Phần mềm Điều phối, tự động hóa & phản ứng an toàn thông tin BkavPro SOAR

Giới thiệu

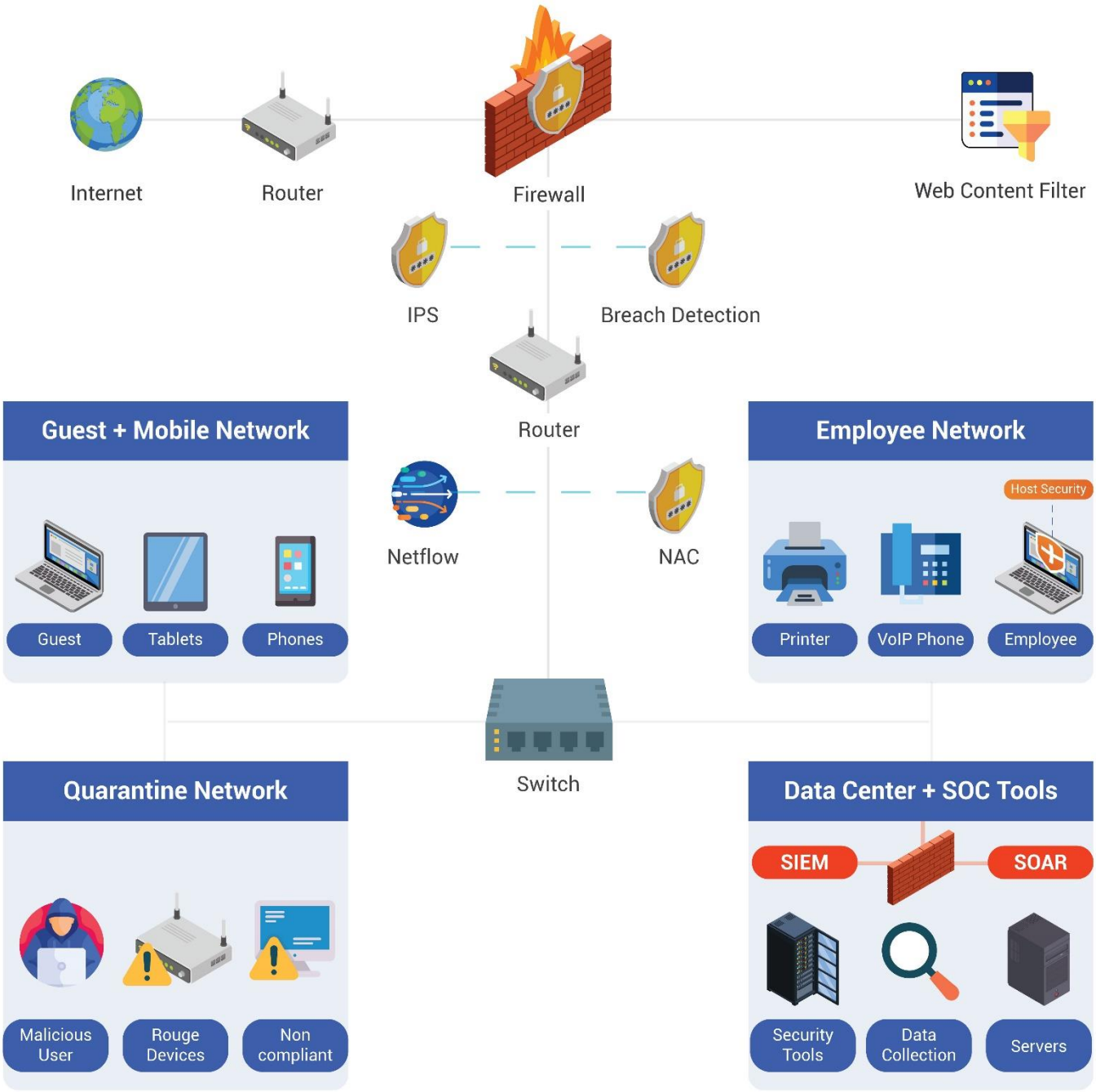
Giải pháp điều phối an ninh, tự động hóa và phản hồi - BkavPro Security Orchestration, Automation & Response (SOAR) cho phép cơ quan, tổ chức, doanh nghiệp thu thập dữ liệu về các mối đe dọa và hỗ trợ xử lý các sự kiện bảo mật cho đội ngũ xử lý sự cố trong SOC

Tính năng

Quản trị hệ thống	Quản lý vận hành
	Quản trị từ xa
	Quản lý xác thực và phân quyền
Kiểm soát lỗi	Bảo vệ cấu hình
	Bảo vệ dữ liệu log, cảnh báo, tình huống và bằng chứng
	Đồng bộ thời gian hệ thống
Tính năng về log	Log quản trị hệ thống
	Định dạng log
	Quản lý log
Hiệu năng xử lý	Độ trễ thời gian phản hồi các yêu cầu truy vấn dữ liệu thấp. BkavPro SOAR đảm bảo độ trễ thời gian tìm kiếm log, cảnh báo và tình huống với độ phức tạp bất kỳ, có phản hồi trong khoảng thời gian tối đa là 01 phút
	Thu thập đồng thời nhiều cảnh báo

Điều phối xử lý và giám sát	Điều phối xử lý cảnh báo
	Điều phối xử lý tình huống
	Giám sát và phân tích sự cố an toàn thông tin
Tính hợp và tự động hóa	Quản lý thành phần tích hợp
	Hỗ trợ tích hợp nhiều nền tảng khác nhau
	Hỗ trợ tích hợp nhiều API
	Hỗ trợ tích hợp API theo hai chiều
	Quản lý kịch bản
	Hỗ trợ thực hiện kịch bản tự động
	Hỗ trợ thực hiện kịch bản bán tự động
Tính năng khác	Làm giàu dữ liệu: Kết hợp với nguồn chia sẻ dữ liệu chính từ BTI (BkavPro Threat Intelligence) và các nguồn khác để làm rõ hơn các thông tin liên quan
	Hỗ trợ tích hợp các giải pháp bảo mật: Tích hợp các công cụ bảo mật khác nhau dễ dàng tìm kiếm thông tin, đánh giá mức độ và tương quan các sự kiện có liên quan đến sự cố cần điều tra
	Cung cấp quy trình xử lý tự động: Cho phép tự động kết nối các công cụ với nhau theo quy trình đã được thiết lập từ trước để xử lý sự cố, và có thể kết hợp với việc giám sát và kiểm tra trạng thái về công việc đó của giám sát viên
	Cung cấp các kịch bản xử lý sự cố và các thông tin liên quan cần thiết để ứng phó các cuộc tấn công phức tạp. Playbook sẽ tự động đưa ra các kịch bản khi kiểm tra thấy các thông tin có trong cảnh báo hay sự kiện về cuộc tấn công diễn ra khớp với các điều kiện của dạng tấn công đó
	Xuất báo cáo: Hỗ trợ các mẫu báo cáo chung hoặc có thể tùy chỉnh báo cáo phù hợp với yêu cầu của tổ chức

Sơ đồ



Thông số kỹ thuật

Yêu cầu	CPU	RAM	HDD
Cấu hình tối thiểu	4 - 8 Cores	8 - 16 GB	600 GB
Cấu hình tiêu chuẩn	16 Cores	32 GB	

Trụ sở chính: Tòa nhà Bkav, Khu đô thị Yên Hòa, Cầu Giấy, Hà Nội
Điện thoại: (024) 37 677 090 / Ext: 1013 Số fax: (024) 3868 4755
Website: security.bkav.com Email: DuAn@bkav.com
Bkav TP. HCM: Số 67, Đường số 3, Khu dân cư City Land, P.7, Q. Gò Vấp, TPHCM
Điện thoại: (028) 6296 6626 Số fax: (028) 2253 6103