SERVICE DESCRIPTION

Network Access Control Non-Managed Product Only

Service Description

Trustwave will provide a Client Premise Equipment or virtual machine (“Trustwave NAC”) that will be used to discover endpoints connecting to the Client network. After each endpoint is discovered, Client can require that those endpoints go through an authentication process leveraging existing credential stores. The Trustwave NAC scans monitored endpoints to assess the compliance status with Client’s policies. Once endpoints are authorized, Trustwave NAC monitors packets from those endpoints to help enforce behavioral policies throughout the monitored segment minimizing risk to the network from non-compliant endpoints. The Trustwave NAC allows Client re-scanning upon any network re-entry to ensure monitored endpoints start and remain compliant.

About the Trustwave NAC Cycle

The following elements comprise the Trustwave NAC Cycle, detailing the flow of each endpoint’s life on the network.

Discover

Trustwave discovers endpoints when they connect to the network. The solution does not require SNMP traps, DHCP requests or any other external mechanism so discovery is efficient and independent of the switching infrastructure. The discovery process is also independent of endpoint type, working the same for every device, operating system and connection method.

Authenticate

After each endpoint is discovered, Client can require that those endpoints go through an authentication process. Leveraging existing credential stores such as Active Directory, LDAP, and RADIUS, there is a seamless identity check to end user workflow using SSO. With this feature Client can enforce identity-based policies, specifying what resources each user can access on the network, and specifying what usage policies should be enforced for each user.

Scan

Trustwave NAC scans managed and unmanaged endpoints that connect to the network, regardless of device type, operating system, or connection method. The scan assesses the compliance status with an organization’s
policies of each endpoint and also allows policies to be crafted based on endpoint type and endpoint characteristics.

**Authorize**

Authorization can be enforced for endpoints based on identity and scan information, allowing for a range of policy options, from allowing full access to known users and denying access to unknown users to allowing full access to compliant machines while denying access to non-compliant machines. Out-of-box policies give organizations the foundational elements needed to get full-cycle NAC, while the advanced policy permutations offer a more robust policy engine for controlling access to a company’s network.

**Monitor**

Once the endpoints are authorized to access the network in any capacity, Trustwave NAC monitors packets from the monitored segment. The ongoing monitoring of such endpoints allows Trustwave NAC to help enforce behavioral policies throughout the monitored segment. This view into network activity also highlights network usage patterns, providing insight to network performance and helping to avoid downtime of the monitored segment.

**Detect**

Trustwave NAC will give Client continuous control while a monitored endpoint is on your network. Trustwave NAC’s available behavioral policy enforcement protects Client’s network interior against threats without requiring signatures or updates. This technology helps minimize risk to the network from non-compliant monitored endpoints, while providing protection that is transparent to the end user.

**Re-Scan**

Trustwave NAC allows Client to designate required intervals for re-scanning to ensure endpoints start and remain compliant. This technology is used to identify changes in an endpoint’s status after a device connects to a network.