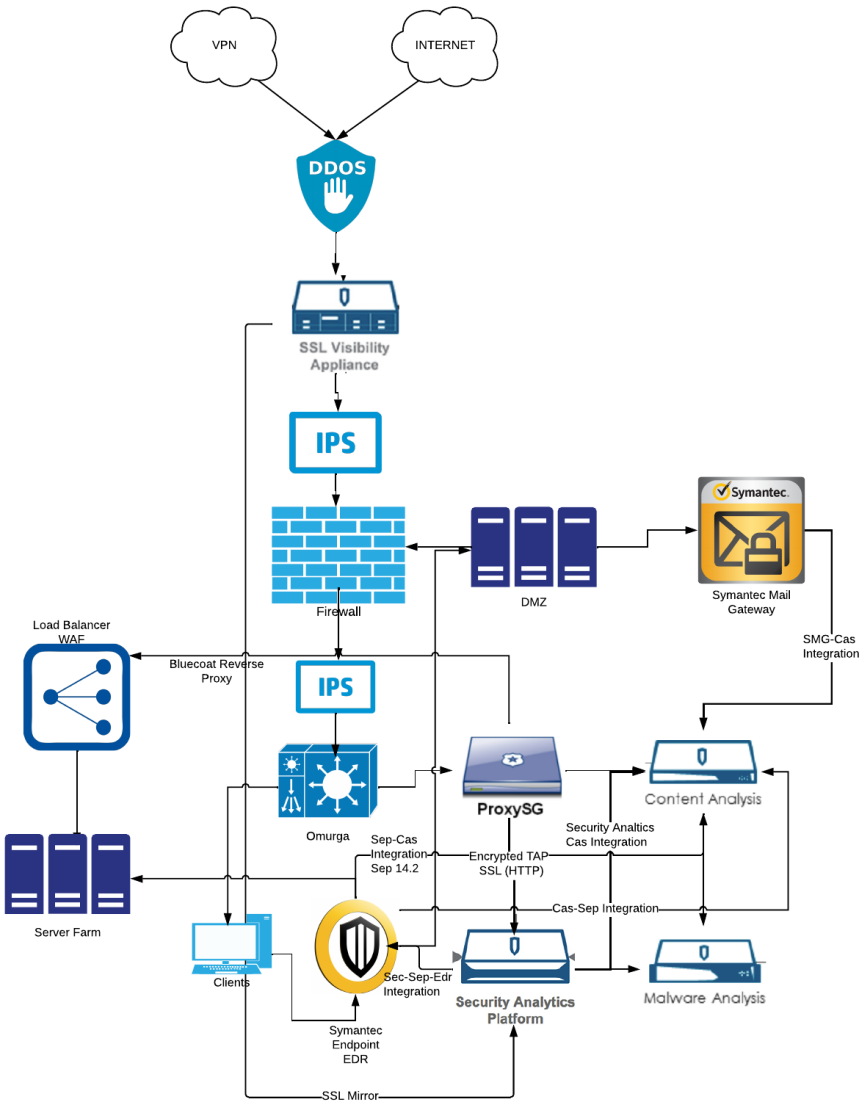
Symantec Endpoint ve Network Security
Genel Değerlendirme

1. Yönetici Özeti

Symantec Network Security ürünlerinin kabiliyetleri ve çalışma prensipleri de göz önüne alındığında, çok geniş bir vektörde (mail, web, network) koruma ve görünürlük sağladığını söyleyebiliriz. Bu konudaki daha fazla bilgiyi Network Security Teknolojilerinin anlatıldığı dökümanımızdan da elde edebilirsiniz.

2. Önerilen Topoloji



Symantec Network Mantıksal Topoloji Önerisi

2.1. ProxySG

Bluecoat ProxySg Proxy olarak birçok metodu desteklemektedir. Bu teknolojilerin detaylarına aşağıda detaylı olarak açıklanmaktadır.

Flow modda çalışan herhangi bir url filter ürünü ile Proxy teknolojisi karıştırılmamalıdır. Proxy eski bir teknoloji olmamakla birlikte, bir ihtiyaç özelinde ortaya çıkan bir teknolojidir. Session'a hükmetmediğimiz sürece onu kontrol etmekte zorlanırız. Bu da session'ı bir yerde sonlandırmayla mümkün olabilir ki bu da Proxy teknolojisi ile mümkündür. Bu konuda teknoloji ayrıntılarını içeren makalemizi ayrıca okumanızı tavsiye edeceğiz.

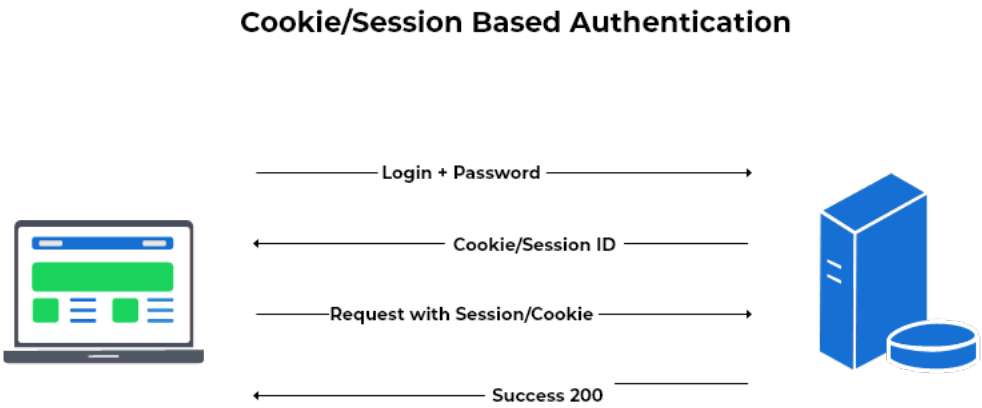
a. Forward Proxy

Forward proxy genel olarak Url filter olarak bilinir ancak bunun dışında güvenlik olarak kattığı birçok özellik bulunmaktadır.

- Authentication

ProxySg session base authentication yapar. Teknik olarak her bir kullanıcı hareketi ayrıca authanticate edilir.

Klasik agent base sistemlerde genelde bir agent kurulur ve kullanıcı logon bilgisi Active Directory'den çekilir. Bu eski ve güvenlik açısından zayıf bir yöntemdir.



Kullanıcı bilgisayarına bir zararlı bulaştığı veya isteğin direk olarak kullanıcı tarafından yapılmadığı durumda, ProxySG bu session a izin vermez. Bu da güvenlik kriteri olarak çok kritik bir durumdur. Flow base olarak çalışan sistemler veya ldap ile kullanıcıyı authanticate eden sistemlerde bu yapılamaz.

Bunun yanında aşağıdaki tüm metodları da desteklemektedir

auto form-cookie form-cookie-redirect form-ip form-ip-redirect proxy proxy-ip origin origin-ip origin-cookie origin-cookie-redirect origin-ip-redirect sg2	

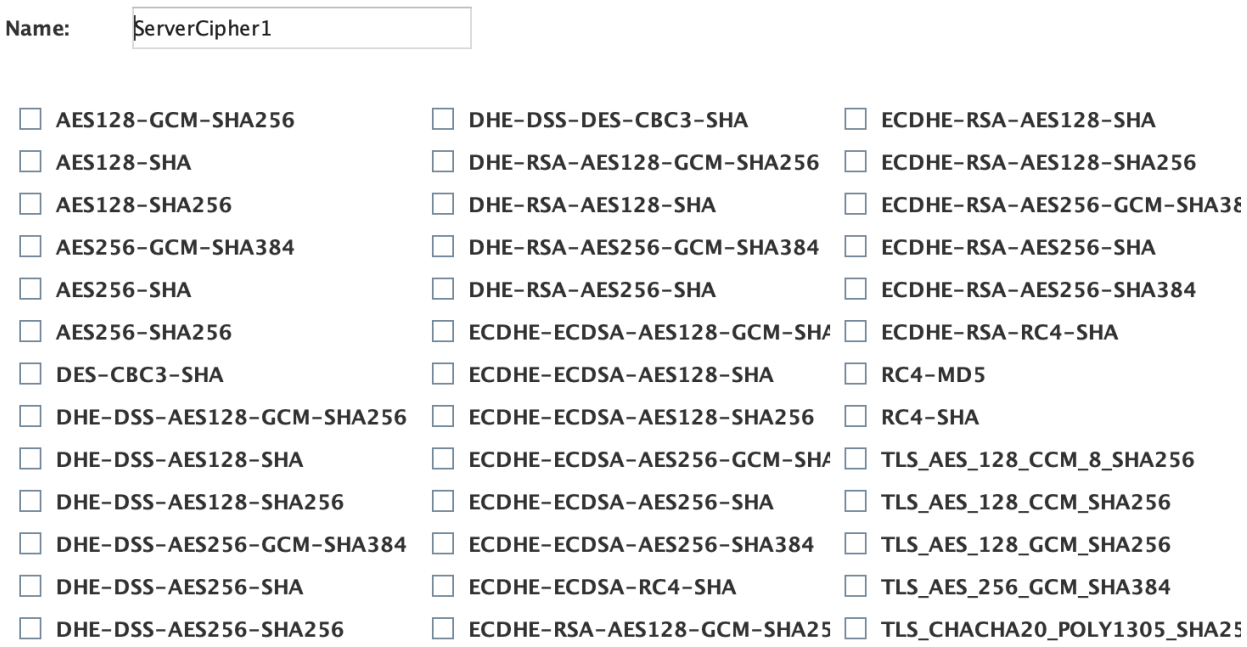
- SSL Inspection

SSL/TLS trafiği çözülmediği durumda, bu vektörden gelebilecek hiçbir tehdit veya yetkisiz paylaşımın kontrolü mümkün olmamaktadır.

ProxySg, one arm, transparent inline, pbr, wccp gibi tüm metodları destekler.

TLS1.3 dahil, neredeyse tüm ciphersuite destekleri mevcuttur.

Gloabal olarak TLS1.3 kapatmadan, TLS versiyon downgrade etmeden, her bir site ve ip için bile ayrı ayrı cipher dahi seçilebilir.



Bunun yanında sertifika verify edemese de ssl bypass kuralı yazılmadan, ssl inspection'a devam edilmesi mümkündür. Self-sign veya expire eden sertifikalarda da ssl inspection yapılabilir.

Çözülen ssl trafiğin bir kopyasının da adli amaçlar için kayıt edilmesi için, bu cihazlardan trafiğin çözülmüş bir kopyası da alınmak zorundadır.

Çözülemeyen, istemci tarafından gerçekleştirilmeyen her türlü trafik bloklanmalıdır, bu özellik mutlaka aktif olmalıdır.

b. Reverse Proxy

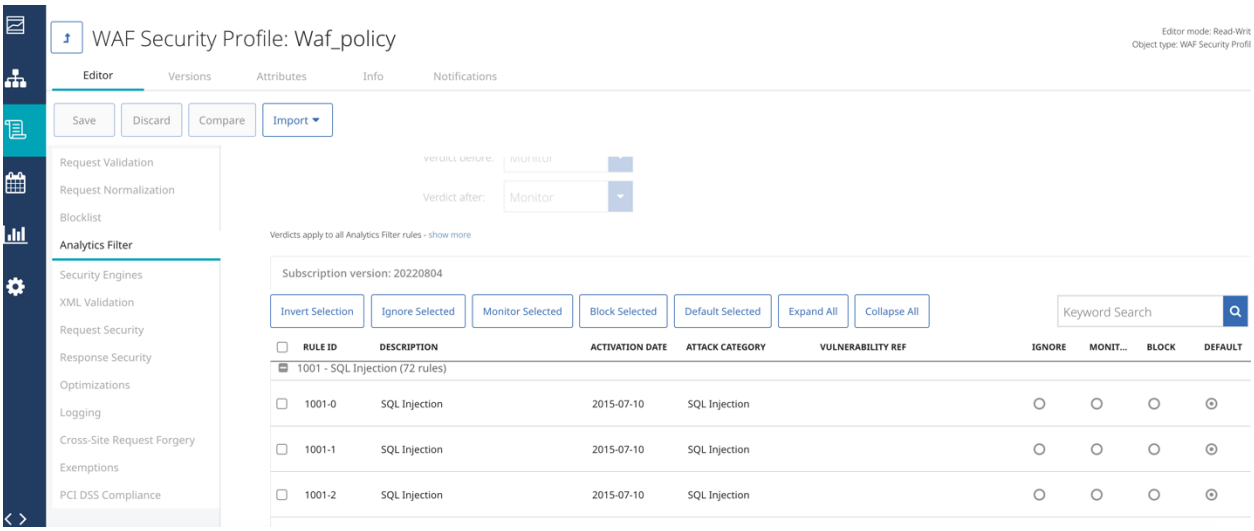
Fwd Proxy dışında Reverse Proxy özelliği de bulunmaktadır.

Sunuculara dışarıdan gelen bağlantılar, Reverse proxy üzerinden geçerken, post edilen dosyalar da içerik analizi yapılmak için Content Analysis cihazına veya icap ile herhangi bir Av. Gw e yollanabilir.

Bu durumun bir diğer avantajı, dosyalar uzantısına göre değil, gerçek özelliklerine göre ayırt edilir, session cihaz üzerinde sonlandığından bypass edilemez, analiz sonucuna göre sunucuya erişme izni verilir veya verilmez.

Reverse proxy altında 3 temel özellik barındırmaktadır.

Bunlardan biri waf yeteneğidir.

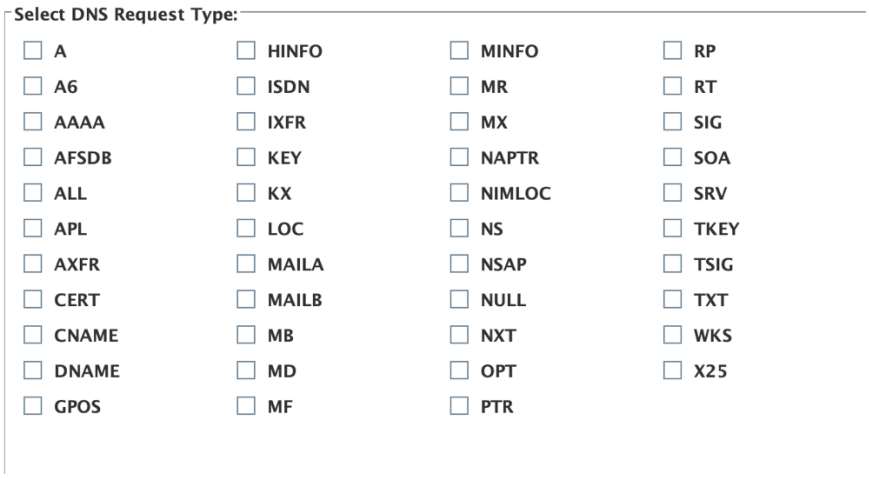


Bu sayede sunuculara gelen web base ataklar bu kısımda kolayca kesilir.

Bir diğeri basit load balancer yetenekleridir. Sonlanan sunucu aynı LTM cihazlarında olduğu gibi arkada birden fazla uygulama sunucusu varsa bu trafik bu cihaz üzerinde de load balance edilebilir.

En önemli kısımlardan biri de Dns Proxy dir.

Dns Proxy sayesinde istenmeyen dns sorguları engellenir, dns tünelleme protokol bazlı kesilir. İmza bağımsız olduğundan atlatılma durumu olmaz.



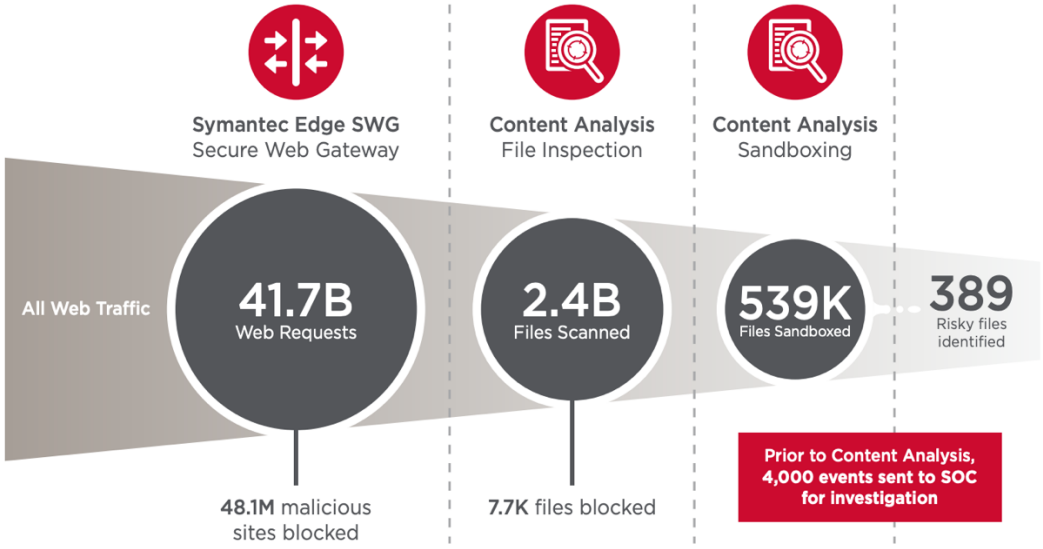
Ülke, type, response, dns over https üzerinden gelen isteklere her bir site bazlı kural bile yazılabilir. Zararlı dns isteklere cevap dönmeyebilir.

2.2. Content Analysis (Av Gateway- Sandbox)

Icap entegrasyonuna açıktır. ICAP konuşabilen herhangi bir Sandbox, Dlp, Antivirüs Gw ile direk konuşabilir. Eş zamanlı API desteği sayesinde Symantec Mail Gw(SMG) ve 3rd party herhangi bir cihaz ile entegre olabilir. Eğer 3rd party cihazın desteği yoksa

Antivirus	
☐	Symantec
☐	Kaspersky Labs
☐	McAfee, Inc.
☐	Sophos, Plc.
☐	ClamAV

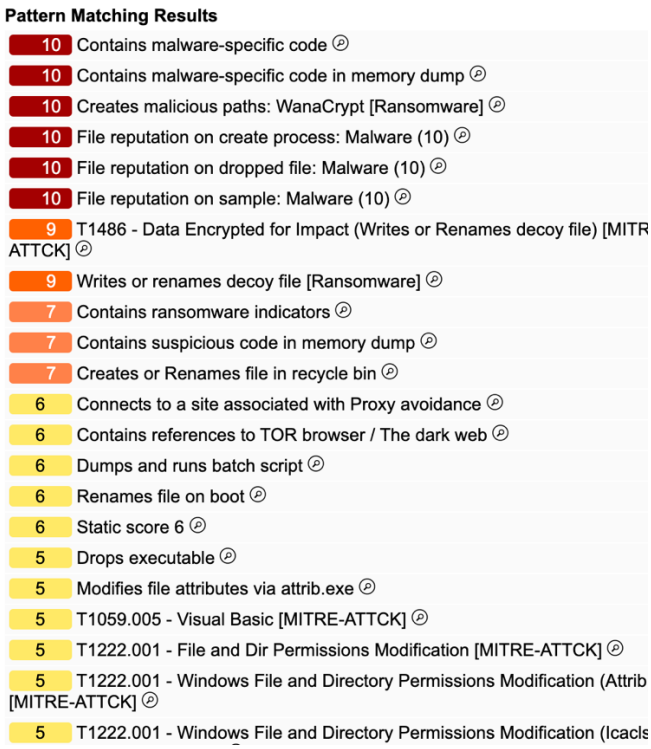
Sahip olunan lisanslara göre belli antivirüs üreticilerinin veri taban ve av ozellikleri de kullanılarak dosyalar gateway seviyesinde taranır. Bunun yanında Symantec File Reputation ve Symantec Advance Machine özellikleri bulunmaktadır.



Trafik, yine bu cihaz üzerinde çalışan sandbox'a gelmeden önce yukarda belirtilen kontrollerden geçirilir ve zararlı tespit edilen dosyalar, sandbox'a gelmeden önce engellenir. Bu sayede sandbox'a çok az dosya gelir ve bu dosyalar analiz edilir.

Sandbox tarafında Emulation ve Simulation eş zamanlı çalışır. Emulation analiz süresi 1 sn civarındadır, Simulation süresi de ortalama 20-25 sn gibi bir süreye denk gelir.
Sandbox tarafında;

- İşletim sistemi özelleştirilebilir
- Her türlü uzantı analiz edilebilir.
- Static ve Davranışşal dosya analizi yapılır.
- YARA kuralları işletilir, özelleştirilebilir.
- Emulasyon ve Simulasyon her iki metod desteklenir.
- Memory Exploit Detection özelliği vardır.
- Ghost Plugin ile Kullanıcı davranışları simüle edilebilir.
- Pattern'ler otomatik olarak güncellenir ve kullanıcı kendi patternini oluşturabilir.

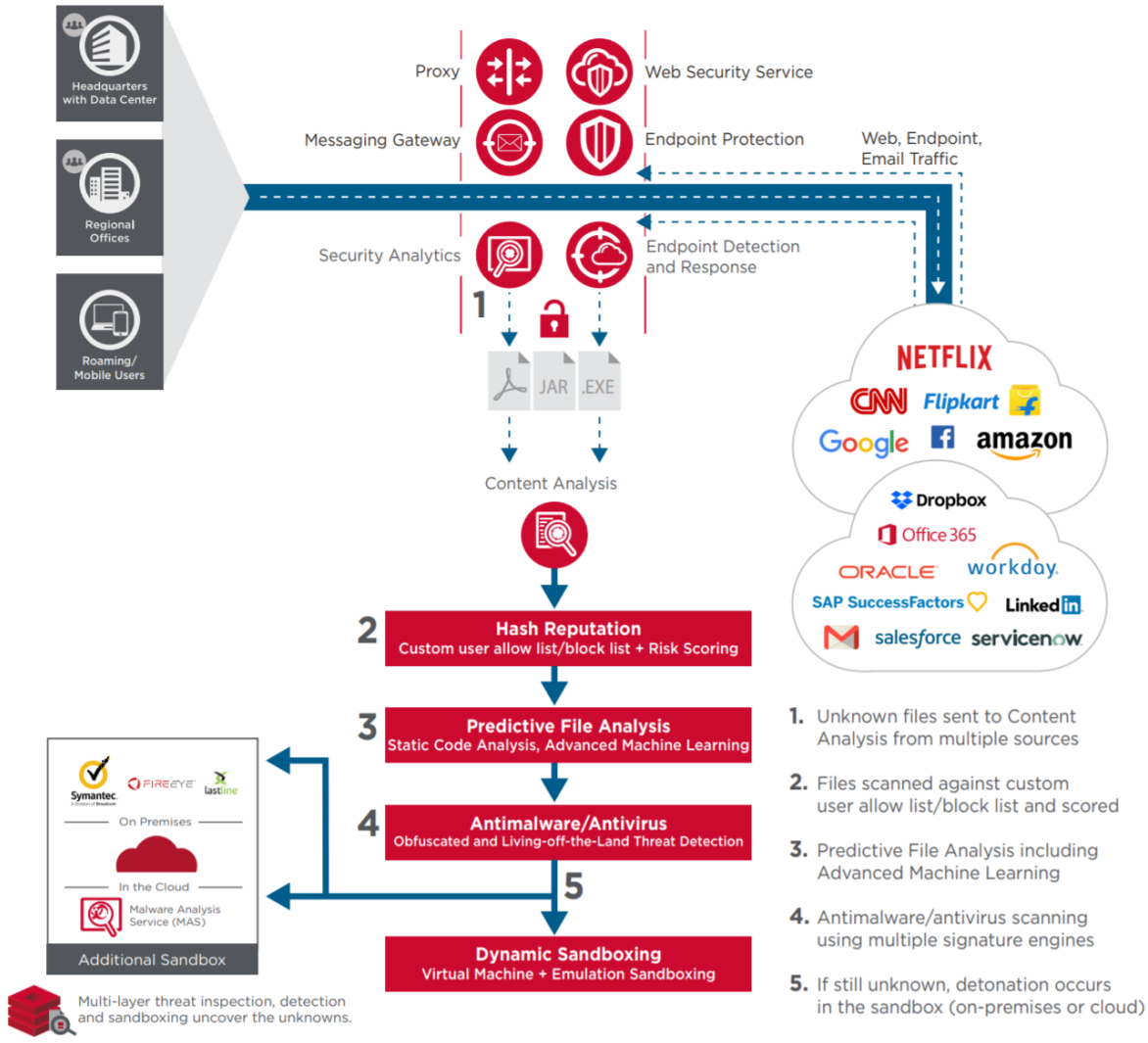


İlgili dosya hangi pattern'e match ettiyse bu ayrıntılı şekilde yer alır, istenirse bu skorlar kullanıcı tarafından değiştirilebilir.

Fireey Nx, Ax, Lastline sandbox ile native entegrasyonu mevcuttur. Api ve Icap ile konuşabilen her ürünle konuşabilir.

Symantec Endpoint ve Edr tarafında da sistem kullanılabilir durumdadır.

Ayrıca Symantec Security Analytics (Network Forensic) ile native entegrasyonu da vardır.



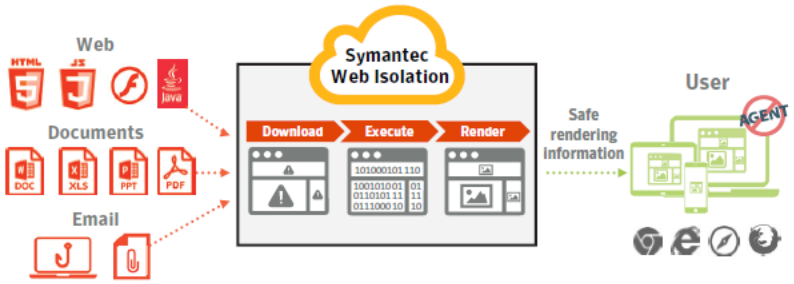
Proxy, Mail Gw, EDR, Endpoint, Security Analytics tarafından ortak olarak kullanılan Content Analysis modülü özetlemek gerekirse;

- Dosyalar buraya Proxy Sg, Mail Gw, tarafından clear text gelir.
- 2-3-4 adımlarından geçtikten sonra tanımlanamayan dosyalar Sandbox modülüne iletilir.
- Sandbox modülü olarak Fireeye ve Lastline da kullanılabilir.
- ProxySg Ve Mail Gw den gelen dosyaların sonucu gelene kadar dosya bu cihazlar tarafından tutulur ve kullanıcıya analiz edilmeden iletilmez. (İlk tehdit bloklanır.)
- Https session ProxySg tarafından çözüldüğünden ilk tehditin bloklanma senaryosu Fireeye ve Lastline ile de olanaklı hale gelir.
- Edr ve Security Analytics tarafından gönderilen dosyalar da burada aynı metodolojide analiz edilir.

2.3. Web Isolation (Cloud Base)

Web Isolation teknolojisi temel olarak ilgili dosyaların ve erişimlerin başka bir sistemde çalıştırılması ve ilgili görüntünün aktarılması esasına dayanır.

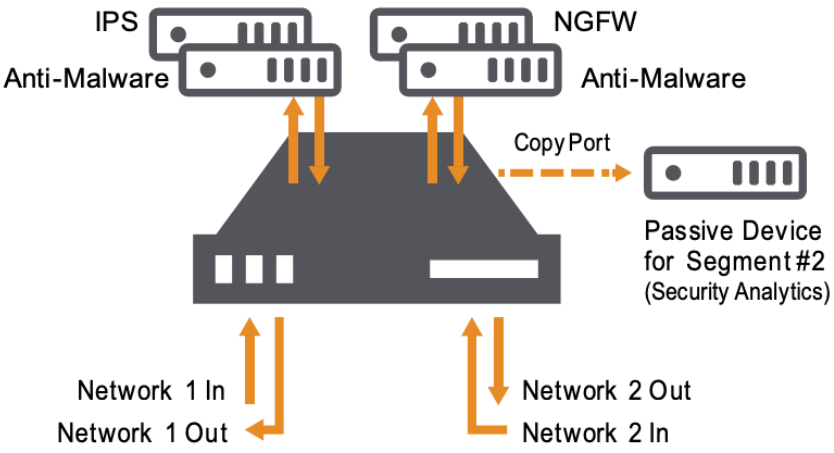
Özetle bilgisayara herhangi bir uygulama yüklenmeden, tamamen ajan bağımsız olarak, riskli içeriklere, temiz bir erişim sağlar.



Tüm erişimler buraya yollanmaz, sadece riskli gözüken erişimler bu kısma aktarılabilir. Bilgisayarda herhangi bir kod çalışmadığından, direk olarak bir şeyin sisteme bu kanalla bulaşmasının da önüne geçilmiş olur.

2.4. Symantec SSL Visibility

Symantec SSL Visibility ürünü inbound(simetrik) ve outbound(asimetrik) ssl trafiğinizi çözerek, ilgili trafiğin cleartext olarak güvenlik ürünleri tarafından analiz edilmesini sağlar.



Symantec SSL Visibility tamamen full transparent Layer2 olarak çalışır. Trafik herhangi bir cihazda değişikliğe uğradığında, bu session'ı otomatik olarak sonlandırır. Cihaz session bütünlüğünü kontrol eder.

Session bütünlüğünün kontrol edilmediği durumda bu cihazların kullanılması anlamsız kalmaktadır.

Packet Broker teknolojileri ile genelde birlikte kullanılır. Bunun en büyük nedeni trafiğin network'e dahil olmadan önce analiz edilip zararlı trafiğin burada engellenmesi, bir diğeri de belli trafik tiplerinde arada olan IPS, WAF gibi cihazların komple bypass edilebilir olması, bu tarafta ciddi bir şekilde yönetilebilir esneklik sağlamakla birlikte, bu durumun network güvenliği tarafında belli problemlere de neden olmaktadır. Bu konudaki ayrıntılı bilgiye teknoloji makalemizden erişilebilir.

2.5. Symantec Security Analytics (Network Forensic)

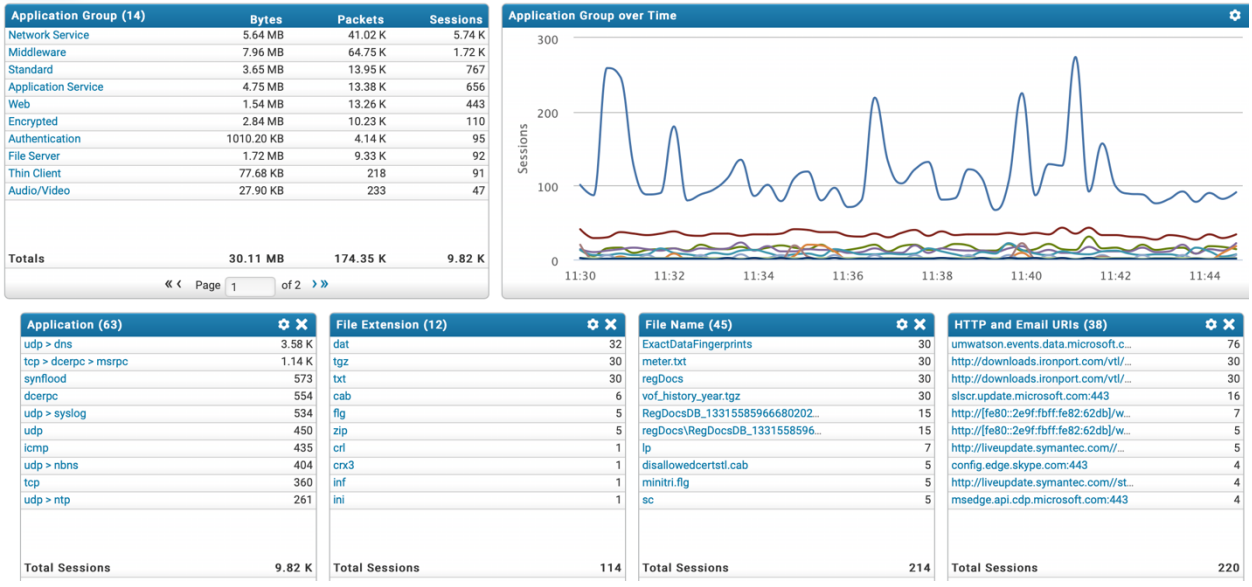
Symantec Network Forensic ürünü temel fonksiyonu, ağ üzerinden herhangi bir sızıntı girişimi veya sızıntı olduğu varsayımda, bunu geçmişe dönük analiz etme imkânı verir.

Siem v.b. ürünler bir sızıntı teşebbüsü olduğunda alarm üretebilir. Ancak herhangi bir olay tetiklenmediği varsayımında, sızıntının boyutu ve izole edilmesi gereken sistemler anlık olarak tespit edilemez. Bunun için belki de yapının büyüklüğü de göz önüne alındığında aylar boyu gerekecek bir analiz gerekmektedir.

Yaşayan ve kapatılamayan sistemlerde aylar boyu böyle bir operasyona girişilse bile, bu hem maliyetli hem de bu süreçte sistemde her zaman sızıntının ve dış erişimlerin devam ediyor olması riskini doğurur.

Cihaz tüm network trafiğini kaydeder.

Bunların parse edilebilinen kısmını meta olarak kaydeder.

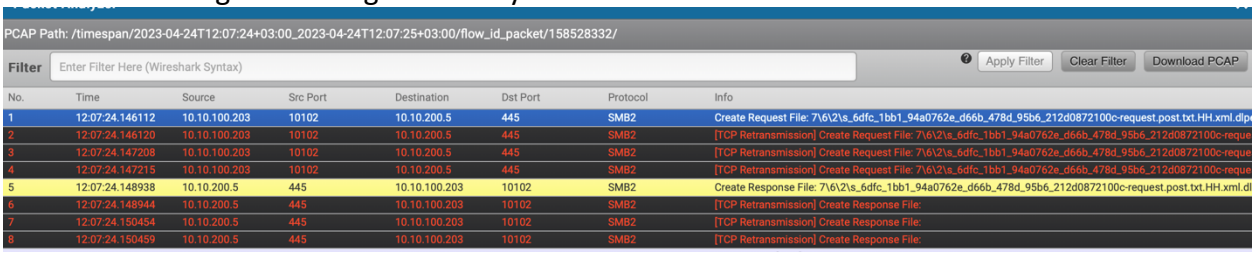


Bu sayede ayrılan alana da göre eski verilere rahatlıkla ulaşılabilir.

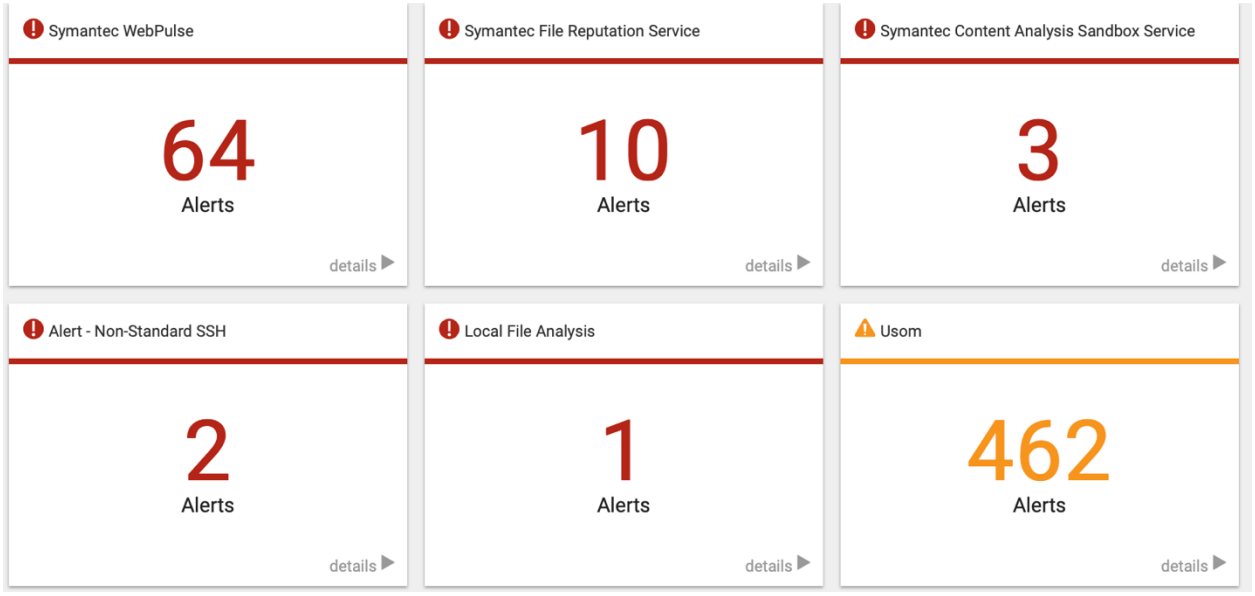
Tüm trafik Raw olarak da kaydedilir.

Time	Source(s)	Type	Method	Size
11:30:01	smb session	protocol/smb		340.52 KB
11:30:01	smb session	protocol/smb		2.07 MB
11:30:02	smb file: a\7\2\s_6dfc_0cf2_4770a729_62b4_4272_a235_c603f8f509c6-request.p...	application/octet-s...		452 B
11:30:02	smb file: b\0\f\s_3f6e_12a3_0969b0f4_196b_4b7c_af84_37a8b7ae6906-request.p...	application/octet-s...		452 B
11:30:02	smb file: a\7\2\s_6dfc_0cf2_4770a729_62b4_4272_a235_c603f8f509c6-metadata.j...	application/octet-s...		436 B
11:30:02	smb file: b\0\f\s_3f6e_12a3_0969b0f4_196b_4b7c_af84_37a8b7ae6906-metadata....	application/octet-s...		436 B
11:30:02	smb file: 2\2\f\s_6dfc_0cfc_5a2022f4_b0dc_4741_9c6e_41db2fa26357-metadata.j...	application/octet-s...		420 B
11:30:02	smb file: 0\9\9\s_3f6e_12ab_222e0991_1cee_4ced_b2fe_13a40853f19e-metadata...	application/octet-s...		468 B
11:30:02	smb file: b\0\f\s_3f6e_12a3_0969b0f4_196b_4b7c_af84_37a8b7ae6906-network.f...	application/octet-s...		228 B
11:30:02	smb file: a\7\2\s_6dfc_0cf2_4770a729_62b4_4272_a235_c603f8f509c6-network.fu...	application/octet-s...		212 B
11:30:02	downloads.ironport.com/vtl/meter.txt	text/plain	GET	46 B
11:30:02	downloads.ironport.com/vtl/vof_history_year.tgz	application/x-gzip	GET	0 B
11:30:02	connectivitycheck.gstatic.com/generate_204	Unknown/Unknown	HEAD	0 B
11:30:02	smb session	protocol/smb		730.66 KB
11:30:02	smb session	protocol/smb		693.87 KB
11:30:03	smb file: 0\9\9\s_3f6e_12ab_222e0991_1cee_4ced_b2fe_13a40853f19e-network.f...	application/octet-s...		324 B

İstenilen herhangi bir trafik geleneksel yöntemlerle de analiz edilebilir.



Bunların dışında custom IOC'ler ile (Usom v.b.) entegre edilip, bu yönde de analiz yapılabilir.



Kategorilere göre alarmlar konsolide edilir.

Açık entegrasyon sayesinde, Fireeye, Lastline, Cuckoo, Icap v.b. Sandbox, DLP ürünleri ile entegre olabildiği gibi native olarak Symantec Edr, Sep, Content Analysis ürünleri ile direk entegrasyon da mevcuttur.

Bu sayede ağ üzerinde oluşabilecek ZeroDay'ler de dahil olmak üzere birçok dosyanın analizi de network seviyesinde sağlanmış olmaktadır.

Ancak trafiğin şifreli olarak (https, ftps, smtps, ssh v.b.) şeklinde kaydedilmesi analizi imkânsız hale getireceğinden, ağ yapısının buna göre analiz edilmesi ve doğru yerden trafiğin iletilmesi kilit noktasındadır.

2.6 Symantec Endpoint Protection

Symantec Endpoint Protection ürünü uç nokta güvenliğinde, genel anlamda zararlı dosyaların tespit edilmesi, sistemler üzerinde erişim denetimlerinin yönetildiği üründür.

Bilinen tehditleri imza veritabanı ve dosya itibar servisi sayesinde tespit edebilirken, kurulu olduğu sistem üzerinde kurum politikasına aykırı davranışların tespit edilmesine yönelik özelleştirilmiş kuralların yazılıp işletilmesine olanak sağlar. Kurum politikasında hangi davranışların olağan ya da olağan dışı olduğu tespit edildikten sonra, illegal aktiviteleri loglayan ya da engelleyen kurallar yazılabilmektedir.

Benzer şekilde kurum içerisinde kullanımı legal olan harici cihazların çalışması ve kurum dışından gelen donanımların çalışmasının engellenmesi için konfigürasyonlar yapılabilmektedir.

2.7 Symantec Endpoint Detection and Response

Symantec'in EDR kategorisindeki bu ürün ile, tehdit avcılığı ve gerçekleşen ihlallere karşı olay müdahale prosedürlerinin uygulanmasına olanak sağlanmaktadır.

Dünyada aktif olan ancak henüz kuruma ulaşmamış tehditlere karşı sistemlerde benzer zararlı davranışların tespit edilmesi gerçekleştirilebilirken, kurum içerisinde prevention çözümlerini aşmayı başarmış tehdit tespit edilmesi ve zararlı process'in sonlandırılması, bu process'in ilgili dosyalarının silinmesi gibi işlemlerin gerçekleştirilmesi sağlanabilir.

2.8 Symantec Data Loss Prevention

Symantec'in veri sızıntısı önleme ürünüdür. Bu ürün, hem uç nokta hem de network üzerinde içerik denetimi yaparak hassas ve kritik verilerin kurum dışına çıkışını denetler.

Kurum politikasına göre hassas ve kritik verilerin tanımı yapıldıktan sonra bu verileri kurum işleyişi çerçevesinde paylaşacak kullanıcıları ya da kullanıcı gruplarının, kullanılacak metotları ve bu verilerin gönderilebileceği hedeflere iletilmesinin denetimi yapılmaktadır.

Bu sayede, hassas ve kritik verilerin yetkisiz kullanıcılar tarafından kurum politikasında izin verilmeyen metotlar ile izin verilen hedefler dışında paylaşılma girişimlerinin kayıt altına alınmasını sağlar.

3. Genel Değerlendirme ve Sonuç

Symantec Network Security ailesi Web tarafında forward proxy ile kullanıcı internet erişimini güvenli hale getirir. Kullanıcıların dosyayı istemcilere indirmesinden önce hem içerik taraması hem de Sandbox kontrollerinden geçirir. Böylece zararlı dosyalar ilk defa da web kanalından geçmeye çalışsa engellenir. Icap entegrasyonu sayesinde Symantec DLP de dahil olmak üzere tüm DLP ürünleri ile açık entegrasyona sahiptir.

Reverse Proxy sayesinde, Dns tünelleme başta olmak üzere, https over dns dahil tüm dns erişimleri güvenli hale getirebilirsiniz.

Waf ile birlikte, dışarı açık uygulamalarınız üzerinde Web Application Firewall özelliklerini çalıştırabilirsiniz.

Isolation özelliği sayesinde, riskli veya tanımladığınız kriterlere göre olan erişimleri güvenli hale getirilebilir.

Cloud özellikleri ile birlikte, mobil/tablet erişimleri de merkezden yönetilebilir seviyede olmaktadır.

Brightmail sayesinde, tüm mail trafiği yönetilebildiği gibi, Proxy ile aynı Sandbox bileşeni kullanılarak benzer güvenlik önlemleri mail kanalı için de yer alır.

SSL Visibility sayesinde Fw, IPS, Waf gibi birçok network cihazı, çözülen trafik üzerinden aktif koruma yapar hale geldiği gibi, bu cihazlar SSL çözümlemesi için ekstra bir kaynak tüketmeşinin önüne geçmektedir.

Network Forensic, Security Analytics cihazı tüm erişim trafiğini kaydeder, zararlı bir erişim varsa tespit eder, olası veri sızıntıları veya izinsiz erişim isteklerinde nokta atış tespitlerde bulunup, minimum servis kesintisi ile maksimum güvenliği tesis eder.

Symantec uç nokta ürünü ile bilinen tehditlere ve kurum politikasına aykırı davranışlara karşı önlem alınıp, EDR ürünü ile olası ihlallere karşı aksiyon alınabilmektedir.