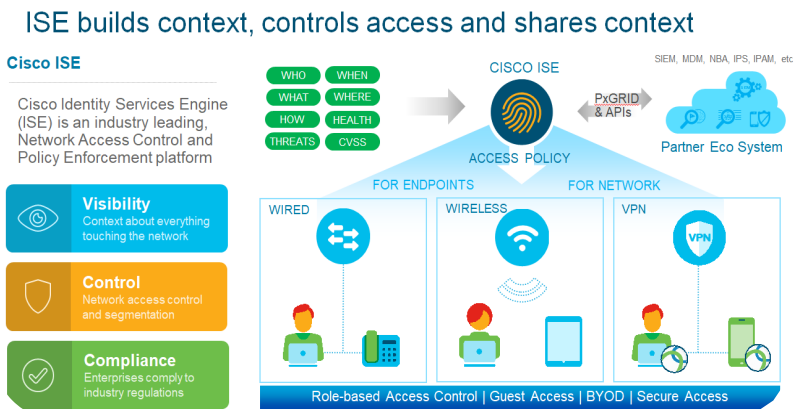
Cisco Security News Digest
02/05/2018 Issue 10

Cisco Identity Services Engine

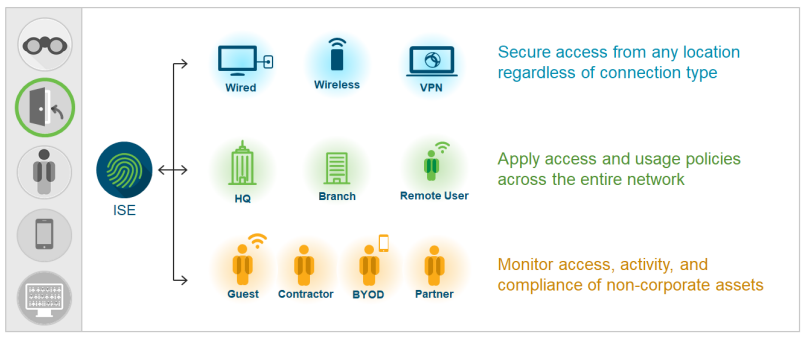
What's in your Network?

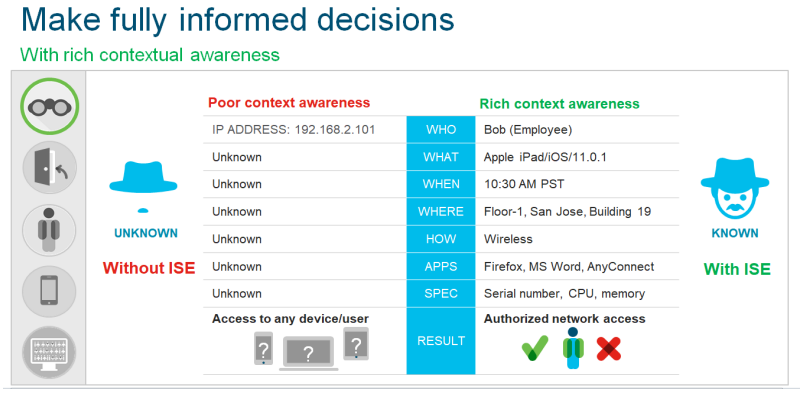
Without a new approach, it's a daunting task to see who and what is on your network. Visibility into all the users and devices connecting to the enterprise networks have become more complex today due to proliferation of mobility, cloud services that have changed the traditional network traffic flows. Adoption and new use cases for IoT network enabled devices are making visibility even more complex as most of them lack monitoring and direct user engagement thus widening the threat surface area Adding to this challenge is industry demand to deliver new digital experiences to the end users.

Cisco Identity Services Engine (ISE) is the market leading access and security policy management and enforcement platform that provides unparallel user and device visibility, intersecting it with cues from the network, applications and other security defense systems.

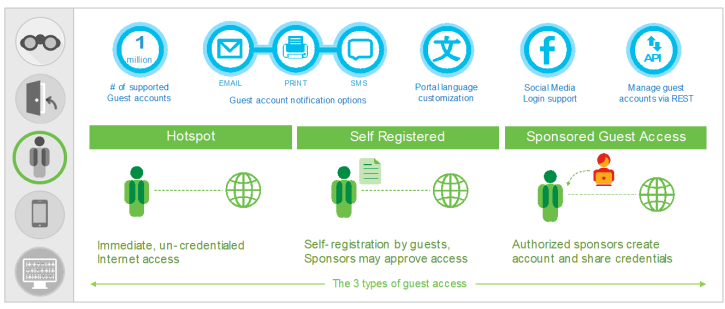


ISE can provide protected connection to all users and devices coming onto network, provide reliable security regardless of connection type or location and increase user productivity whether they are on-premises or remote. The automated profiling service in Cisco ISE identifies and collects significant amount of attribute information about devices and users that connect to your network. The out of box profilers help gather rich contextual user and device information that could centrally be monitored in ISE intuitive and customizable dashboard. This allows network and security teams to easily get deeper visibility, correlate security information from disparate tools, enforce policies, provide better threat containment and remediation. ISE also has extensive AAA server capabilities for network device administration.

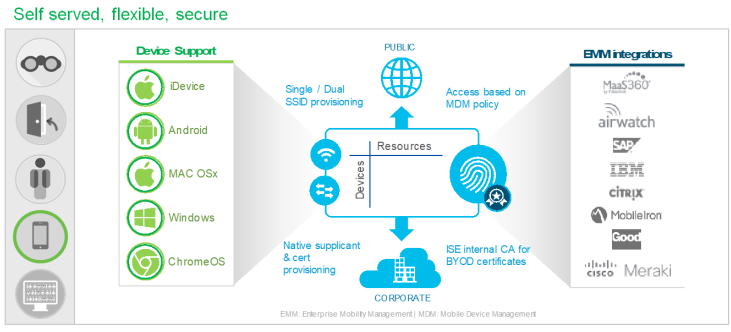


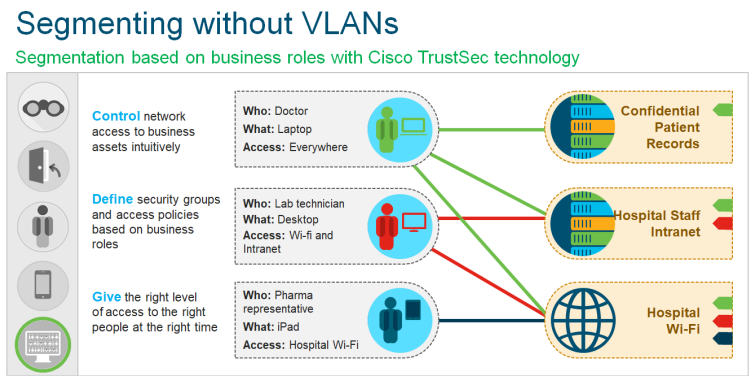


ISE guest services can provide a streamlined experience for implementing and customizing secure network access by creating a hotspot, self-service registered access, or sponsored access easily. ISE portal allows you to easily view active endpoints and provide accounting information for security, compliance, and guest auditing. Cisco ISE Portal Builder is a web-based tool that helps create dynamic and professional-looking portals for the Cisco Identity Services Engine (ISE). It can easily add company branding and communication requirements to intranet access portals. It can give guests hotspot access to branded site, complete with advertisements, while providing corporate employees with a self-service bring-your-own-device (BYOD) portal.

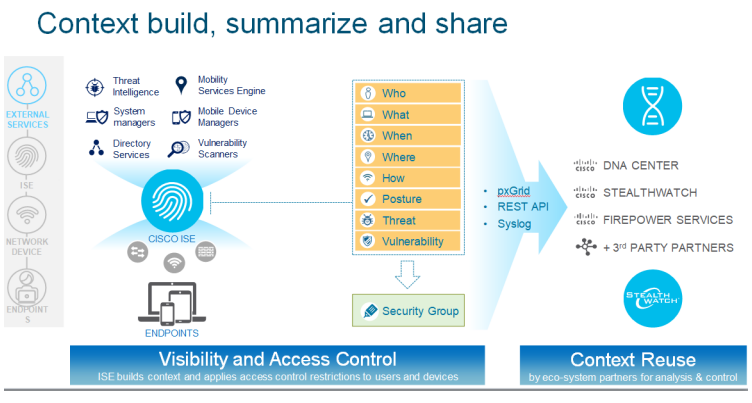


Mobility and cloud technologies have fueled the growth of BYOD in organizations. ISE allows organizations to enable their employees to participate in BYOD securely. Once on-boarded, ISE can tie in with MDM solution to further verify compliance and provide controlled access, reducing the risk. ISE could also let users manage their own devices and report a lost or stolen device for which the certificate would be revoked preventing unauthorized access.





Segmenting the network has become critical than ever before due to changes in technology landscape. Traditional VLAN based segmentation can be complex to maintain and limits scalability. Cisco TrustSec software-defined segmentation is simpler to enable than VLAN-based segmentation. Policy is defined by security groups and the process of tagging is based on contextual identity, not dependent on IP addresses schemes. This give users access that is consistently maintained as resources move across domains. Further it helps IT to avoid VLAN sprawl and segment the network without redesign. TrustSec policies could be easily propagated across the network from a simple TrustSec matrix in the dashboard.



By sharing contextual identity using a pxGrid framework, ISE can consolidate security operations through open integration with other eco-system partners and Cisco technologies. ISE can receive high fidelity actionable threat information such as Indicators of Compromise, Threat Detected events and CVSS scores from Cisco AMP to create threat-centric access policies to change the privilege of the endpoint accordingly. Cisco Firepower Management Center can enforce an organizations security policy based on ISE session attribute available through pxGrid. When Cisco Stealthwatch detects anomalous traffic, it can alert the admin the option to quarantine the user via ISE.

For more information on Cisco Security solutions and products, please contact your **Cisco Account Manager**

Suggestions/comments on this newsletter contact Joby James at jobyj@cisco.com
Newsletter Archive: http://cs.co/SecurityNewsDigest

Free, 90-day ISE Evaluations: http://cs.co/ise-eval
ISE Deployment Assistant: IDA
ISE Public Community: http://cs.co/ise-community
ISE YouTube Channel: http://cs.co/ise-videos
ISE Compatibility Guides: http://cs.co/ise-compatibility
ISE Design & Integration Guides: http://cs.co/ise-guides