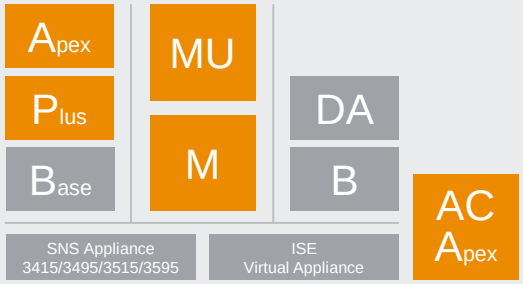
Cisco ISE Offerings

Cisco ISE appliances and software licenses are packaged and priced separately.



Licenses and Functionality

- **Base (B)** – 802.1X, guest mgmt, TrustSec
- **Plus (P)** – BYOD onboarding (with Certification Authority), profiling and feed services, pxGrid
- **Apex (A)** – Posture assessment, remediation, Enterprise Mobility Management (EMM) integration
- **Mobility (M)** – Combination of Base, Plus and Apex for wireless and VPN endpoints
- **Mobility Upgrade (MU)** – Adds wired support to mobility license
- **Device Administration (DA)** – TACACS+ for network device administration
- **AnyConnect Apex (AC Apex)** – AnyConnect Apex license for some posture assessment use cases

Appliances and Node Personas

Cisco ISE appliance nodes can have personas that provide different deployment functions. All personas can run on a single appliance or each persona can run on a dedicated appliance.

- **Policy Administration Node (PAN)** – Manage deployment and policy configuration
- **Policy Service Node (PSN)** – Implement policy decisions and host RADIUS server
- **Monitoring & Troubleshooting Node (MnT)** – Log collector and storage
- **pxGrid Node** – Facilitates information sharing with other Cisco and third-party products

Cisco Claims	ForeScout Response
To be effective, ForeScout requires appliances and SPAN traffic at each site	ForeScout can be deployed effectively in a centralized, distributed or hybrid manner. In centralized deployments, appliances are not required at each site. Additionally, SPAN traffic is only one of several monitoring and profiling techniques used – others include NetFlow, DHCP, DNS, HTTP user agent, SNMP traps, authentication requests, switch, wireless, VPN, firewall and AD integrations.
ForeScout is not truly agentless. It requires SecureConnector agent for full endpoint visibility and control.	ForeScout does not require agents for endpoint discovery, classification, authentication and network access controls for managed and unmanaged devices. Compliance assessment can also be performed without an agent using credentials for remote inspection. For BYOD posture assessment, SecureConnector can be auto-installed temporarily and dissolves upon reboot.
ForeScout doesn't have built-in Certificate Authority (CA) and end-user self-service BYOD	ForeScout provides self-BYOD onboarding using employee's corporate credentials and also supports posture assessment for Windows, Mac and Linux BYOD. While ForeScout doesn't provide a built-in CA, we work with customers' existing CA for certificate-based onboarding.
ForeScout lacks complete guest lifecycle management solution	ForeScout provides a robust guest management solution for both wired and wireless deployments without dependency on 802.1X. Various guest workflows such hotspots, self service and sponsor portal are supported.
ForeScout does not perform pre-admission compliance assessment	Just like Cisco ISE, ForeScout requires an endpoint to have an IP address for deep posture assessment. However, if required, ForeScout can use network controls (ACLs, VLANs, virtual firewall) to restrict endpoint access during the posture assessment. Cisco ISE uses a similar approach to restrict endpoint access during posture assessment by means of ACLs.
Cisco's market leadership in network infrastructure and NAC experience make ISE the natural choice for large customers	ForeScout works in heterogeneous network environments with support for 20+ switch and 7+ wireless vendors, including Cisco. Feedback from large customers with Cisco network infrastructure indicates that ForeScout is fast to deploy, easy to manage, non-disruptive and scalable across their Cisco environment.
ForeScout does not support TACACS+ for network device authentication and authorization for administrators	True. However, best practices recommend separating network device administration from endpoint discovery, classification, authentication and assessment. Even Cisco advocates this separation, and when deploying ISE 2.x for network device administration and authentication, Cisco requires customers to purchase a separate ISE device administration license and additional appliance capacity, hence treating it like a separate product deployment. Additionally, ISE does not currently have TACACS+ feature parity with Cisco ACS. Cisco has not yet EOL'ed ACS and continues to release new versions such as ACS 5.8.
ForeScout requires separately licensed Modules for integrations with third-party products	ForeScout provides base integrations with 60+ third-party products that are included in the CounterACT license at no additional cost. Only Extended Modules for security orchestration are licensed separately.

ForeScout Strengths

- **Agentless solution.** Provides visibility and control of corporate, BYOD, guest/contractor and IoT devices on the network. Offers real-time asset intelligence via the built-in and searchable inventory tool.
- **Heterogeneous support.** ForeScout integrates with 20+ switch and 7+ wireless vendors for ease of deployment in multi-vendor networks, without the need for hardware and software upgrades to support 802.1X.
- **Easy to deploy and manage.** Non-disruptive, out-of-band deployment with built-in configuration wizards and customizable policy templates for rapid time-to-value.
- **Robust non-802.1X architecture.** Direct integration with network infrastructure devices and directory services provides an easier non-802.1X alternative that is well suited for environments with increasing number of BYOD, guest/contractor and IoT devices.
- **Security Orchestration.** Bi-directional information sharing and workflow automation with security technologies such as Advanced Threat Detection (ATD), Vulnerability Assessment (VA), Enterprise Mobility Management (EMM), Next-gen firewalls, Endpoint Protection Platforms (EPP), Security Information and Event Management (SIEM) etc. help accelerate system-wide response and achieve operational efficiencies.

Cisco Weaknesses

- **Reliance on 802.1X.** Cisco ISE is largely reliant on 802.1X, which presents several deployment, operational and troubleshooting challenges, especially on wired networks. This increases the total cost to deploy and maintain the solution. Dependence on 802.1X usually necessitates manually maintaining a MAC address whitelist for IoT & other non-802.1X capable devices, increasing IT overhead and impacting security due to risk of MAC spoofing. The Easy Connect feature in ISE 2.1 only provides non-802.1X authentication for corporate Windows machines connecting to wired networks (still requires agent for assessment).
- **Limited network device support.** ISE integrates with only 4 switch and 4 wireless vendors. Also, several profiling, posture assessment and guest/BYOD onboarding features may require network devices to support Change of Authorization (CoA) and URL-Redirect. This can necessitate H/W and S/W upgrades prior to an ISE deployment.
- **Agent required for posture assessment.** Cisco ISE requires either the NAC agent or the AnyConnect agent with ISE posture module for posture assessment and remediation. For certain posture use cases, customers have to purchase the AnyConnect agent Apex license for all endpoints that are to be assessed. This is in addition to the ISE Apex license.
- **Limited posture assessment and remediation features.** ISE does not provide posture assessment of Linux endpoints or inventory of applications, processes and open ports on an endpoint. In addition, ISE does not include remediation actions such as kill processes, run scripts, set registry keys or disable dual-homed device adaptors.
- **Limited third-party integration and security orchestration.** Cisco ISE does not currently integrate with leading non-Cisco ATD and Threat Intelligence platforms (such as those from FireEye, Palo Alto and McAfee) for automating threat response. ISE does not provide IOC scanning to discover and mitigate threats from infected endpoints.

COMPARISON	ForeScout	Cisco
SEE		
Endpoint profiling	Yes	Requires ISE Plus license
Posture assessment	Yes	Requires ISE Apex license[1]
Agentless assessment	Yes[2]	No
Software inventory	Comprehensive/searchable	No[3]
CONTROL		
Non-802.1X option	Yes	Limited[4]
Wired/wireless 802.1X	Yes	Yes
Self-service BYOD	Yes	Yes
Built-in CA	No[5]	Yes
Wired/wireless guest	Yes	Yes
Policy engine	Easy and intuitive with compound Boolean policies[6]	Complex with disjointed auth and posture policies
Response actions	Yes	Limited[7]
ORCHESTRATE		
EMM integration	Yes	Yes
IOC scanning	Yes	No
EPP integration	Advanced	Basic[8]
VMware integration	Yes	No
Integration architecture	ControlFabric	pxGrid
DEPLOY / MANAGE		
Multi-vendor support	20+ switch, 7+ wireless	4 switch, 4 wireless
Scalability (deployment)	Up to 1M endpoints	Up to 500K endpoints
Built-in TACACS+	No	Yes

[1] May also require AnyConnect agent Apex license for some posture assessment use cases
[2] Using remote inspection with credentials
[3] Software information is limited to on-demand queries
[4] Easy Connect is only for corporate Windows machines on wired networks
[5] ForeScout integrates with existing CA
[6] Compound policies that incorporate classification, posture, access, remediation and orchestration
[7] Lacks capabilities such as kill process, run scripts, set registry, HTTP notification, VM controls etc.
[8] Only check if AV is installed and bring it up-to-date. No orchestration with EPP management system.