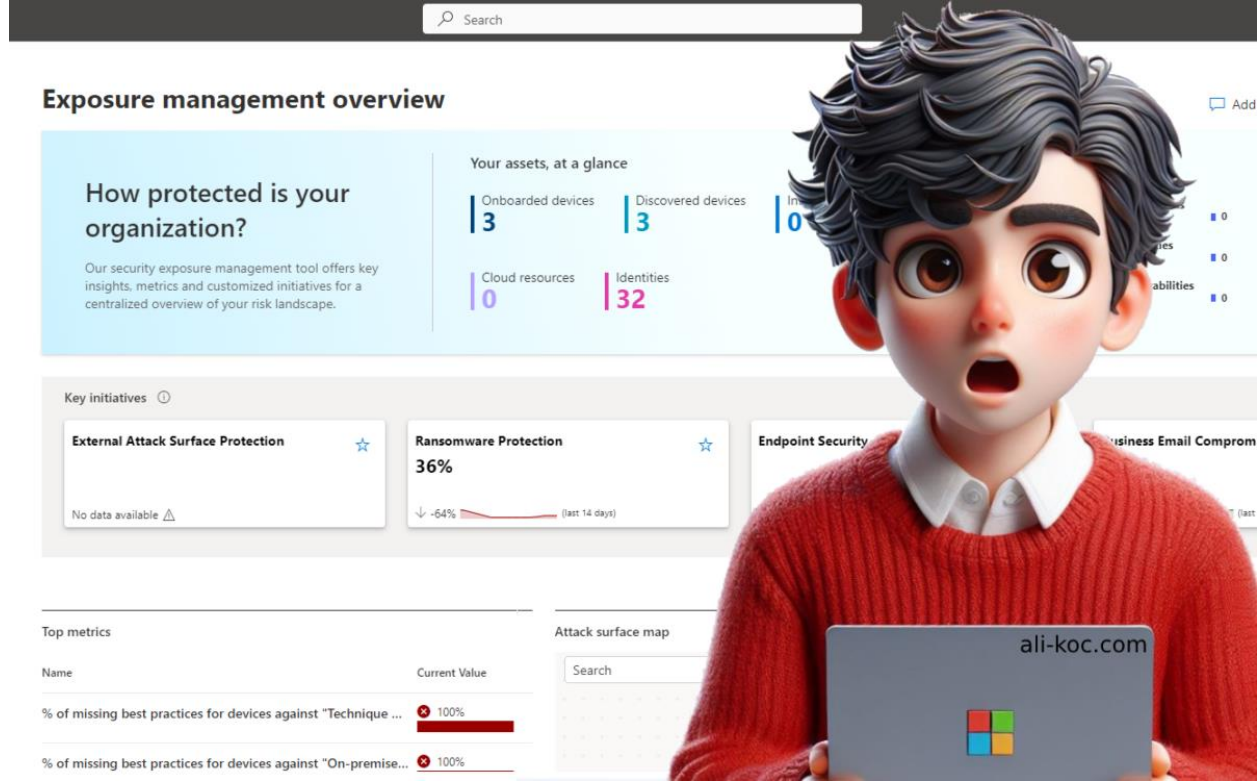


YAYINLANDI ! Exposure Management Genel Kullanıma Sunuldu



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 durumu 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.

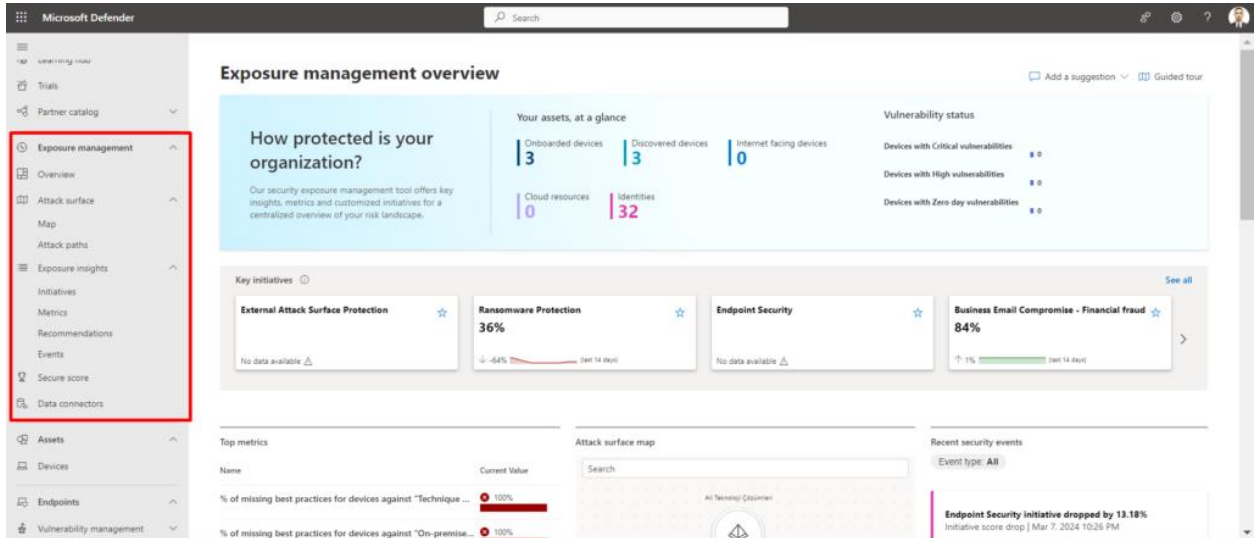
Drill-down capabilities: Güvenlik yöneticileri belirli güvenlik programlarını veya tehditleri inceleyerek o segmentte ne kadar maruz kaldıklarını görebilirler. Bu, düzeltme çabalarını iş bağlamına ve verilere dayalı olarak en büyük risk alanlarına odaklamalarına olanak tanır.

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.

Microsoft Defender

Settings > Microsoft Defender XDR

Search

Learning tour

Trials

Partner catalog

Exposure management

Overview

Attack surface

Map

Attack paths

Exposure insights

Initiatives

Metrics

Recommendations

Events

Secure score

Data connectors

Assets

Devices

Endpoints

Vulnerability management

Microsoft Defender XDR

General

Account

Email notifications

Alert service settings

Permissions and roles

Streaming API

Multi-tenant content source

Rules

Asset rule management

Alert tuning

Critical asset management

Automation

Identity automated response

How protected are your critical assets?

Gain insights and recommendations in the critical asset protection initiative.

Critical asset management

Manage the criticality level of your organization's assets, either according to predefined classifications or by creating your own custom ones.

Note While we employ behavior-based logic to automatically identify assets of interest, there may be instances where not all relevant assets are identified. To ensure comprehensive coverage, we encourage you to utilize our custom queries feature to proactively search for critical assets.

Create a new classification 46 items Suggest new classification Customize columns

Classification	Status	Assets	Criticality level	Created on	Updated on	Last run	...	Create...
Predefined classifications (46)								
Databases with sensitive data	On	0	High			Mar 13, 2024 4...	Microsoft	
Enterprise Admins	On	0	High			Mar 13, 2024 4...	Microsoft	
Domain Admin Workstations	On	0	High			Mar 13, 2024 4...	Microsoft	

Create critical asset classification > Create a critical asset classification

Create critical asset classification

Preview assets

Assign criticality

Review and finish

Create a critical asset classification

Create and define a critical asset classification for your assets, including devices, identities or cloud resources. By classifying specific types of assets, you'll be able to better manage and track them.

Name *

New classification

Description

Add a description for this classification

Query builder

☒ Device ☐ Identity ☐ Cloud resource

AND

Select a filter

+ Add filter + Add subgroup

Next

Cancel

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

Device Inventory

Manage critical assets
Classify and protect your most important assets

12 devices are involved in attack paths putting critical asset at risk...
Fix them now

Computers & mobile

Network devices

IoT devices

Total

Critical assets

High risk

High exposure

Not onboarded

12K

46

324

745

88

Export

12K items

Search

30 days

Choose columns

Manage tags

Filters

Filters: Critical asset: High

Device name	Domain	Risk level	Exposure level	OS platform	OS version	Criticality level	Device role	Onboarding status	Last device update	Seen by	Tags
sinmp001	Workgroup	Low	High	Windows	4.3.1	Critical - tier 0	Domain controller	Onboarded	2/3/20, 7:57 AM	ComputerPti_x00... +2	ATTN: MANAGER
ashfpa202	Workgroup	Low	High	Windows	4.3.1	Critical - tier 0	ADFS	Onboarded	2/3/20, 7:57 AM	ComputerPti_x00... +1	ATTN: MANAGER
ston101.network.com	domain.test.local	Low	High	Windows	4.3.1	Critical - tier 0	Exchange server	Onboarded	2/3/20, 7:57 AM	ComputerPti_x00... +5	ATTN: MANAGER

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.

Attack paths

Attack path

Choke points

Explore the potential attack paths that attackers could use to breach your environment, and which assets could be affected. [Learn more](#)

3182 items

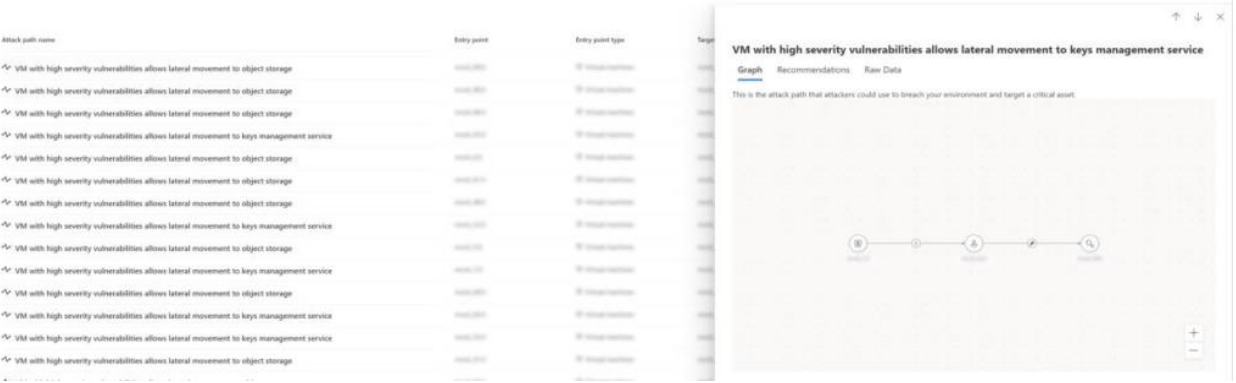
Customize columns

Export

Filters: Target type: Any

Attack path name	Entry point	Entry point type	Target	Target type	Target criticality	Affected assets	Recommendations
Device with high severity vulnerabilities allows lateral movement to domain controller	10.10.10.10	IP Address	10.10.10.10	IP Address	Critical	1	1
Device with high severity vulnerabilities allows lateral movement to identity	10.10.10.10	IP Address	10.10.10.10	IP Address	Critical	1	1
Device with high severity vulnerabilities allows lateral movement to domain controller	10.10.10.10	IP Address	10.10.10.10	IP Address	Critical	1	1
Device with high severity vulnerabilities allows lateral movement to identity	10.10.10.10	IP Address	10.10.10.10	IP Address	Critical	1	1
Device with high severity vulnerabilities allows lateral movement to identity	10.10.10.10	IP Address	10.10.10.10	IP Address	Critical	1	1
Device with high severity vulnerabilities allows lateral movement to identity	10.10.10.10	IP Address	10.10.10.10	IP Address	Critical	1	1
Device with high severity vulnerabilities allows lateral movement to identity	10.10.10.10	IP Address	10.10.10.10	IP Address	Critical	1	1
Device with high severity vulnerabilities allows lateral movement to identity	10.10.10.10	IP Address	10.10.10.10	IP Address	Critical	1	1
Device with high severity vulnerabilities allows lateral movement to identity	10.10.10.10	IP Address	10.10.10.10	IP Address	Critical	1	1
Device with high severity vulnerabilities allows lateral movement to identity	10.10.10.10	IP Address	10.10.10.10	IP Address	Critical	1	1
Device with high severity vulnerabilities allows lateral movement to identity	10.10.10.10	IP Address	10.10.10.10	IP Address	Critical	1	1
Device with high severity vulnerabilities allows lateral movement to identity	10.10.10.10	IP Address	10.10.10.10	IP Address	Critical	1	1

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.

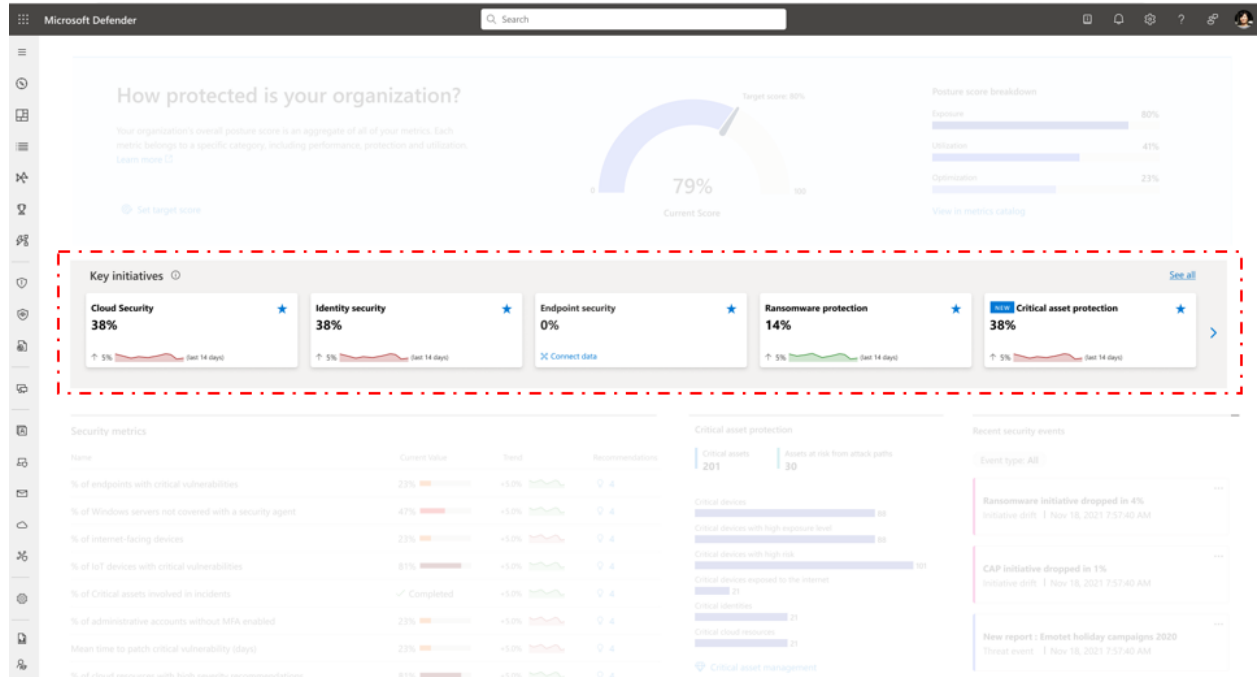
- Verilere ve iş bağlamına dayalı olarak odak alanlarını önceliklendirmektedir.
- Kurum genelinde riski azaltmak için eyleme geçirilebilir araçlar sağlamaktadır.

Security Initiatives

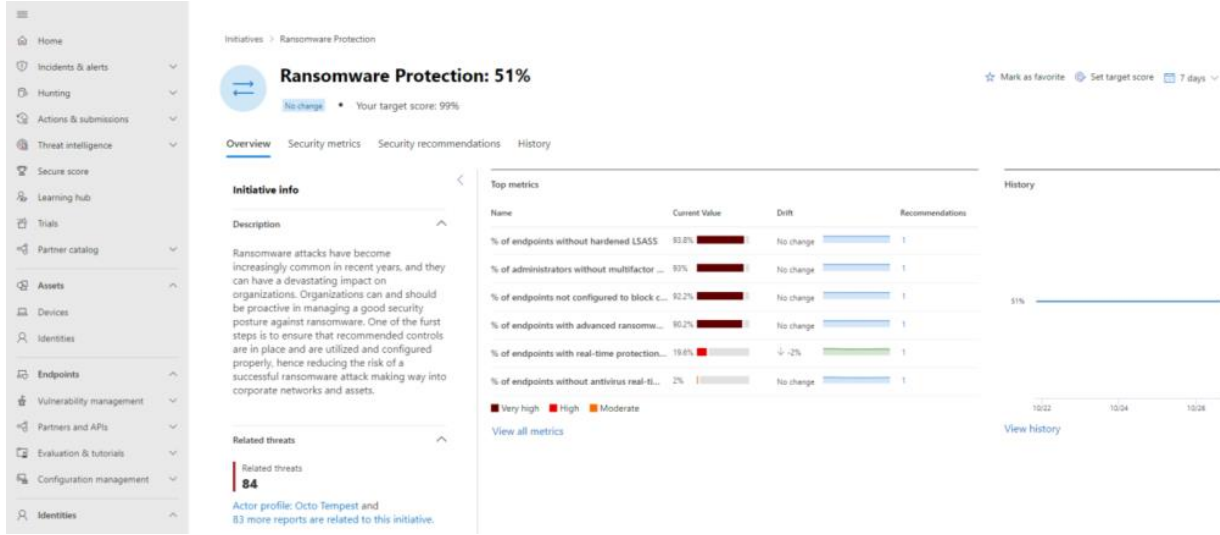
Maruziyet Yönetimi iki tür girişim arasında ayırım yapmaktadır.

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

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

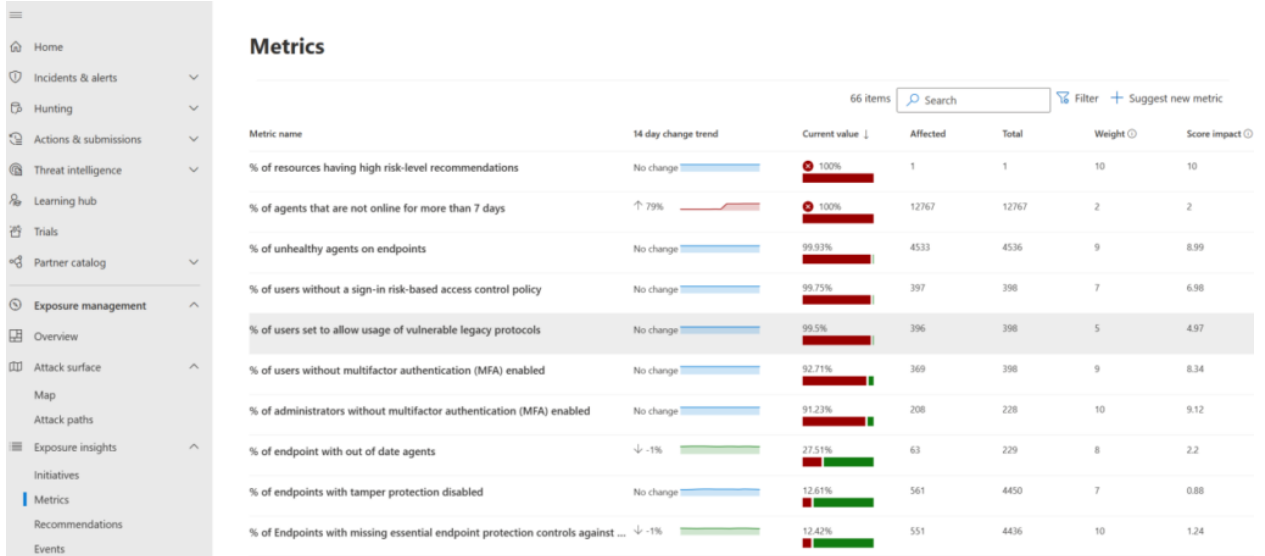


Bu intiativeler her birinin maruz kalma durumu, puanları aracılığıyla yansıtılır. Puan, girişimle ilişkili metriklerle dayalı olarak hesaplanır. Kullanıcılar metriklerini iyileştirdikçe (çoğunlukla ilgili tavsiyeleri uygulayarak), girişim puanı yükselecek ve bu da söz konusu etki alanında daha iyi bir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



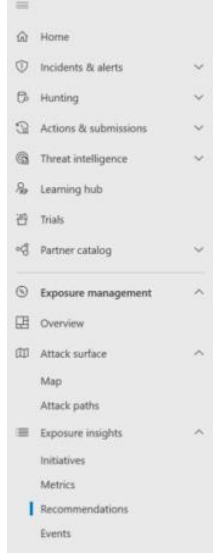
Security Metrics

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.



Recommendations

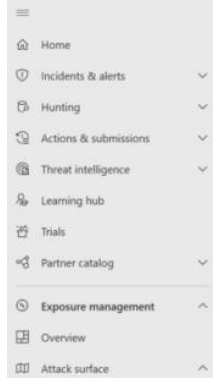
Complete cloud data is available for customers with CSPM subscriptions. If this subscription is missing, only partial cloud data will be displayed.

Export 279 items Search Filter

Name ↑	State	Impact	Last calculated	Last state change	Related initiatives	Related metrics	Source
A maximum of 3 owners should be designated for subscriptions	COMPLIANT	High	Oct 29, 2023 6:13 AM	None in 90 days	-	-	-
Accounts with owner permissions on Azure resources should be MFA enabled	NOT COMPLIANT	High	Oct 29, 2023 6:13 AM	None in 90 days	-	-	-
Accounts with read permissions on Azure resources should be MFA enabled	NOT COMPLIANT	High	Oct 29, 2023 6:13 AM	Oct 12, 2023 4:22 PM	-	-	-
Accounts with write permissions on Azure resources should be MFA enabled	NOT COMPLIANT	High	Oct 29, 2023 6:13 AM	None in 90 days	-	-	-
Block abuse of exploited vulnerable signed drivers	NOT COMPLIANT	High	Nov 2, 2023 3:06 PM	None in 90 days	1	1	Microso
Block Adobe Reader from creating child processes	NOT COMPLIANT	High	Nov 2, 2023 3:06 PM	None in 90 days	1	1	Microso
Block all Office applications from creating child processes	NOT COMPLIANT	High	Nov 2, 2023 3:06 PM	None in 90 days	1	1	Microso
Block credential stealing from the Windows local security authority subsystem	NOT COMPLIANT	High	Nov 2, 2023 3:06 PM	None in 90 days	1	1	Microso
Block executable content from email client and webmail	NOT COMPLIANT	High	Nov 2, 2023 3:06 PM	None in 90 days	1	1	Microso
Block executable files from running unless they meet a prevalence, age, or L...	NOT COMPLIANT	High	Nov 2, 2023 3:06 PM	None in 90 days	1	1	Microso
Block execution of potentially obfuscated scripts	NOT COMPLIANT	High	Nov 2, 2023 3:06 PM	None in 90 days	1	1	Microso
Block Flash activation in Office documents	COMPLIANT	Medium	Nov 2, 2023 3:06 PM	None in 90 days	-	-	Microso

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.



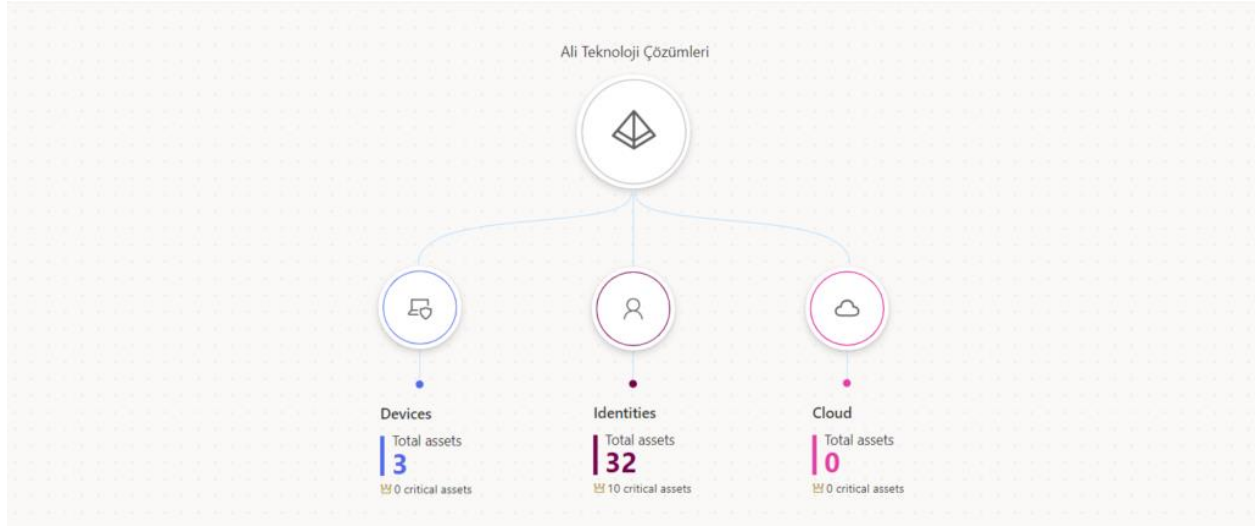
Events

Initiative drift 3 Metric drift 11

Export 30 Days

Event	Date	Type
Cloud Security initiative dropped by 50.00%	Oct 29, 2023 11:48 PM	Initiative drift
% of agents that are not online for more than 7 days metric dropped by 80.50%	Oct 28, 2023 12:05 AM	Metric drift
Ransomware Protection initiative dropped by 25.00%	Oct 24, 2023 12:43 AM	Initiative drift
% of agents that are not online for more than 7 days metric dropped by 2.50%	Oct 20, 2023 12:37 AM	Metric drift
Business Email Compromise - Financial fraud initiative dropped by 36.00%	Oct 16, 2023 12:46 AM	Initiative drift

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**