

Cisco pxGrid and McAfee OpenDXL integration for Cisco ISE, McAfee ePO and threat response Ecosystem

Enable consistent access policy and threat response from network to endpoint with Cisco, McAfee and Alliance Partners

Cisco® pxGrid and McAfee OpenDXL are open frameworks that support multivendor, cross-platform collaboration on network systems, including security monitoring and detection systems, network policy platforms, identity and access management platforms, and virtually any other IT operations platform. Cisco and McAfee have integrated our respective security fabrics as well as the Cisco Identity Services Engine (ISE) and McAfee® ePolicy Orchestrator® (ePO). Together, they deliver:

- Coordinated network and endpoint threat responses
- Comprehensive visibility into network-attached endpoints
- Threat response interoperability among our respective vendor partner ecosystems

Cisco ISE provides a wealth of user identity, endpoint device, and network context information that is useful to many IT platforms. To bring greater insight to risky user activities on the network, and to mitigate those events, Cisco ISE uses the pxGrid technology to share its network-attached endpoint session inventory with OpenDXL. The information is then relayed to McAfee ePO. This process provides ePO with visibility of endpoints that it may not have under its management. ePO can then determine whether to bring a newly discovered endpoint under management. Similarly, Cisco ISE can detect whether an endpoint has McAfee ePO installed and can create network access policy based on its presence.

Benefits

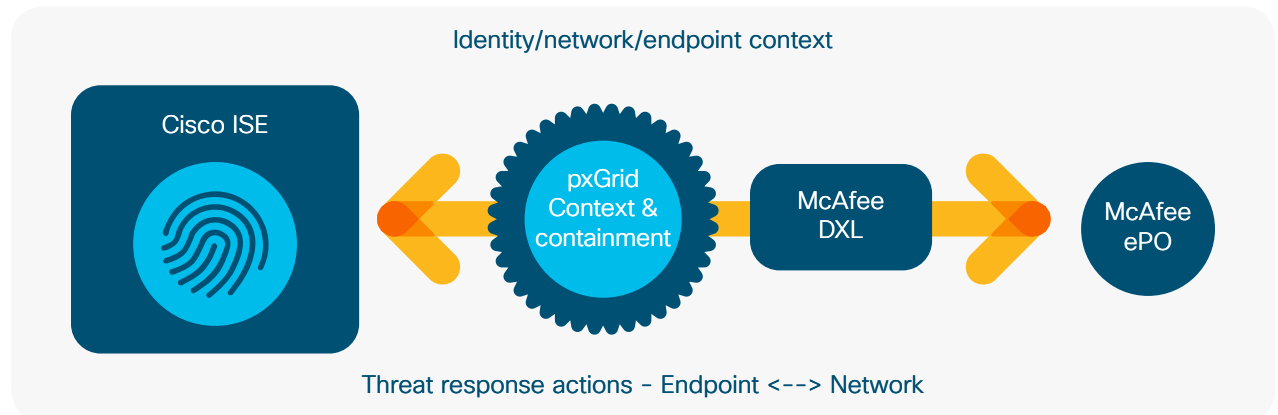
- Simplify and expedite security threat response from network to endpoint
- Deploy Cisco ISE for comprehensive network endpoint visibility for McAfee ePO
- Enforce network access policies in McAfee ePO environments
- Utilize an ecosystem of nearly 100 vendors that can collaborate on network and endpoint threat response

How the integration works

This solution is composed of Cisco ISE running pxGrid context exchange and Cisco Rapid Threat Containment (RTC) capabilities, an ISE Plus or Advanced Feature license, and McAfee ePO.

- pxGrid and DXL share ISE and ePO context, as well as information about the threat response actions each has taken.
- Cisco ISE provides its network user and device session inventory over Open DXL to ePO. ePO matches this information to devices it has under management.
- Cisco ISE detects if an endpoint has McAfee ePO installed. ISE can differentiate the network access privilege of the endpoint based on whether ePO is installed or not.
- ePO informs ISE when it has taken an endpoint remediation action in response to a security threat. ISE may then make an appropriate network access threat response using its Rapid Threat Containment function.
- ISE informs ePO when it has responded to a security threat. ePO may then make an appropriate endpoint threat response.

Cisco ISE plus McAfee ePO: Network and endpoint visibility and threat response



ISE and ePO can also inform each other when one has responded to a threat. The other can then respond according to its respective policy. The threat response is more effective because the endpoint and network take the appropriate actions for the threat conditions.

Integration between pxGrid and OpenDXL also helps our respective threat response ecosystem partners collaborate through Cisco ISE and McAfee ePO. When a partner responds to a threat through pxGrid or OpenDXL, that response is captured and relayed to ISE and ePO for their own threat response. This integration delivers a combined threat response partner community composed of nearly 100 vendors from every type of security technology, as well as a growing set of contributions from an open source community.

This suite of endpoint and network collaboration capabilities resulting from Cisco pxGrid and McAfee OpenDXL integration streamlines endpoint security management and threat response. It reduces the time it takes to remediate network security threats as well as respond to inappropriate network use.

Next steps

To learn more about the Cisco Identity Services Engine, visit the [ISE webpage](#).

To learn more about Cisco pxGrid, visit the [pxGrid webpage](#).

To learn more about McAfee OpenDXL, visit <http://opendxl.com>.

For additional information regarding Identity Services Engine and other partner integrations, visit <http://www.cisco.com/c/en/us/products/security/partner-ecosystem.html>.