Bitdefender GravityZone, kaynak açısından verimli bir güvenlik çözümüdür.Merkezi yönetim, kolay dağıtım ve bulut veya şirket içinde barındırılan bir yönetim konsolu arasında seçim yapma özgürlüğü sunarken yüksek performans ve koruma sağlar.

GravityZone Business Security, küçük veya orta ölçekli, herhangi bir sayıdaki dosya sunucusunu, masaüstünü veya dizüstü bilgisayarını, fiziksel veya sanal makineleri kapsayan kuruluşları korumak için tasarlanmıştır. İş Güvenliği, kanıtlanmış makine öğrenme teknikleri, davranış analizi ve çalışan süreçlerin sürekli izlenmesi ile endüstrinin en iyi önleme, algılama ve engelleme yeteneklerine sahip katmanlı bir sonraki gen son nokta koruma platformuna dayanmaktadır.

"En İyi Performans" ve "En İyi Koruma" kombinasyonu, 2017 boyunca prestijli AV-TEST tarafından gerçekleştirilen altı testin hepsinde bu kategorilerde en iyi skoru olan Bitdefender'a özgüdür.

TEMEL ÖZELLİKLER

Machine Learning Anti-Malware

Makine öğrenme teknikleri, gelişmiş saldırıları tahmin etmek ve engellemek için iyi eğitimli makine modelleri ve algoritmalar kullanır. Bitdefender'ın makine öğrenim modelleri 40.000 statik ve dinamik özellik kullanmaktadır ve dünya çapında 500 milyondan fazla uçtan toplanan milyarlarca temiz ve kötü niyetli örnek üzerinde sürekli olarak eğitilmektedir. Bu, kötü amaçlı yazılım tespitinin etkinliğini önemli ölçüde artırır ve yanlış pozitifleri en aza indirir.

Proses Inspector

Process Inspector, işletim sisteminde çalışan tüm süreçleri sürekli olarak izleyerek sıfır güven modunda çalışır. Şüpheli faaliyetler veya süreç türünü gizleme girişimleri, başka bir işlemin alanında kod yürütme (ayrıcalık yükseltme için işlem belleğini kaçırma), çoğaltma, bırakma, işlem sayım uygulamalarından gizleme ve daha fazlası gibi, anormal işlem davranışları için avlanır. Süreç sonlandırma ve yapılan işlemi geri alma değişiklikleri de dahil olmak üzere uygun iyileştirme eylemlerini gerçekleştirir. Ransomware dahil olmak üzere, bilinmeyen gelişmiş kötü amaçlı yazılımları tespit etmede oldukça etkilidir.

Advanced anti-Exploit

Exploit önleme teknolojisi, tarayıcıları, belge okuyucularını, medya dosyalarını ve çalışma zamanlarını (örn. Flash, Java) hafızayı ve savunmasız uygulamaları korur. Gelişmiş mekanizmalar, API aralama doğrulaması, stack pivot, return-oriented-programming (ROP) ve diğerleri gibi istismar tekniklerinin algılanması ve engellenmesi için bellek erişim rutinlerini izler. GravityZone'un teknolojisi, saldırıları hedef alan bir altyapıya sızmak için kullandığı gelişmiş ve kaçak sömürüleri ele almak için donatılmıştır.

Endpoint Control and Hardening

Policy tabanlı uç nokta denetimleri arasında güvenlik duvarı, USB taramasıyla aygıt denetimi ve URL sınıflandırmasıyla web içeriği kontrolü bulunur.

Anti-Phishing and Web Security Filtering

Web Güvenliği filtrelemesi, kötü amaçlı yazılımın uç noktaya indirilmesini önlemek için SSL, http ve https trafik dahil olmak üzere gelen web trafiğinin gerçek zamanlı olarak taranmasını sağlar. Kimlik avı koruması, kimlik avı ve dolandırıcı web sayfalarını otomatik olarak engeller.

Full Disk Encryption

GravityZone-full disk encryption, işletim sistemlerinde yerleşik teknolojiden yararlanarak, Windows BitLocker ve Mac FileVault kullanır. GravityZone Bussiness Security bu ikisini de kapsar ve Add-On key olarak satın alınır.

Patch Management

Güncellenmeyen sistemler, kuruluşları kötü amaçlı yazılım olaylarına, salgınlara ve veri ihlallerine maruz bırakır. GravityZone Patch Management, işletim sisteminizi, fiziksel sunucularınızı ve sanal sunucularınızı tüm işletim sistemi ve işletim sisteminizde güncel tutmanıza yardımcı olur GravityZone Bussiness Security bu ikisini de kapsar ve Add-On key olarak satın alınır.

Response and Containment

GravityZone piyasadaki en iyi temizleme teknolojisini sunar. Tehditleri otomatik olarak engeller / içerir, kötü amaçlı işlemleri öldürür ve değişiklikleri geri alır.

Ransomware Protection

Çözüm, dünya çapında 500 milyondan fazla uç noktadan 1 trilyon numune temel alınarak eğitilmiştir. Kötü amaçlı yazılım veya Ransomware yazılımı ne kadar değiştirilirse değiştirilsin, Bitdefender, hem çalıştırma öncesi hem de çalışma zamanı modunda yeni fidye yazılım modellerini doğru şekilde algılayabilir.

Largest Security Intelligence Cloud

500 milyondan fazla makine korumalı Bitdefender Küresel Koruyucu Ağ günde 11 milyar sorgu gerçekleştirir ve kullanıcıları yavaşlatmadan tehditleri tespit etmek için makine öğrenimi ve olay korelasyonunu kullanır.

Automate Threat Remediation and Response

Bir tehdit tespit edildikten sonra, GravityZone BS, süreci sonlandırma, karantina, kötü amaçlı değişikliklerin kaldırılması ve geri alınması gibi işlemlerle anında etkisiz hale getirir. Dünya çapında benzer saldırıları önlemek için, GPN, Bitdefender'in bulut tabanlı tehdit istihbarat servisi ile tehdit bilgilerini gerçek zamanlı olarak paylaşır.

GravityZone Business Security, kanıtlanmış makine öğrenme teknikleri, davranış analizi ve çalışan süreçlerin sürekli izlenmesi ile endüstrinin en iyi önleme, algılama ve engelleme özelliklerine sahip katmanlı next-gen endpoint koruma platformuna dayanmaktadır.

GravityZone Control Center

GravityZone Kontrol Merkezi, tüm güvenlik yönetimi bileşenleri için tek bir pencere görünümü sağlayan entegre ve merkezi bir yönetim konsoludur. Lokal olarak veya bulut olarak dağıtılabilir. GravityZone yönetim merkezi birden fazla rol içerir ve veritabanı sunucusu, iletişim sunucusu, güncelleme sunucusu ve web konsolu içerir.

AVANTAJLAR

Tek Ajan ve Entegre Konsol ile Operasyonel Verimliliği Artırın

Bitdefender'ın tek ve entegre uç nokta güvenlik ajanı, ajan yorgunluğunu ortadan kaldırıyor. Modüler tasarım maksimum esneklik sunar ve yöneticilerin güvenlik politikaları belirlemesine izin verir. GravityZone, yükleme paketini otomatik olarak özelleştirir ve ajan footprinti en aza indirir. Sanallaştırma sonrası ve bulut sonrası güvenlik mimarileri için temelden tasarlanan GravityZone, fiziksel, sanallaştırılmış ve bulut ortamlarını korumak için birleşik bir güvenlik yönetimi platformu sunar

• Güçlü ama basit bir çözüm uygulayın ve özel sunucular, bakım veya daha fazla BT personeli için ihtiyacı ortadan kaldırın

• Sağlanan güvenlik ilkesi şablonları ile daha hızlı başlayın

• Merkezi yönetim

• Az sayıda kullanıcı için daha düşük maliyetler ve merkezi güvenlik

• Merkezi yönetim sayesinde, çalışanlar güvenliği bir daha güncellememeli, izlememeli veya gidermemelidir ve işin %100'üne odaklanabilir.

• Basit uzaktan dağıtım

• Ayrıntılı raporlar, Gelişmiş yöneticiler için ayrıntılı politika ayarları kullanılabilir, ancak BT arka planı olmayanlar da yönetimi basit bir şekilde bulabilir

• Güncellemeler otomatiktir ve kullanıcılar ayarlara müdahale edemez veya korumayı devre dışı bırakamaz, böylece işletmeniz korunur

• Politikaları yere veya kullanıcıya göre uygulamak ve farklı özgürlük seviyelerine izin vermek; Önceden oluşturulmuş olanları kullanarak yeni politikalar oluştururken zamandan tasarruf edin.