At-A-Glance

Benefits

- **Centralize and unify highly secure access control** to provide a consistent network access policy for end users whether they connect through a wired or wireless network or VPN.
- **Gain greater visibility and more accurate device identification** with Cisco ISE's superior device profiling and device profile feed service, which together reduce the number of unknown endpoints and potential threats on your network by 74 percent, on average, based on Cisco engagements.
- **Simplify guest experiences** for easier guest onboarding and administration through fully customizable branded mobile and desktop guest portals, created in minutes with dynamic visual workflows that let you easily manage every aspect of guest access.

Cisco Identity Services Engine

The enterprise network no longer sits within four secure walls. Employees today demand access to work resources from more devices and through more non-enterprise networks than ever before. Mobility is changing the way we live and work, and enterprises must support a mobile workforce to keep workers productive and stay competitive. However, a myriad of security threats as well as highly publicized data breaches clearly demonstrate the importance of securing access to this evolving enterprise network.

As the network expands, the complexity of marshaling resources, managing disparate security solutions, and controlling risk grows as well. Factor in the proliferation of the "Internet of Things," with already constrained IT resources, and the potential impact of failing to identify and remediate security threats becomes very large indeed.

A different approach is required for both the management and security of the evolving mobile enterprise. It's called the Cisco® Identity Services Engine (ISE).

Narrow Your Exposure and Reduce Your Risk

It all starts with getting ahead of threats by using visibility and control – visibility into the users and devices accessing your network and the control to help ensure that only the **right** people from the **right** devices get the **right** access to the enterprise services they need.

This is where Cisco ISE can help. Cisco ISE is the market-leading security policy management platform that unifies and automates access control to proactively enforce role-based access to enterprise networks and resources, regardless of how a user chooses to connect – by wired or wireless networks or VPN.

Traditionally, security solutions, focused on preventing compromised devices or users from gaining access to network resources, have generally been too complex to configure and deploy, requiring weeks of setup and large investments in resources.

The latest release of Cisco ISE is different. With out-of-the-box configured workflows, Cisco ISE accelerates the deployment of guest access and 802.1X RADIUS authentication. Enterprises can choose to expand their deployments and use Cisco ISE to create access policies using Cisco TrustSec® Security Group Tags (SGTs). These define access based on simple "plain English" rules and use built-in technology within the Cisco infrastructure to enforce policy across the network.

Benefits

- **Accelerate BYOD and enterprise mobility** with easy out-of-the-box setup, self-service device onboarding and management, internal device certificate management, and integrated enterprise mobility management (EMM) partner software.
- **Deploy logical network segmentation based on business rules** by using Cisco TrustSec technology to create a role-based access policy. This dynamically segments access without the complexity of multiple VLANs or the need to change the network architecture.
- **Share deep contextual data with third-party partner network and security solutions** to improve their overall efficacy as well as accelerate the identification, mitigation, and remediation of network threats.

Additionally, Cisco ISE uses Cisco Platform Exchange Grid (pxGrid) technology to share rich contextual data with integrated partner ecosystem solutions. This technology accelerates their capabilities to identify, mitigate, and remediate security threats across your extended network. Overall, secure access control is centralized and simplified to securely deliver vital business services, enhance infrastructure security, enforce compliance, and streamline service operations.

Providing control with context makes Cisco ISE a key component in the Cisco security portfolio as well as the Cisco Open Network Environment (ONE) architecture, which promotes the easier connection of people, processes, data, and things with greater intelligence and efficiency. Cisco ISE is one of the three pillars of the Cisco Unified Access solution, which lets you work your way with "One Policy, One Management, and One Network." Through its ecosystem integrations with leading security information and event management and threat defense (SIEM/TD) solutions and its secure access policy capabilities, Cisco ISE delivers the visibility, context, and dynamic control needed by enterprises to effectively implement security that targets the entire attack continuum – managing network access **before** an attack while improving detection, mitigation, and remediation **during** and **after** an attack as well.

Next Steps

To learn more about the Cisco Identity Services Engine, visit www.cisco.com/go/ise or contact your local account representative.

C45-654884-11 09/14