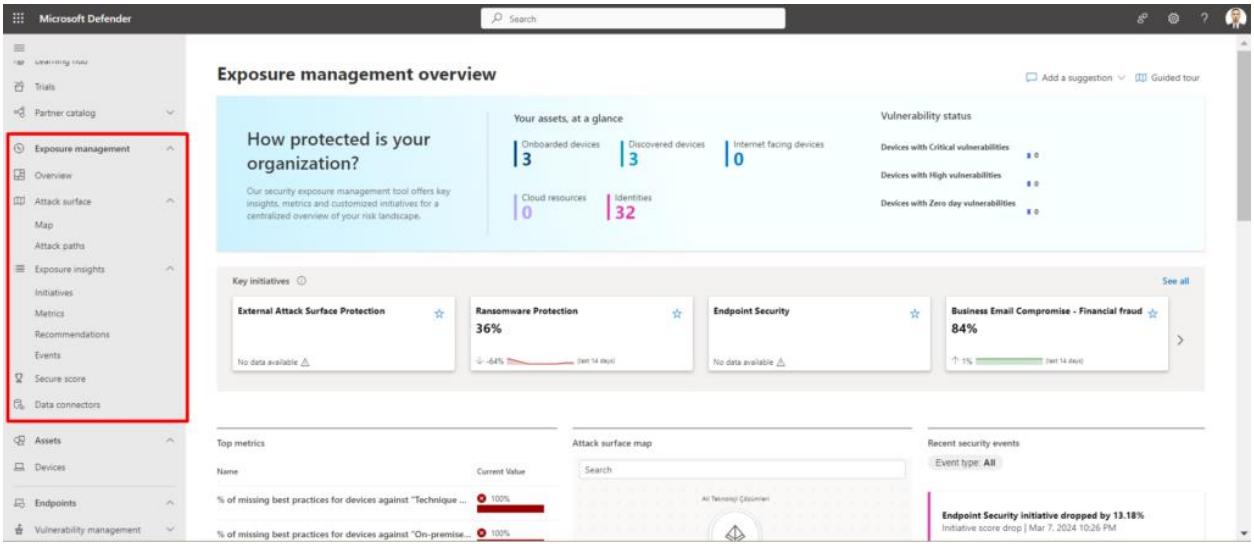
Drill-down capabilities: Güvenlik yöneticileri belirli güvenlik programlarını veya tehditleri inceleyerek o segmentte ne kadar maruz kaldıklarını görebilirler. Bu, düzeltme çabalarını iş bağlamına ve verilere dayalı olarak en büyük risk alanlarına odaklamalarına olanak tanır.

Actionable recommendations: Platform, maruziyeti azaltmak için eyleme geçirilebilir öneriler sunmaktadır. Bu, güvenlik yöneticilerinin iyileştirme çabalarını önceliklendirmelerine ve kaynaklarından en iyi şekilde yararlanmalarına yardımcı olacaktır.

Exposure events feed: Güvenlik ekiplerinin izlemesi ve yanıt vermesi için hayati önem taşıyan kritik maruz kalma olaylarını derler. Bu maruz kalma olayları, kuruluşunuzun varlıklarıyla ilgili temel koşullardaki değişiklikler ve ortaya çıkan güvenlik açıkları hakkında içgörüler sunmaktadır.

Critical Asset Identification: Platform, kuruluşunuzdaki kritik varlıkları otomatik olarak tanımlar, maruz kalma ve potansiyel güvenlik açıkları ile ilgili önemlerini vurgular. Kullanıcılar ayrıca kuruluşlarındaki kritik varlıkları tanımlamak için kendi mantıklarını tanımlayabilirler. Bu, güvenlik yöneticilerine hangi varlıkların korunmasının en hayati öneme sahip olduğunu net bir şekilde anlama yetkisi verir ve kilit kaynaklarınızı korumak için proaktif bir yaklaşım sağlamaktadır.

Attack Path Management: Platform, saldırganların kritik varlıklarınıza erişmek ve bunları tehlikeye atmak için kullanabilecekleri potansiyel rotaları belirleyerek saldırı yollarını etkili bir şekilde yönetir. Güvenlik yöneticileri bu yolları proaktif olarak ele alarak güvenlik ihlali riskini azaltabilir ve kuruluşunuzun en önemli veri ve sistemlerinin güvenliğini sağlayabilir. Bu proaktif yaklaşım, potansiyel tehditlerin önüne geçmenizi ve kritik varlıklarınızı etkili bir şekilde korumanızı sağlar.



Critical asset protection

Günümüzün dinamik tehdit ortamında, kritik varlıkların korunması kuruluşlar için büyük önem taşımaktadır. Kritik varlık koruması, kuruluşunuzun en değerli kaynaklarını, işinizi yürüten varlıkları proaktif olarak belirlemenize ve güvence altına almanıza ve veri ihlalleri ve

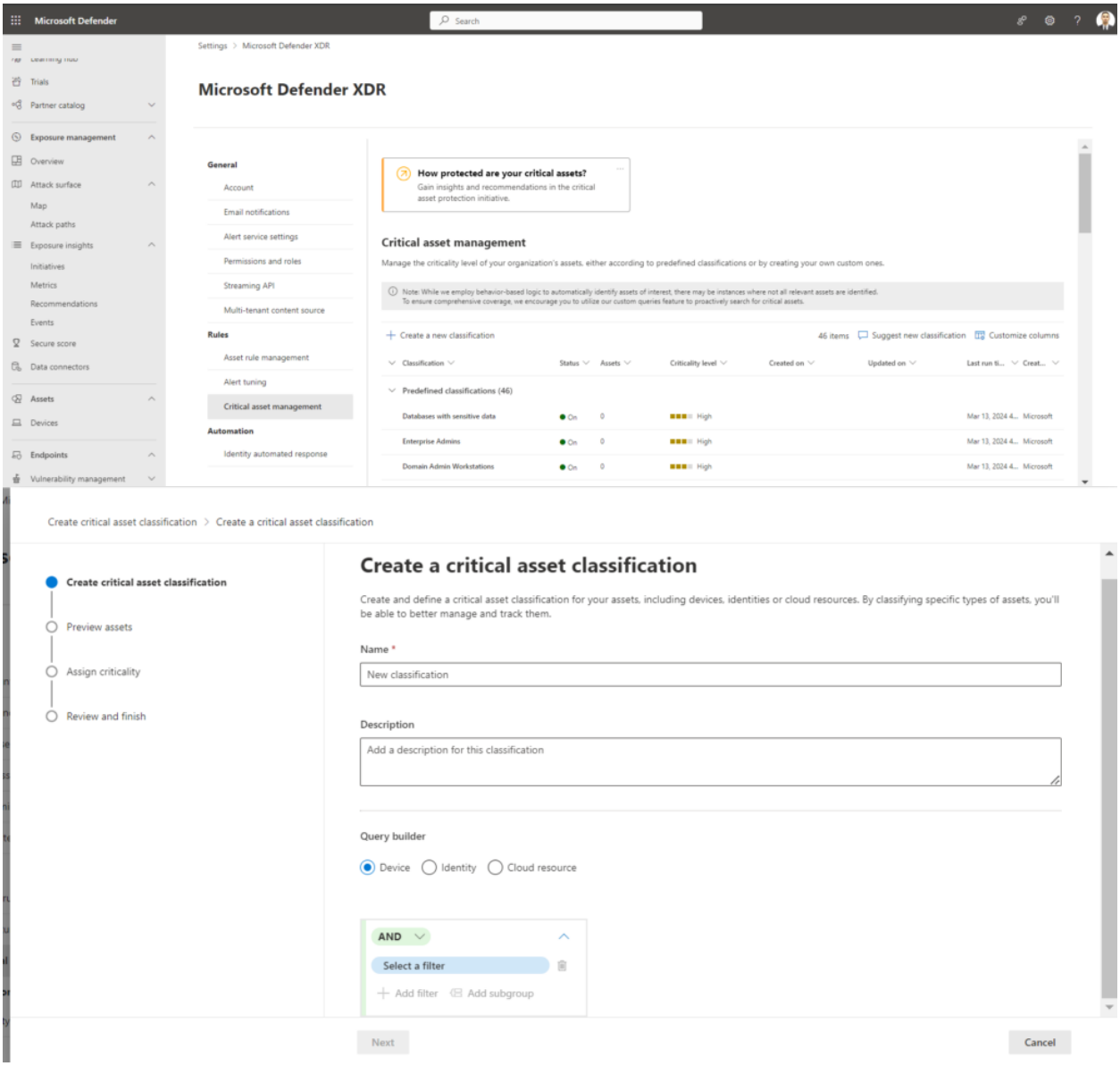
operasyonel kesinti riskini azaltmanıza yardımcı olmak için aşağıda özetlenen yetenekleri sağlar.

Automatically: Çözüm, kuruluşunuzdaki kritik varlıkları otomatik olarak belirlemek için gelişmiş analitik kullanır. Bu, süreci kolaylaştırarak daha yüksek koruma ve acil dikkat gerektiren varlıkları belirlemenizi sağlamaktadır.

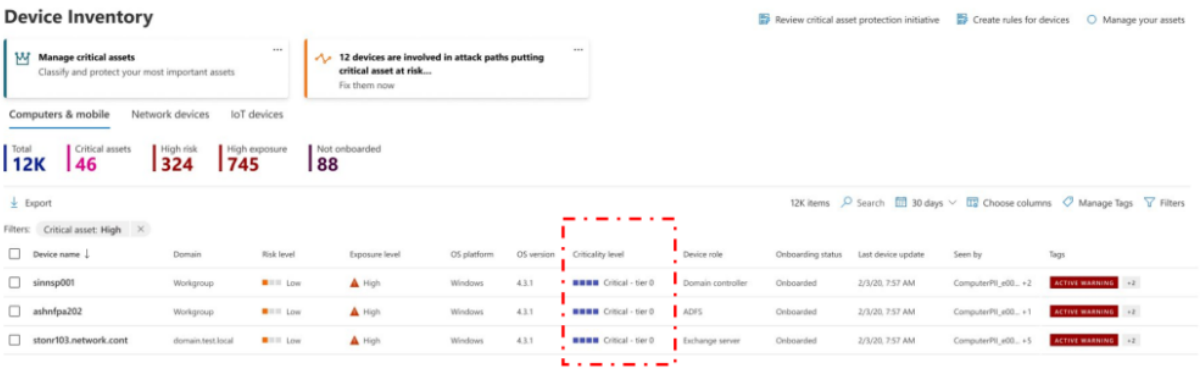
With custom queries: Özel sorgular oluşturabilme özelliği, benzersiz kriterlere dayalı olarak kuruluşunuzun "en önemli değerlerini" belirlemenize olanak tanır. Bu granüler kontrol, güvenlik çabalarınızı tam olarak ihtiyaç duyulan yerlere odaklayabilmenizi sağlamaktadır.

Critical asset Management:
Kritiklik seviyelerini yalnızca önceden tanımlanmış varlık sınıflandırmaları için değil, aynı zamanda kuruluşunuza özgü varlıklar için de özelleştirin ve yönetebilirsiniz.

Kuruluşunuzun varlıklarının kritiklik düzeyini yönetmek için Critical Asset Management menüsünü seçiyoruz. Kritik varlık yönetimi sayfasından yeni sınıflandırmalar oluşturabilir veya kuruluşunuzdaki mevcut sınıflandırmalar için kritiklik seviyelerini güncelleyebilirsiniz.



Yeni sınıflandırmanız için kriterleri belirleyin ve İleri'yi seçin. Sonraki sayfalarda, etkilenecek varlıkları önizleyebilir ve varlık kümesi için kritiklik düzeyini atayabilirsiniz.



Attack Path Management
Kritik varlıkların belirlenmesi, siber güvenliğin karmaşık ortamında hikayenin yalnızca bir tarafıdır. Diğer kritik husus ise potansiyel tehditlerin bu değerli varlıklara nasıl ulaşabileceğini ve onları nasıl tehlikeye atabileceğini anlamaktır. Saldırı Yolu Yönetimi, kritik varlıkları riske atan saldırı yollarını otomatik olarak oluşturup görselleştirerek bu sorunu çözmek için tasarlanmıştır. Saldırı yolu yönetimi şunları sağlar
Kurumlar potansiyel tehditleri proaktif olarak belirler, görselleştirir ve ele alır, böylece kritik varlıklarını hedef alan güvenlik ihlalleri riskini azaltır.

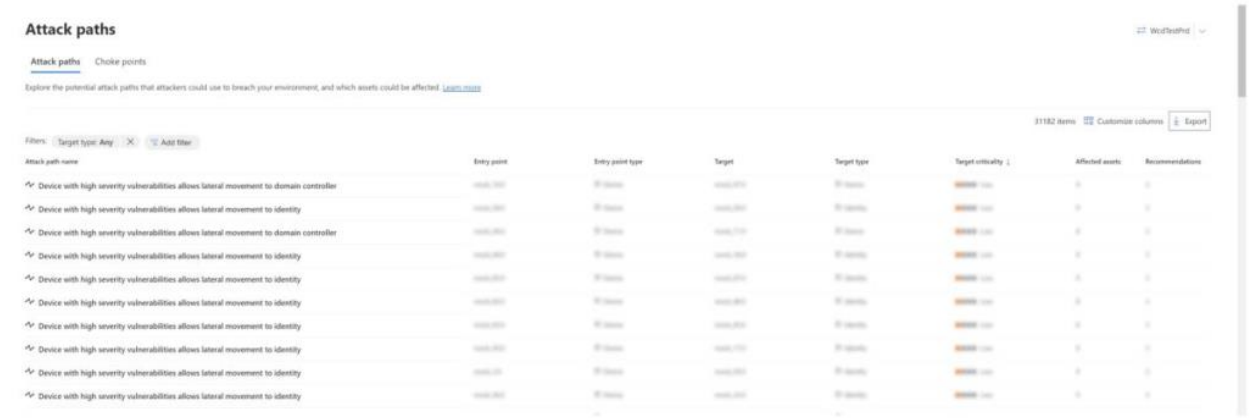
Automatically generates attack paths: Çeşitli saldırı senaryolarını simüle ederek, bir saldırının yararlanabileceği kuruluşun güvenlik duruşundaki güvenlik açıklarını ve zayıflıkları belirler.

Provides visibility into attack paths with graph view: Bu grafik görünümü, potansiyel tehditlerin nasıl ortaya çıkabileceğinin net bir şekilde anlaşılmasını sağlayarak tehdit değerlendirmesine ve karar verme sürecine yardımcı olacaktır.

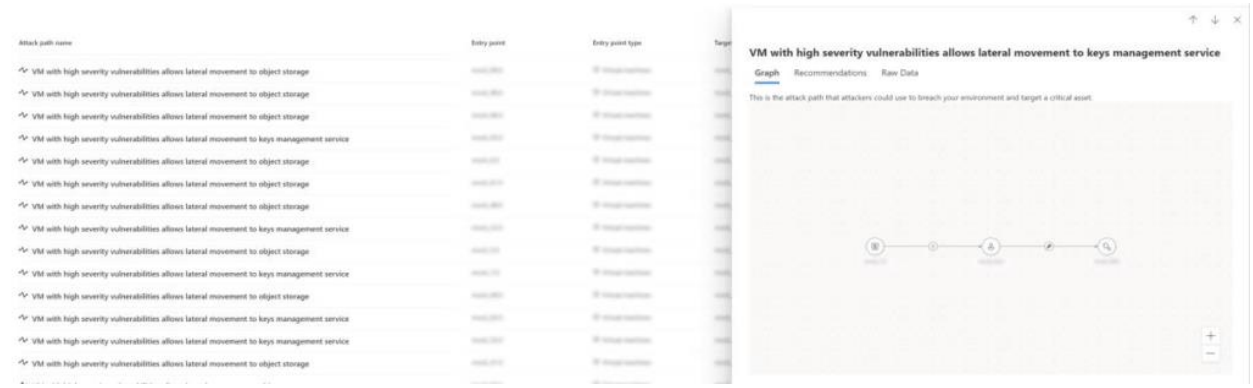
Provides recommendations: Belirlenen saldırı yollarını azaltmak için eyleme geçirilebilir öneriler sağlanır.

Gives visibility into choke points: Çözüm, birçok saldırı yolunun aktığı tıkanma noktalarını vurgular. Bu görünürlük, kullanıcıların ağdaki bu kritik noktaları güvence altına alarak birden fazla saldırı yolunu ele alarak azaltma çabalarını stratejik olarak odaklamalarını sağlamaktadır.

Attack surface -> Attack path ‘e gidelim.



Bir yan bölmede ilgili Grafik ve Önerileri görmek için herhangi birini seçebiliriz.



Yalnızca kritik varlıkları belirlemekle kalmayıp aynı zamanda bunları tehlikeye atabilecek tehditleri anlamak ve azaltmak için **Attack Path Management** benimseyerek kuruluşunuzun siber güvenlik direncini artırın.

Exposure Insights

Ortamlar, ekipler ve ürünler arasında güvenlik maruziyetini yönetmek, özellikle ilgili ürünlerin güvenlik ekiplerinin elde ettiği parçalı görünürlük nedeniyle telaşlı bir iştir. Exposure Insights, CISO, güvenlik karar vericileri, risk sahipleri ve güvenlik yöneticilerinin tüm kuruluş genelinde maruziyeti yönetmeleri için tek durak noktasıdır. Kurum genelinde güvenlik hijyenini ve maruz kalma yönetimini önceliklendirmek ve yönlendirmek için sürekli ve birleşik bir duruş gözetimi sağlar.

- Kurumsal güvenlik duruşunu en önemli girişimlere ayırır.
- Her bir girişimdeki temel exposure unsurlarını ölçmenize ve izlemenize olanak tanır.

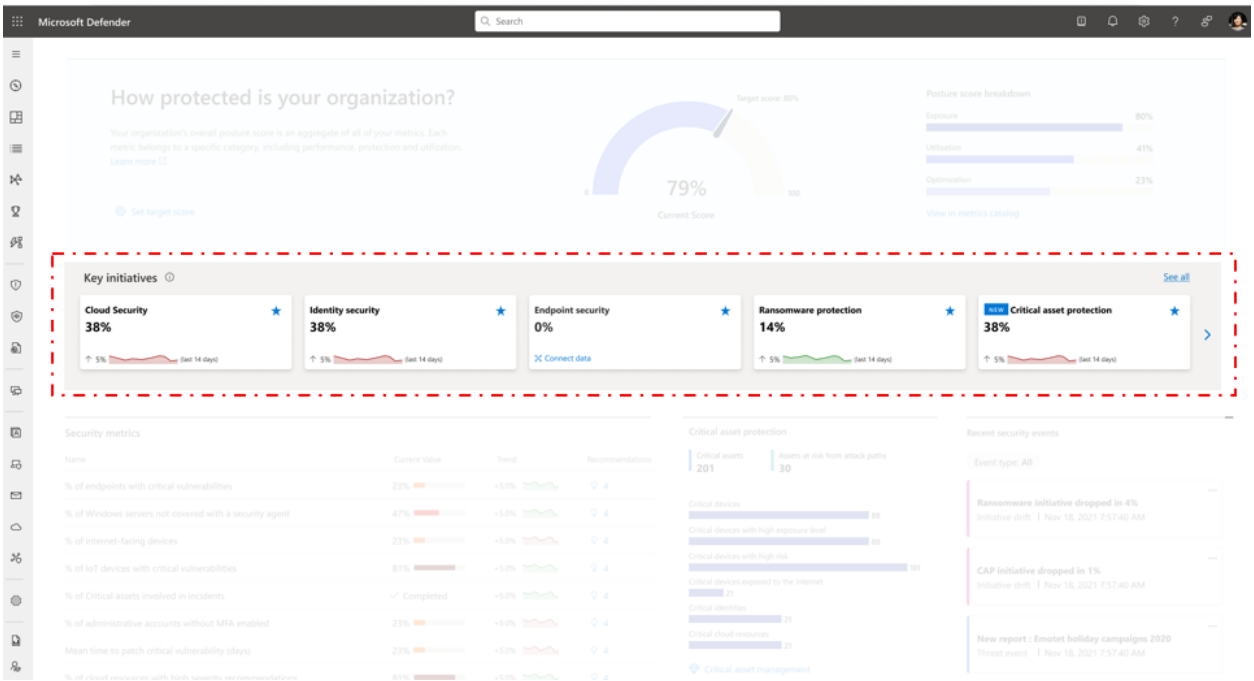
- Verilere ve iş bağlamına dayalı olarak odak alanlarını önceliklendirmektedir.
- Kurum genelinde riski azaltmak için eyleme geçirilebilir araçlar sağlamaktadır.

Security Initiavites

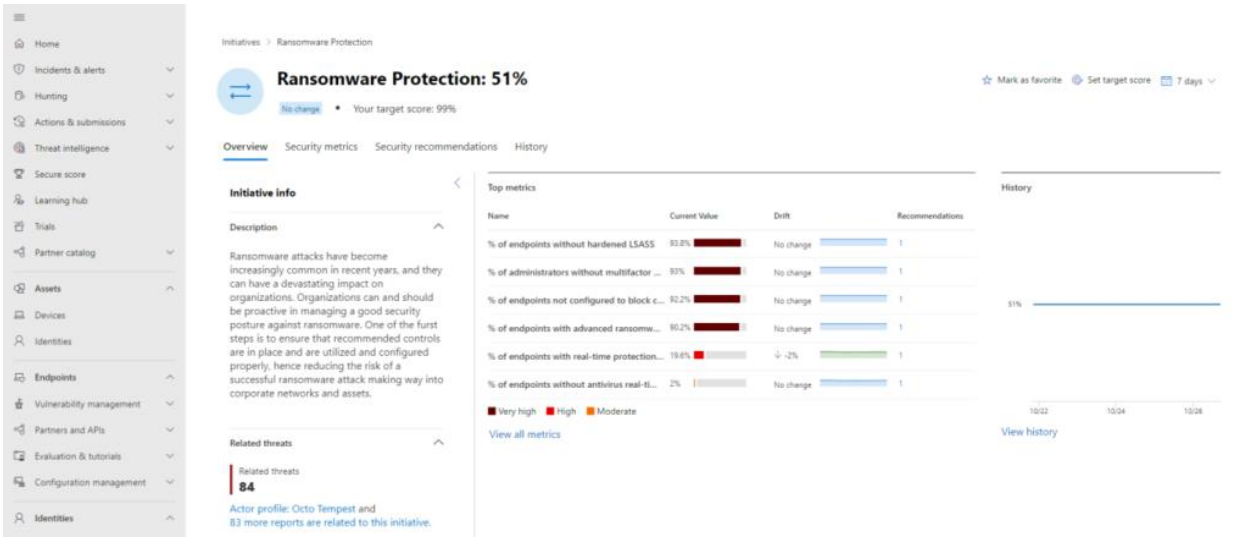
Maruziyet Yönetimi iki tür girişim arasında ayrım yapmaktadır.

Vertical initiatives: belirli bir ürün kategorisini veya türünü ele alan, genellikle kurumsal ve pazar tanımıyla uyumlu girişimler. Bu önizlemede yer alan ilk dikey girişimler Uç Nokta Güvenliği, Kimlik Güvenliği ve Bulut Güvenliğidir.

Horizontal initiatives: Birden fazla ürün kategorisini veya türünü kapsayan bilinen bir tehdidi veya paradigmayı ele alan girişimler. Bu önizlemede yer alan ilk yatay girişimler Ransomware Protection, Finansal Dolandırıcılık ve Critical Asset Protection 'dır.

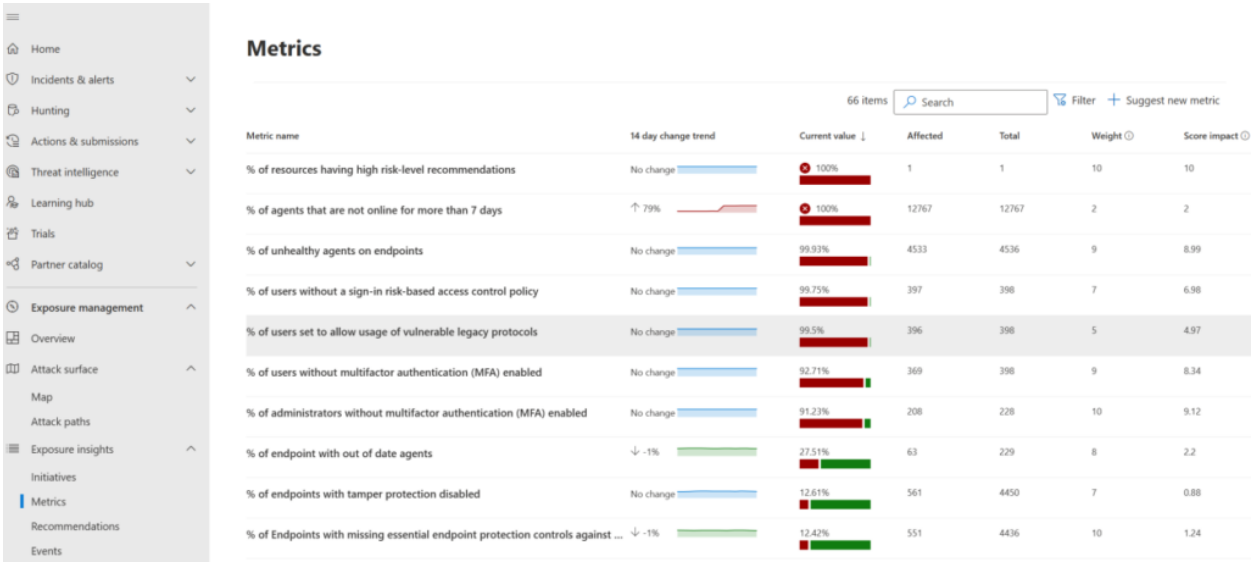


Bu intiativeler her birinin maruz kalma durumu, puanları aracılığıyla yansıtılır. Puan, girişimle ilişkili metriklere dayalı olarak hesaplanır. Kullanıcılar metriklerini iyileştirdikçe (çoğunlukla ilgili tavsiyeleri uygulayarak), girişim puanı yükselecek ve bu da söz konusu etki alanında daha iyi bir duruşu yansıtacaktır. Bir intiative'i seçerek o girişimle ilgili daha fazla ayrıntıya ulaşabilirsiniz.



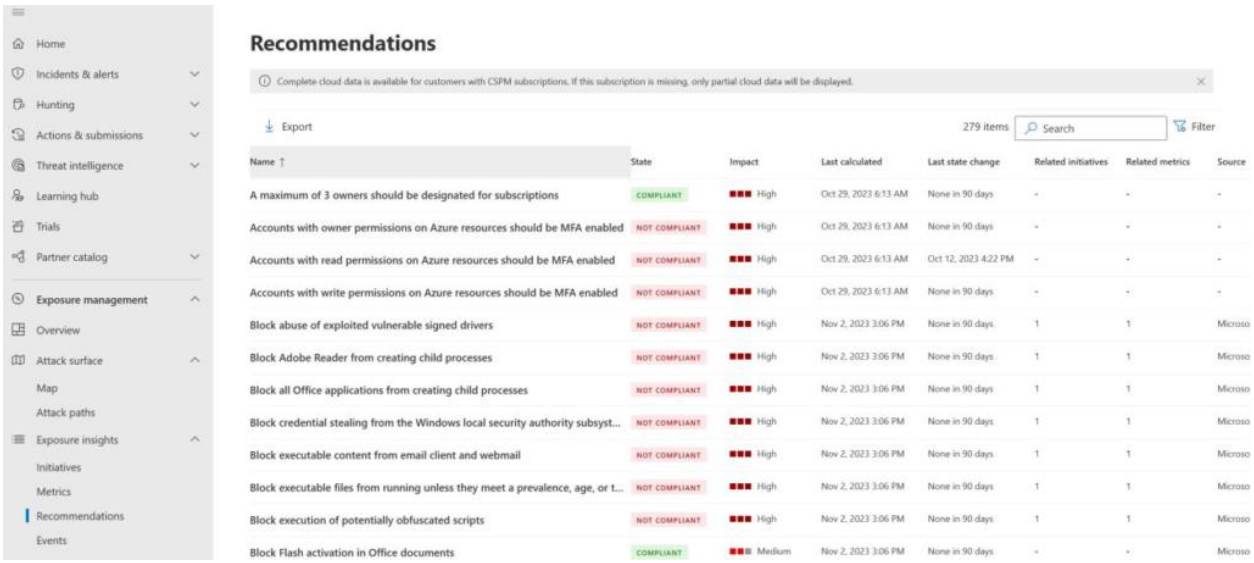
Security Metrics

Kullanıcıların bir girişimin maruz kalma durumunu değerlendirmesine ve maruz kalan veya iç standartları karşılamayan alanları belirlemesine olanak tanımaktadır. Bu bilgiler daha sonra hangi alanların öncelikle ele alınması gerektiğini önceliklendirmek için kullanılabilir.



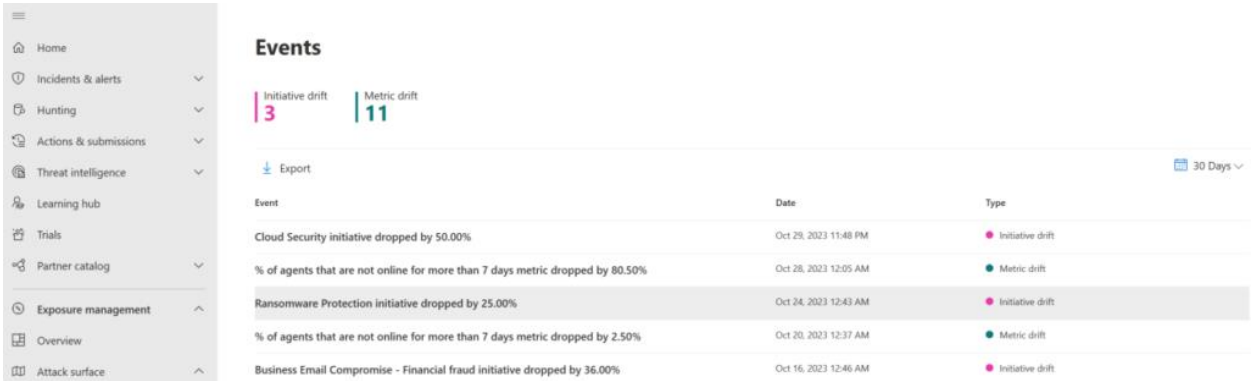
Security Recommendations

Bu çözümdeki öneri kataloğu, tüm kaynaklarını kapsayan Microsoft Secure Score ve Bulut için Microsoft Defender dahil olmak üzere farklı kaynaklardan gelen güvenlik önerileri için merkezi bir havuz görevi görür.



Security Events

'Security Events' özelliği, müşterilerimizi duruş yönetimi alanında tespit edilen her türlü değişiklik hakkında bilgilendirmek için tasarlanmıştır. Bu bilgiler, müşterilerin sağlam bir güvenlik duruşu sürdürmelerini sağlamak için ayarlamalar yapmalarına olanak tanıyacaktır.



Exposure Management , yukarıda bulunan bu iş yüklerinin maruziyet ve duruşla ilgili yönlerinin yerini almayacak. Bunun yerine, bunları birleşik bir görünümde birleştirerek maruz kalma, potansiyel saldırı yolları ve güvenlik programlarının olgunluğu hakkında içgörüler sunarak iş önceliklerini göz önünde bulundururken sürekli güvenlik duruşu iyileştirmesini sağlayacaktır.

Bir sonraki makalede görüşmek üzere.

Kaynak: **CCP Security Connection Program – Exposure Management Discussion**