

## NATEK Audit Manager

NATEK Audit Manager bilgi sisteminde gerçekleşen güvenlik ile ilgili aktivitelerin izlenmesini ve kritik olaylar gerçekleştiğinde, bilgi işlem güvenlik biriminin uyarılmasını sağlayan bir yazılımdır. Bilgisayar sayısının fazla olduğu ortamlarda yüksek bir ölçeklenebilirlik sağlayan NATEK Audit Manager, diğer güvenlik yönetim sistemleri ile entegre olabilmektedir.

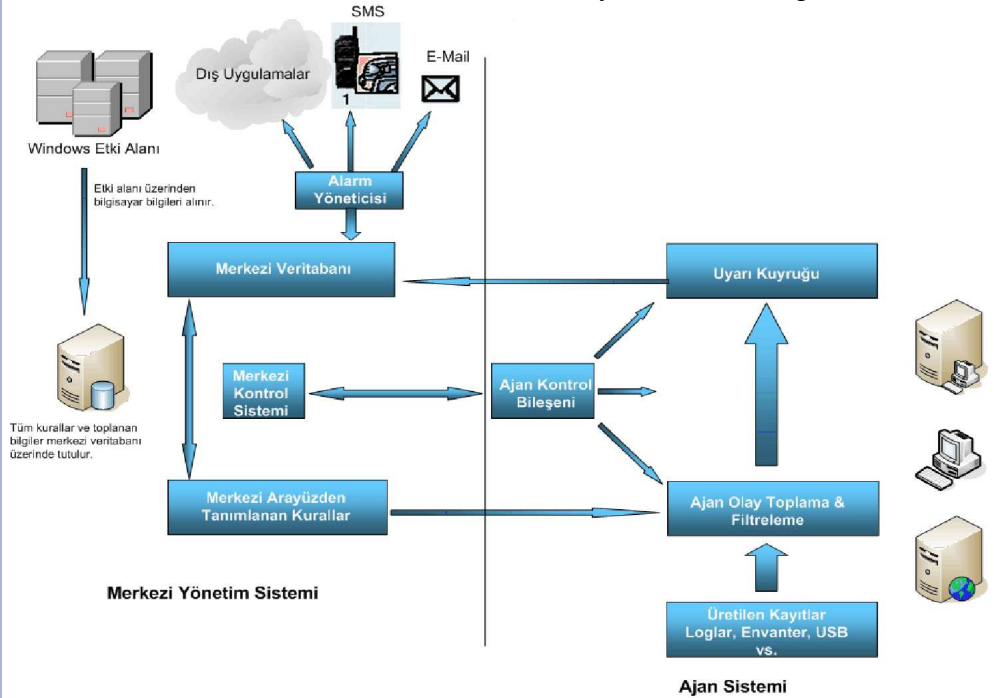
### Temel Özellikleri

- Merkezi Log Yönetim Kabiliyeti
- Kritik Dosyalara Erişimin Takip Edilmesi
- Yetkisiz Yapılan İşlemlerin Tespit Edilmesi
- Kritik Güvenlik Olaylarının Gerçek Zamanlı Takibinin Sağlanması
- Tek Merkezden Kayıt Politikalarının Belirlenmesi
- Tek Merkezden Kritik Olayların ve Alarm Politikasının Belirlenmesi
- Yetkisiz Bilgisayar Girişlerinin Tespit Edilmesi
- Yönetici Hesaplarının Kullanımının Takip Edilmesi
- Bilgisayar Yönetici Hesapları Şifrelerinin Merkezi Olarak Yönetilmesi
- Sadece Belirlenen Kritik Olay Kayıtlarının Analiz Edilmesi
- Kayıt Kaybının Engellenmesi
- USB Diske Kopyalanan Dosyaların Takip Edilmesi
- Merkezi Kurulum Sistemi
- Gelişmiş Ajan Durum Takip Sistemi
- Sisteme Kontrol Dışı Gelen Bilgisayarların Tespit Edilmesi
- Kontrolsüz Güvenlik Duvarı Kullanımı, Yetkisiz güvenlik Ayarlarının Değiştirilmesi Gibi Nedenlerden Dolayı Sistem Yöneticileri Tarafından Erişilemeyen Bilgisayarların Bulunması
- Belirlenen Bilgisayarların Ağ Erişimine Kapatılması
- Modüllerin Durumlarının Merkezi Takibi
- Bilgisayar Adı Değişimlerinin Takip Edilmesi
- Gelişmiş ve Dış Sistemler İle Entegre Olabilen Web Tabanlı Raporlama Sistemi
- Tamamen Web Tabanlı
- Konfigürasyon Arayüzü
- Ajanlı ve Ajansız Log Toplama Kabiliyeti
- Gelişmiş Korelasyon Yeteneği

Kurumlarda bilgisayar sistemlerinde yer alan bilginin önem derecesinin artması bu sistemlerde yaşanan aktivitelerin takip edilmesi ve ilgili sistemlerin daha iyi korunması gibi ihtiyaçları ortaya çıkartmıştır. Bu kapsamda, bilgisayarlardaki aktivitelerin incelenmesi, kritik olayların olması durumunda da yöneticilerin durumdan anında haberdar edilebilmesi oldukça önemlidir.

### Yapısal Özellikleri

NATEK Audit Manager bilgisayar sistemlerinde yer alan önemli aktivitelerin izlenerek önemli olanların merkezi bir veritabanında tutulmasını, kritik işlemler doğrultusunda gerçek zamanlı alarmlar üretilmesini sağlayan bir yazılımdır.

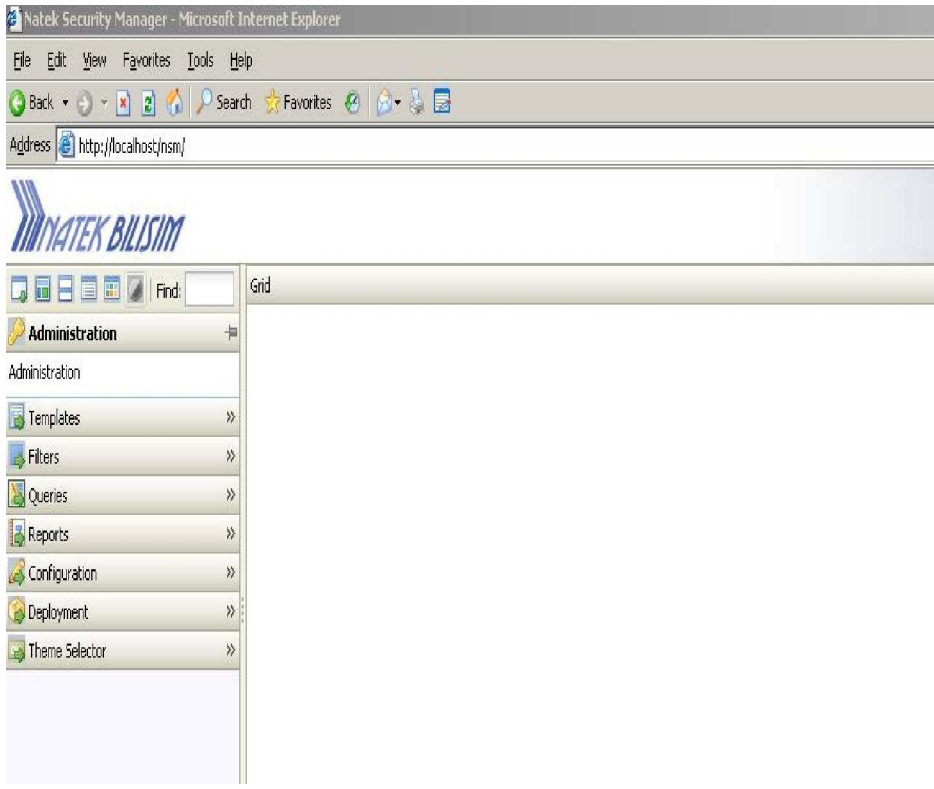


Ajan kurulumunun ardından ilgili sistemlerde ajanların durumları izlenmeye başlanmakta ve ajanda bir sorun olması durumunda bunun tespiti ve ilgili personele uyarımı gerçekleştirilebilmektedir. Böylelikle sayıları yüksek olan istemcilerde

Sistem, Windows etki alanı ile entegre çalışarak veya sistemi sürekli olarak tarayarak bilgisayar sistemindeki değişikliklerin otomatik olarak NATEK Audit Manager Veritabanında güncellenmesini sağlamaktadır. İncelenmek istenen tüm aktiviteler için kurallar merkezi yönetim konsolu üzerinde oluşturulmakta ve ajanların olduğu noktalara dağıtılmaktadır. Böylelikle kritik aktiviteler için alarm üretilmesi sağlanmaktadır. Bilgi, merkezi sisteme gönderildikten sonra istenilen işlemler yapılarak alarm üretimi sağlanmaktadır.

NATEK Audit Manager, Windows Etki Alanı ile entegre olarak kurumda yer alan bilgisayarların tespit edilmesini sağlamakta ve bu bilgisayarlara otomatik olarak ajan kurulmasını sağlamaktadır.

ajanların durumlarının tespit edilmesi sağlanabilmektedir. Ajanlar periyodik olan çalışma durumlarını merkezi yönetim sistemine düzenli olarak bildirmektedir. Bu sayede ajan üzerindeki herhangi bir bileşende sorun olması durumunda ilgili sorunun ayrıntıları hızla tespit edilebilmektedir.



USB diske veya disket sürücüsüne kopyalanan dosyaların takip edilmesi ve raporlanması NATEK Audit Manager yazılımının diğer önemli bir özelliğidir.

### **Mimari Yapı**

Sistem merkezi yönetim konsolu ve ajanlardan oluşmaktadır. Ajanların temel görevi bilgisayar kaynaklarını gerçek zamanlı izlemek, önemli işlemleri belirlemek, belirlenmiş olanları merkezi veritabanına göndermek, kritik olaylar için de alarm üretmektir. Yönetim konsolunun temel görevi de hangi ajanlara hangi kuralların uygulanacağını belirlenmesi, ajanların statülerinin takip edilmesi ve merkezi yazılım yüklemesini sağlamak için da programın yüklenmesini sağlamaktır. Ayrıca yönetim konsolu Windows etki alanı ile de entegre çalışarak, etki alanında ajan kurulu olmayan makineleri de takip edebilmektedir.

### **Yönetim Bileşeni Platform Desteği**

Windows XP/2000/2003

### **Ajan Platform Desteği**

Windows XP/2000/2003

Linux

### **Kullanılan Veritabanları**

Windows MS-SQL

Oracle

My-SQL

## **İLETİŞİM**

### **Genel Müdürlük**

Mutlukent Mahallesi Angora Bulvarı 1996 Sk. No:4 BEYSUKENT / ANKARA

Tel: +90 312 225 14 41

Fax: +90 312 225 27 22

### **AR-GE 1**

Hacettepe Teknokent 2. Ar-Ge Binası No:15 Hacettepe Üniversitesi 06800

BEYTEPE / ANKARA

Tel: +90 312 299 26 18

Fax: +90 312 299 26 28

### **AR-GE 2**

Hacettepe Teknokent 1. Ar-Ge Binası No:13 Hacettepe Üniversitesi 06800

BEYTEPE / ANKARA

Tel: +90 312 286 19 74

Fax: +90 312 286 19 74

### **İstanbul Bölge Müdürlüğü**

Uphill Towers 1-A Blok D.132 ATAŞEHİR / İSTANBUL

Tel: +90 216 688 56 35

Fax: +90 216 688 56 33

