Internal Vulnerability Scan

eSentire will scan internal Client IP addresses, including all Client servers (domain controllers, email servers, fileservers, database servers, application servers), all non-server infrastructure (firewalls, switches and routers, and VPN equipment) and all high-profile workstations ("**Internal Vulnerability Scan**").

Client is responsible to provide to eSentire domain administrator credentials to allow eSentire to provide a vulnerability assessment.

Internal Vulnerability Rescan. eSentire will perform an Internal Vulnerability Rescan if Client received a one-time or annual recurring Internal Vulnerability Scan. After remediation activities undertaken by Client have been completed following an Internal Vulnerability Scan, eSentire will, no later than three (3) months following eSentire delivering to Client its draft report, rescan only those servers identified by eSentire to have "high" or "critical" security issues to validate such remediation.