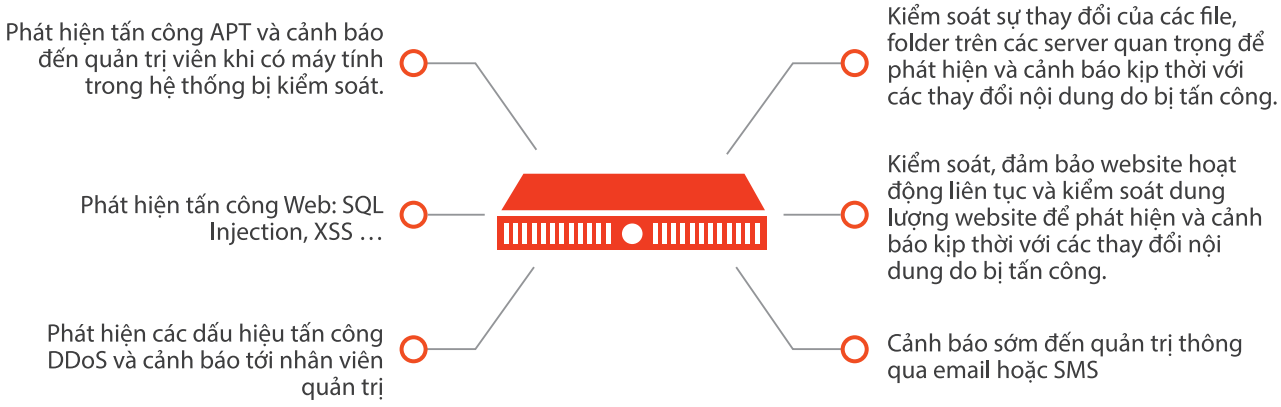
Bkav Network Inspector

Trong tấn công có chủ đích (APT), một khi đã lây nhiễm thành công vào một máy tính trong hệ thống, virus sẽ được kích hoạt để kết nối nhận lệnh điều khiển của hacker, sau đó tìm cách lây nhiễm rộng ra các máy tính khác trong hệ thống mạng để đánh cắp dữ liệu. Việc kết nối nhận lệnh điều khiển để lây nhiễm rộng, đánh cắp dữ liệu quan trọng có thể diễn ra trong thời gian dài, thậm chí vài năm. Khi này các virus đang ở trạng thái "nằm vùng". Việc phát hiện sớm nhất các virus "nằm vùng" khi nó bắt đầu xâm nhập thành công vào hệ thống ngăn chặn việc lây nhiễm rộng và chống lại được cuộc tấn công có chủ đích đó.

Bkav Network Inspector là thiết bị phát hiện và cảnh báo tấn công sớm theo thời gian thực, ngoài các khả năng giám sát và cảnh báo tấn công mạng thông thường như tấn công từ chối dịch vụ DdoS, tấn công vào ứng dụng web, tấn công Brute Force… BNI cung cấp khả năng phát hiện sớm các cuộc tấn công có chủ đích (APT) vào hệ thống.

Tính năng của BNI



Mô hình triển khai