Cisco Identity Services Engine (ISE)

Dynamic Visibility

See everything and take back the network

What is dynamic visibility? Well, it is just that, dynamic. It is fluid and moving. It is not assuming trust and allowing access based only on a single identifier such as login credentials, device ID, or a MAC address.

Dynamic visibility has context that can be verified to keep up with threats, so your endpoint's posture and risk levels are continuously updated without the use of agents. Dynamic visibility recognizes that authentication and authorization do not happen just once. It is continual and re-accomplished at decision points throughout the network, closest to the resource to maintain a zero-trust framework and increase organizational posture.

Yes, organizations do not have enough visibility. But it is just not about quantity; it is about getting the right visibility into endpoints only to allow access based on least privilege. And this must be accomplished continually as the endpoint moves throughout the network, regardless of its location. This is dynamic visibility for zero trust in the workplace.

Benefits

- Conquer endpoint visibility challenges and become all-seeing and all-knowing
- Improve security posture and automate threat containment
- Streamline access control and policy management
- Increase endpoint visibility into unmanaged devices without agents
- Embrace zero trust and gain visibility required for network segmentation

Gain visibility that is dynamic to keep up with threats

The agentless approach of Cisco Identity Services Engine (ISE) identifies all connected endpoints by several device identifiers to correctly classify endpoint type and apply policy based on profiled groups. Gaining granular visibility gives you the granular control required to ensure your access policy provides protection without disrupting the business intent across wired, wireless, and VPN connections.

Endpoint visibility is continually updated and maintained to ensure that the proper authorization policy is applied before access is granted. To maintain compliance, the endpoint's posture is updated with or without the use of agents to give teams the flexibility they require to balance meeting business objectives with reducing organizational risk. Increased visibility and intelligence are provided through integration with third-party solutions, both on-premises and in the cloud* to keep up with the ever-changing threat landscape and to give you an active arm of protection within the network. With dynamic visibility, organizations are gaining the asset inventories they need. More importantly, they are taking the next step in building and providing visibility into profiled endpoints required to build network segmentation and zero trust within the workplace.

> "With Cisco ISE, IT operation has become easy."
>
> Munish Dhiman, Consultant
> Tata Consultancy Services

Beginning with Cisco ISE 3.3, network visibility will improve even more as pxGrid Direct Visibility has seen an improved transparency from the last iteration of Cisco ISE (ISE 3.2). Now users are able to get improved endpoint attributes via external databases such as Service Now. So whether the data comes from endpoints, users, devices or which apps are running over the network and its different attributes, it provides a lot of information such as the device type and owner and other things like whether the device is operational.

A Cisco-only feature called Wi-Fi Edge Analytics will allow network admins to mine data from Apple, Intel and Samsung devices to better improve profiling. Cisco Catalyst 9800 wireless controllers will pass along endpoint-specific attributes, such as model, OS version, firmware, among others, to ISE via RADIUS. From there this information will be used to profile common endpoints found on the network.

Getting this network data from both sources in an easily accessible fashion allowing network admins to make better decisions based on facts.

This data can then be spun to run the network in a more efficient manner allowing for a safer network and less time spent on translating information.

Gaining visibility into network endpoints is the first step in adopting a zero-trust framework in the workplace and gaining the control you need to provide secure access to all connections on the network. Read the Visibility-Driven Segmentation use case to learn how to control policy.

Learn more: cisco.com/go/ise