Cisco Identity Services Engine

Asset Visibility

Visibility might be the most overused word in cybersecurity today.

An internet search for “cyber visibility” yields thousands and thousands of results. Additional searches on the name of any cybersecurity vendor paired with “visibility” undoubtedly shows that word splattered across their materials. It might leave you with the impression that “visibility” just the latest marketing buzzword and nothing more.

Don’t let it blind you. Remember that many cyber threats are either unknown or cleverly hidden from view. For example, our Chief Information Security Officer (CISO) Benchmark Study for 2019 begins with “See No Evil, Block No Evil” because nearly a quarter of participants said that threats from rogue employees or careless contractors are the most serious risks to their organizations. With all we know about cyber defenses today, why do CISOs still cite this as their biggest concern in 2019?

The reason is that “seeing” has just gotten so much harder.

© 2019 Cisco and/or its affiliates. All rights reserved.

What’s making asset visibility so difficult?

- People are bringing their own devices into the workplace
- People are working from wherever they are
- Business apps are no longer confined to the traditional data center
- New Internet of Things (IoT) devices are constantly being deployed

With Cisco ISE, you can:

- Grant and control the right level of network access
- Improve your security posture and quickly contain breaches
- Gain complete endpoint visibility with context
- Streamline your access control policy management

Licensing

Asset Visibility requires the **Plus** license if you assign the asset's profile to an authorization policy. Check out the Ordering Guide to learn more.

Learn More

To learn more, please visit https://www.cisco.com/go/ise or contact your account representative.

Cisco ISE delivers essential visibility and control

Cisco Identity Services Engine (ISE) makes it easy to gain visibility and control over who and what's on your network consistently across wireless, wired, and VPN connections. Asset visibility is just one of several use cases that makes ISE a critical part of your cybersecurity program.

Device profiling is the heart of asset visibility. ISE uses active probes and device sensors to listen to the way devices connect to the network. It then compares that gathered information with its extensive profile database to classify the device. For IoT devices, ISE supports the Manufacturer Usage Description (MUD) standard that allows device manufacturers to disclose device types and their intended purposes.

With Cisco ISE, you'll get the visibility and context you need to grant just the right level of network access... and nothing beyond what's appropriate.

Context	Without ISE	With ISE
Who	192.168.2.101	✓ Robert Smith (Employee)
What	Unknown	✓ Apple iPhone / iOS 12.3.1
When	Unknown	✓ 10:30 AM PST
Where	Unknown	✓ Floor-1, San Jose, Building 19
How	Unknown	✓ Wireless
Apps	Unknown	✓ Chrome, WebEx, AnyConnect
Spec	Unknown	✓ Serial number, CPU, memory
Result	Permit or Deny	✓ Authorized network access only

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R) 07/19