At-a-Glance

Manage and Protect the Mobile Enterprise

The enterprise network no longer sits within four secure walls. It extends to wherever employees and data travel. Employees today demand access to work resources from more devices and through more nonenterprise networks than ever before. Mobility and the Internet of Everything (IoE) are changing the way we live and work. Enterprises are challenged with supporting a proliferation of new network-enabled devices as a myriad of security threats and highly publicized data breaches clearly demonstrate the importance of securing access to the evolving enterprise network.

As the modern network expands, the complexity of marshaling resources, managing disparate security solutions, and controlling risk grows as well. Factor in the ubiquitous connectivity of IoE 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

Get ahead of threats. Gain deep visibility into the users and devices accessing your network and exercise dynamic control so that only the right people with the right devices get the right access to enterprise services.

The redesigned ISE 2.0 simplifies the delivery of consistent, highly secure access control across wired and wireless multivendor networks and remote VPN connections. With intelligent sensor and profiling capabilities, Cisco ISE can reach deep into the network to deliver superior visibility into who and what is accessing resources.

Through the sharing of vital contextual data with ecosystem partner integrations and the implementation of Cisco TrustSec® policy for software-defined segmentation, ISE transforms the network from simply a conduit for data into a security enforcer that reduces the time to detection and time to resolution of network threats.

Benefits

- **Centralize and unify highly secure access control** based on business role to provide a consistent network access policy for end users whether users connect through a wired or wireless network or VPN.
- **Gain greater visibility and more accurate device identification** with Cisco® Identity Services Engine (ISE) device profiling and device profile feed service, which together reduce the number of unknown endpoints.
- **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 the guest experience.
ISE 2.0 updates and enhancements include:

- Integration with the Cisco Mobility Services Engine to provide location data. You can create and enforce location-specific access so that, for example, medical professionals can access patient medical records only in the emergency room.
- Enhancement of our open architecture for certain ISE ecosystem partners, so customers can use their existing security solutions to work with ISE to identify threats in the network for rapid containment and remediation.
- Support for third-party network access devices (NADs) and IPv6 endpoints to extend the reach and scope of ISE for endpoint compliance across a more varied range of networks.
- Streamlined policy management, including simplified device administration with TACACS+ and easy wired-access capabilities, to make deploying a highly secure access control policy for wired networks much easier.
- With Cisco AnyConnect® 4.2 comes the new Network Visibility Module. This component provides a level of detail into application traffic flows previously unavailable from off-premises endpoints.

Additionally, 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, access control is centralized and simplified to deliver vital business services, enhance infrastructure security, enforce compliance, and streamline service operations, all with a high degree of security.

Through its integrations with leading security information and event management (SIEM) and threat defense solutions, its deep network visibility, and its access control capabilities, the ISE plays an integral role in the Cisco Cyber Threat Defense, Cisco “network as a sensor,” and Cisco “network as an enforcer” solutions. Ultimately, 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; providing visibility into and containment of threats during an attack; and improving time to detection (TTD) and time to resolution (TTR) after an attack.

Next Steps
To learn more about the Cisco Identity Services Engine, visit [http://www.cisco.com/go/ise](http://www.cisco.com/go/ise) or contact your local account representative.