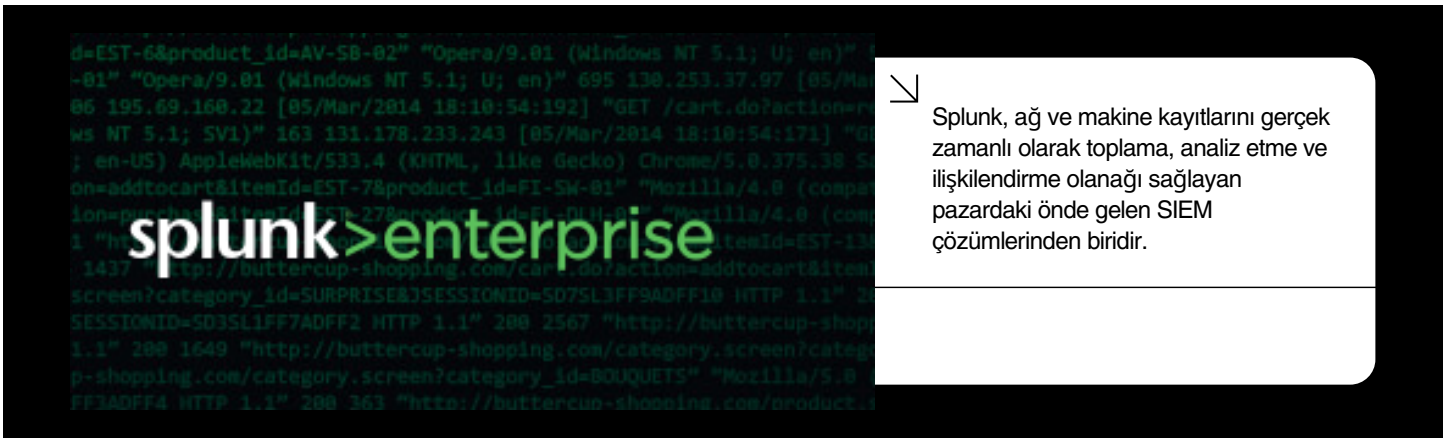
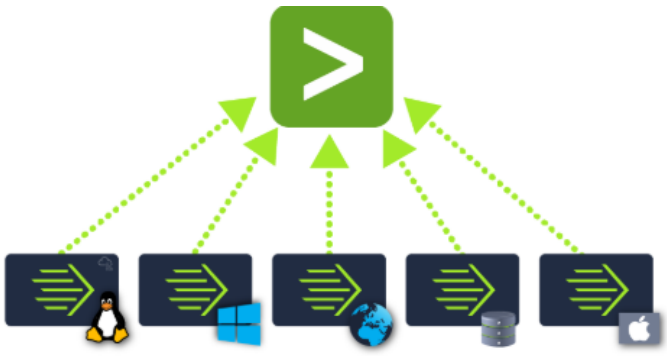


Splunk'un üç ana bileşeni vardır, bunlar Forwarder, Indexer ve Search Head'dir. Bu bileşenler aşağıda açıklanmıştır:

Splunk Forwarder

Splunk Forwarder, izlenmesi amaçlanan uç noktaya kurulan hafif bir aracıdır ve temel görevi verileri toplayıp Splunk örneğine göndermektir.İşlem için çok az kaynak gerektiğinden uç noktanın performansını etkilemez. Bazı önemli veri kaynakları şunlardır:

- Web trafiği üreten web sunucusu.
- Windows makinesi Windows Olay Günlükleri, PowerShell ve Sysmon verileri üretiyor.
- Linux ana bilgisayarı ana bilgisayar merkezli günlükler üretiyor.
- Veritabanı, DB bağlantı istekleri, yanıtları ve hataları üretiyor.



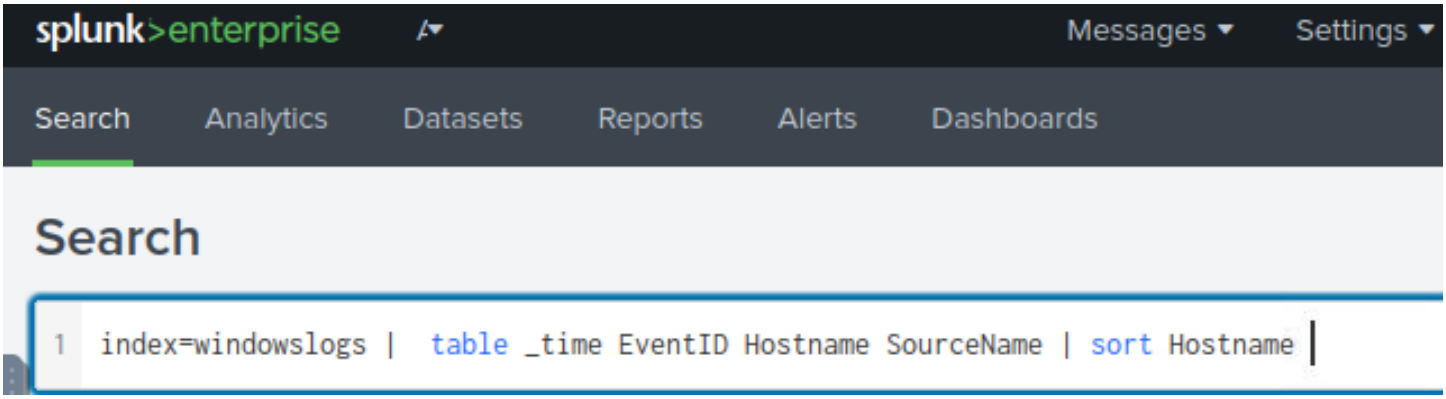
Splunk Indexer

Splunk Indexer, forwarderlardan aldığı verilerin işlenmesinde ana rolü üstlenir.Verileri alır, alan–değer çiftlerine normalleştirir, verilerin veri türünü belirler ve bunları olaylar olarak depolar. İşlenmiş verilerde arama yapmak ve analiz etmek kolaydır.

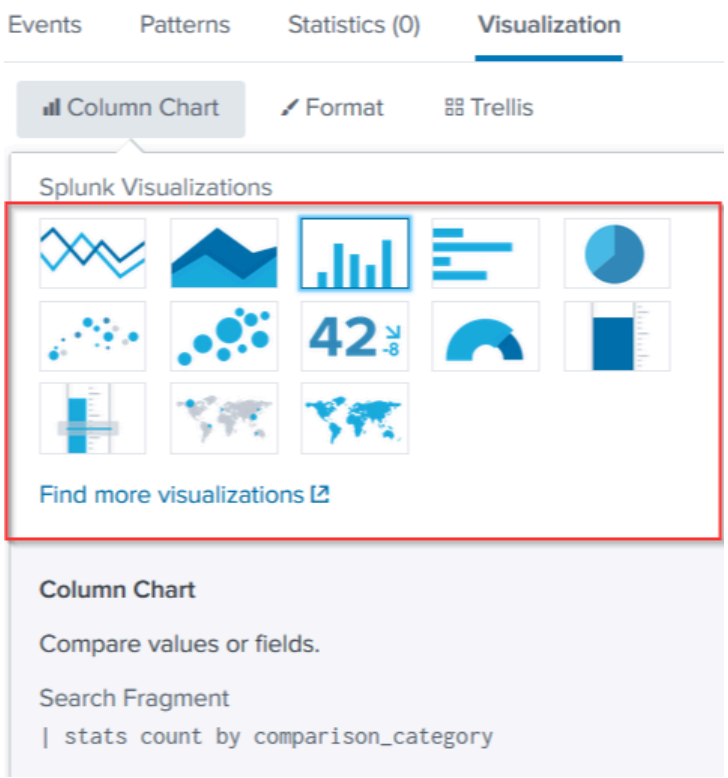
Search Head (Arama Başlığı)

Splunk Search Head, kullanıcıların aşağıda gösterildiği gibi dizinlenmiş günlükleri arayabilecekleri Arama ve Raporlama Uygulaması içindeki yerdir.

Kullanıcı bir terim aradığında veya Splunk Arama İşleme Dili olarak bilinen bir Arama dili kullandığında, istek indeksleyiciye gönderilir ve ilgili olaylar alan–değer çiftleri biçiminde döndürülür.

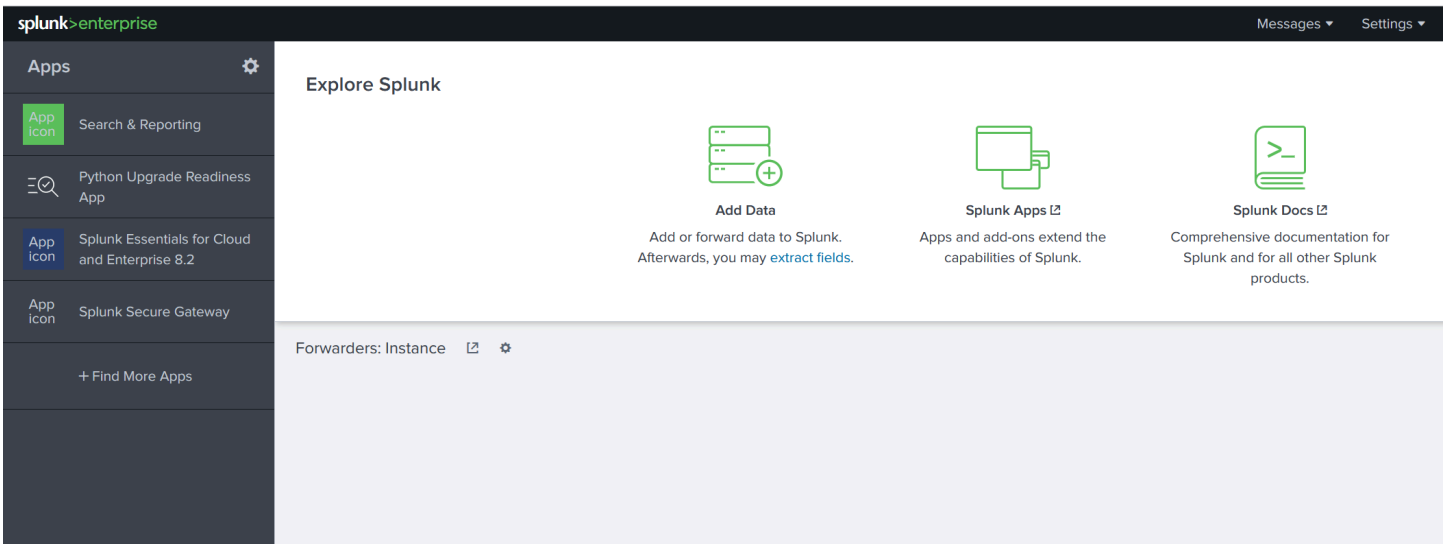


Search Head ayrıca sonuçları aşağıda gösterildiği gibi sunulabilir tablolara, pasta grafiği, çubuk grafiği ve sütun grafiği gibi görselleştirmelere dönüştürme olanağı da sağlar:



Splunk'ta gezinme

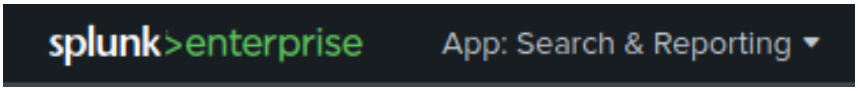
Splunk Bar: Splunk'a eriştiğinizde aşağıdaki ekran görüntüsüne benzer varsayılan ana ekranı göreceksiniz.



Ana ekranı oluşturan her bir bölüme veya panele bakalım. Üst panel Splunk Bar'dır (aşağıdaki resim).

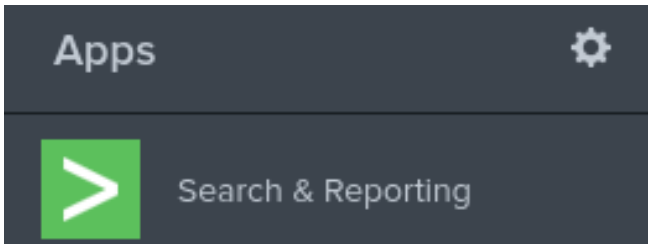
Splunk Çubuğu'nda sistem düzeyindeki mesajları Messages– (**Mesajlar**) görebilir, Splunk örneğini yapılandırabilir Settings– (**Ayarlar**), işlerin ilerleme durumunu inceleyebilir Activity– (**Etkinlik**), eğitimler gibi çeşitli bilgileri Help– (**Yardım**) ve bir arama özelliğini Find (**Bul**) kullanabilirsiniz.

Uygulamalar panelini kullanmak yerine yüklü Splunk uygulamaları arasında geçiş yapma olanağı, aşağıdaki görseldeki gibi Splunk Çubuğu'ndan sağlanabilir.

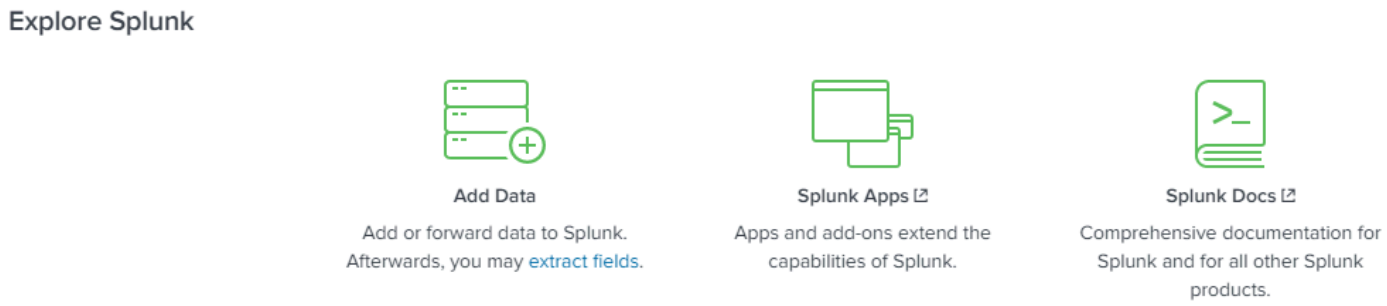


Apps Panel: Sırada Uygulamalar Paneli var. Bu panelde, Splunk örneği için yüklenen uygulamaları görebilirsiniz. Her Splunk kurulumu için varsayılan uygulama Arama ve Raporlama'dır.

Her Splunk kurulumu için varsayılan uygulama **Search and Reporting**– Arama ve Raporlama'dır.



Explore Splunk: Bir sonraki bölüm Splunk'u Keşfet'tir. Bu panel, Splunk örneğine veri eklemek, yeni Splunk uygulamaları eklemek ve Splunk belgelerine erişmek için hızlı bağlantılar içerir.



Splunk Dashboard: Son bölüm Ana Pano'dur. Varsayılan olarak hiçbir pano görüntülenmez.Splunk örneğinizde kolayca erişebileceğiniz çeşitli panolardan seçim yapabilirsiniz. Açılır menüden veya panolar listeleme sayfasını ziyaret ederek bir pano seçebilirsiniz.

Ayrıca panolar oluşturabilir ve bunları Ana Pano'ya ekleyebilirsiniz. Oluşturduğunuz panolar, Yours sekmesine tıklanarak diğer panolardan ayrı olarak görüntülenebilir.