

DLP Nedir?

Data Loss Prevention'un (Veri Kaybı Önleme) kısaltması olan DLP veri güvenliğinizi sağlamak için standartlaştırılmaya çalışılan bir teknolojidir. KoruMail içerisindeki DLP modülü mime-type bazında dosya tipi kontrolü, e-posta içerisinde kredi kartı bilgileri, sosyal güvenlik numara bilgileri gibi verilerin dışarıya aktarılmasını önlemek gibi çok önemli bir görev gerçekleştirmektedir.

DLP temel olarak, belli politikalar üreterek kurum bilgilerinizin kötü niyetli kişiler tarafından dışarıya sızdırılmasını önlemek olarak açıklanabilir. Günümüzde, bilgi iletişiminde önemli bir yer tutan e-posta iletişimi de dışarı bilgi sızdırmak için kullanılan en yaygın yöntemlerdendir.

Firmanız içerisinden bilgi sızdırmaya çalışan kötü niyetli kişiler bazen siz ekli dosyalarda kontrol gerçekleştirseniz bile uzantıları değiştirerek dışarıya dosya gönderebilmektedir. KoruMail dosyanın mime-type kısmından kontrol gerçekleştirerek uzantısı değişse dahi dosyanın asıl olarak tipini tespit edebilmekte ve KoruMail DLP Profilinizde belirtmiş olduğunuz yasaklı uzantılar arasındaysa gönderimi engellemektedir. Ayrıca sahte e-postalarla kullanıcılardan kredi kartı ve sosyal güvenlik numarası gibi kişiye özel bilgileri elde etmeye çalışan kötü niyetli kişilere karşı önlem olarak e-posta içerisinde kredi kartı ve sosyal güvenlik numarası tespit edilirse bu e-postanın teslimi de engellenmektedir.

DLP Modülü Nasıl Etkinleştirilir?

KoruMail üzerinde öncelikle Menü Altında "Modüller" – "DLP" sekmesinde modülü uygulamak istediğiniz Profili seçip kaydetmelisiniz. (Şekil 1)





Bu işlem sonrası "Profil Yönetimi" – "Profiller" – "Uygulamak istediğiniz Profil" – "DLP" sekmesinde detaylı DLP ayarları gerçekleştirilebilmektedir. <mark>(Şekil 2)</mark>

		Profili düzenle: Default Incoming Profile								
		Üyeler Anti-virüs Anti-spam Kara Liste Beyaz Liste SMTP Eklenti Filtresi Başlık Filtresi Arşiv ve Karantina RBL DLP								
		DLP Aksiyon								
	Kullanıcı Yönetimi	DLP Aksiyon Xok 🗸								
	Sistem	DLP Karantina	-							
Sekil 2	> SMTP	OLP Bildirim								
ŞCKIT Z	Modüller	Eklenti Listesi DLP Metin Filtresi								
	 Profil Yönetimi 		_							
	Profiller	Telif Hakka 2006-2015 Comodo KoruMall. Tüm haklan saklıdır. KoruMall ismi ve logoşus Comodo tescilli markalandır.								
	Raporlar	orocover and the								
	Karantina ve Arşiv									

DLP Detaylı Ayarlar

DLP özelliğini kullanmak istediğimiz Profilimizde DLP sekmesinde Aşağıdaki sekmeler bizi karşılamaktadır. (Şekil - 2)

DLP Aksiyon

DLP tarafından tespit edilen maillerde uygulanacak işlemlerdir. Bu durumlar aşağıdaki gibidir.

- Reddet
- Yoksay
- Aksiyon yok

Bu seçeneklerden "Reddet" seçili durumda olduğu zaman DLP tarafından tespit edilen mailler reddedilir, "Yoksay" seçili durumda olduğu zaman DLP tarafından tespit edilen mailler karşı tarafa iletilir ve Sistem yöneticisine bilgi verilir. "Aksiyon Yok" seçili durumda olduğu zaman DLP pasif durumdadır.

DLP Karantina

		Profili düzenle: Default Incoming Profile									
	Nord Matt	Üyeler Anti-virüs Anti-spam Kara Liste Beyaz Liste SMTP Eklenti Filtresi Başlık Filtresi Arşiv ve Karantina RBL DLP									
	Kullanıcı Yönetimi	DLP Aksiyon DLP Karantina									
	→ Sistem	DLP Karantina'yı Etkinleştir									
C 1110	→ SMTP	DLP Bildirim Eklenti Listesi									
Şekil 3	Modüller	DLP Metin Filtresi									
	 Profil Yönetimi 										
	Profiller	Telif Hakka 2006-2015 Comodo KoruMail. Tüm hakları saklıdır. KoruMail ismi ve logosu Comodo tescilli markalarıdır. Sürüm: 4.0.3048									
	Raporlar										
	Karantina ve Arşiv										



DLP Karantina, Aksiyon durumu "Reddet" olduğu zaman Tespit edilen maillerin KoruMail Karantina bölgesine alınmasını sağlayan özelliktir. (Şekil 3)

	KoruMail	Profili düzenle: Default Incoming Profile
	Kullanıcı Yönetimi	Úyeler Anti-vírüs Anti-spam Kara Liste Beyaz Liste SMTP Eklenti Filtresi Başlık Filtresi Arşiv ve Karantina RBL DL DLP Aksiyon DLP Karantina
	Sistem SMTP	DLP Karantina'yı Etkinleştir DLP Bildirim
Şekil 4	Modüller Profil Yönetimi	DLP Metin Filtresi
	Profiller Raporlar	Telif Hakkı 2006-2015 Comodo KoruMall. Tüm hakları saklıdır. KoruMail ismi ve logosu Comodo tescili markalandır. Sürüm: 4.0.3048
	Karantina ve Arşiv	

DLP Aksiyon Durumu "Reddet" ve "Yoksay" olduğu durumlarda DLP tarafından algılanan maillerin Sistem Yöneticisine bilgi verilmesini sağlayan özelliktir. (Şekil 4) DLP aktif Durumda ise mutlaka açık olması tavsiye edilir.

DLP Eklenti Listesi

	~
	~
	•
	~
Profil Yönetimi Profiler Raportar Profiler Prof	^
Profiller PGP Secret Keyring Transport Neutral Encapsulation Format (TNEF) Transport Neutral Encapsulation Format (TNEF)	^
Raporlar Transport Neutral Encapsulation Format (TNEF) Transport Neutral Encapsulation Format (TNEF)	
7 sie Eermat	
Karantina ve Arşiv Dosya Sınıfı Seç Encapsulaton Format U Jup Format	Ekle
DHA Archive Java Archive (JAR)	
	×
SI	
Dosya Sinit Ismi Dosya Tipleri Durum	
Encapsulation Format Java Archive (JAR) Etkin	



Engellemek istediğimiz eklentileri seçmek için öncelikle "Eklenti Listesini Etkinleştir" işaretlenmelidir. Mail içeriğindeki eklenti Arşiv dosyası (zip, rar, tar, jar vb.) ise içeriğinin taranması için "Arşiv Dosyaları Tara" etkin olmalıdır. <mark>(Şekil 5)</mark>

Dosy	ya Sınıfı Seç Encapsulation For	rmat 🗸	Unix Compress Microsoft Cabi Gzip ASCII-armore PGP Public Key	s net File (CAB) d PGP Data yring	
Sil]				
	Dosya Sınıf İsmi		Dosya Tipleri	Durum	
	Dosya Sınıf İsmi Executable File	Dynamic Li	Dosya Tipleri nk Library (DLL)	Durum <u>Etkin</u>	
	Dosya Sınıf İsmi Executable File Encapsulation Format	Dynamic Lin Java Archiv	Dosya Tipleri nk Library (DLL) re (JAR)	Durum <u>Etkin</u> <u>Etkin</u>	
	Dosya Sınıf İsmi Executable File Encapsulation Format Encapsulation Format	Dynamic Li Java Archiv Microsoft C	Dosya Tipleri nk Library (DLL) re (JAR) abinet File (CAB)	Durum Etkin Etkin Etkin	

Eklenti Listesini Etkinleştir sekmesinde "Dosya Sınıfı Seç" bölümünde ilgili dosyanın Sınıfını seçiyoruz ve sağ taraftaki "Dosya Tipleri" menüsü içinde dosya sınıfına ait dosya tipleri listeleniyor. Bu listeden engellemek istediğimiz dosya tipini seçip "Ekle" butonu ile Engellenecek dosya listemize ekliyoruz. (Şekil 6) Eklenti kuralları için mime-type bazında engelleme sağlandığı için, Uzantısı değişse dahi eklenti engellenecektir.



DLP Metin Filtresi

	MESSAGING GATEWAY	Üyeler Ant	-virüs Anti-spam	Kara Liste Beyaz Lis	ste SI	ATP	Eklenti Filtresi	Başlık Filtresi	Arşiv ve Karantina	RBL	
	Kullanıcı Yönetimi	DLP Aksiyon									
	▹ Sistem	DLP Bildirim									
	→ SMTP	Eklenti Listes	resi								
	> Modüller	DLP Metin Fil	resini Etkinleştir	•							
	✓ Profil Yönetimi	Politika									
il 7	Profiller	Ekle									
	> Raporlar	Durum	DLP Metin Fi	ltresini Etkinleştir	E	ylem					
	Karantina ve Arşiv		Credit Card		9		×				
			Email Address Turkish Identity Numb	er	Q		<u>x</u>				

Sahteciliği önlemek için, kredi kartı ve sosyal güvenlik numarası gibi kişi veya kuruma özel olabilecek bilgilerin sahte e-postalarla dışarı sızdırılmasının engellenmesi için oluşturulmuş bir filtrelemedir. DLP Metin Filtresini aktif etmek için "DLP Metin Filtresini Etkinleştir" karşısındaki kutucuğu işaretlememiz gerekmektedir. (Şekil 7)

Varsayılan olarak 3 şablon mevcuttur. Herhangi bir sablon üzerine tıklatıp göster dediğinizde içeriğini görebilirsiniz. Ekle kısmında ise kendiniz bir şablon oluşturarak bu tarz denetimleri fazlalaştırabilirsiniz. Şablon örnekleri için aşağıdaki adresten faydalanabilirsiniz.

- http://www.regexlib.com

- http://regex101.com/





KoruMail DLP Modülü açık iken modül tarafından engellenen maillerin bilgisini KoruMail arayüzünden "Raporlar" – "Posta Günlükleri" menüsünden "Gelişmiş Arama" linkini tıklayarak. <mark>(Şekil 8)</mark> Aşağıdaki örnekteki gibi filtreleyerek öğrenebilirsiniz.

Ρ	osta Gü	inlükler	ri					
_ s	Subject Sender Recipients P							
Son	uç v	EŞİT 🕠	ULP RED V					
						Arama Temizie		
Eyk	mier v	Yapt						
	Konu	Sonuç	Alinma	Gönderici	Ahcı(l	ar) IP	Açıklar	
0	Surcrypti	DLP	08.05.2014 10:55:55	noktatest@test.com	i @test.com	10.41.0.1	SurGATE DLP detected a forbidden file (tomcat-api.jar) or body fi	
0	Surcrypt:	DLP	08.05.2014 10:26:07	noktatest@test.com	i @test.com	10.41.0.1	SurGATE DLP detected a forbidden file () or body filter ()	
0	Surcrypti	DLP	08.05.2014 10:25:02	noktatest@test.com	i @test.com	10.41.0.1	SurGATE DLP detected a forbidden file () or body filter ()	
0	Surcrypt:	DLP	07.05.2014 16:39:26	noktatest@test.com	i @test.com	10.41.0.1	SurGATE DLP detected a forbidden file (advapi32.dll) or body filte	
0	Surcrypt:	DLP	07.05.2014 16:38:20	noktatest@test.com	i @test.com	10.41.0.1	SurGATE DLP detected a forbidden file (tomcat-api.jar) or body fi	
Eyk	mier v	Yapt					Brinci Önceki	
				Telif	Hakkı 2006-2015 C KoruMail ismi ve lo	Comodo KoruMail. Tüm haklaı ıgosu Comodo tescilli markala Sürüm: 4.0.3048	n saklıdır. Indir.	
	P Son Eye	Posta Gü subject Sonuç v fyemer v fyemer survyst: Surv	Posta Günlükler	Posta Günlükleri Sender Receients P Senuç v Eşir v DLP RED v + Evener v Yaşı Senuç v Eşir v DLP RED v + Senuç v Eşir v DLP RED v +	Posta Günlükleri	Posta Günlükleri Arama Tenzie Beleris atama Benug vEğit VDLP RED v + Verener VBgit V Serveysti DLP 00:00214 10:25:05 reklaratetiğtest.com i Gest.com Serveysti DLP 00:02214 10:25:05 reklaratetiğtest.com i Gest.com Serveysti DLP 00:02214 10:25:05 reklaratetiğtest.com i Gest.com Serveysti DLP 00:02214 10:25:05 reklaratetiğtest.com i Gest.com Serveysti DLP 00:02214 10:25:05 reklaratetiğtest.com i Gest.com Serveysti DLP 00:02214 10:25:05 reklaratetiğtest.com i Gest.com Serveysti DLP 00:05:2014 10:25:05 reklaratetiğtest.com i Gest.com Serveysti DLP 00:05:2014 10:25:05 reklaratetiğtest.com i Gest.com Serveysti DLP 00:05:2014 10:25:05 reklaratetiğtest.com i Gest.com	Posta Günlükleri Arama Tende dana aram Benuç vEşir vDLP RED v + Senuç vEşir vDLP RED v + Senuç vEşir vDLP RED v + Senuş vEşir vDLP v + Senuş vEşir vDLP RED v + Senuş vEşir vDLP RED v + Senuş vEşir vDLP RED v + Senuş vEşir vDLP RED v + Senuş vEşir vDLP RED v + Senuş vEşir vDLP RED v + Senuş vEşir vDLP RED v + Senuş vEşir vDLP RED v + Senuş vEşir vEş	

KoruMail Hakkında

İstanbul Yıldız Teknopark'ta faaliyet gösteren KoruMail; 2006 yılında e-posta konusundaki derin tecrübelerini Ar-Ge'ye aktararak ilk ürünü Secure Email Gateway çözümünü pazara sunmuştur. 35 kişilik genç ve dinamik kadrosuyla "E-posta ve Mesajlaşma" konusuna odaklanan KoruMail kendi geliştirdiği ürünlerle alanında lider global bir firma olmayı hedeflemektedir. KoruMail 2014 Eylül ayında Comodo Yazılım AŞ tarafından satın alınmış olup, Comodo bünyesinde faaliyetine devam etmektedir.

Adres: Yıldız Teknopark Atatürk Bulvarı İkitelli/İstanbul 1. Kat Ofis No:101

KoruMail bir **COMODO** firmasıdır.