SOLUTION BRIEF

Integrated McAfee and Cisco Fabrics Demolish Enterprise Boundaries

First united and open ecosystem to support enterprise-wide visibility and rapid response

The cybersecurity industry needs a more efficient way to counter adversaries. Now, Cisco and McAfee have interconnected their platforms and ecosystems for comprehensive visibility, threat context sharing, and real-time security orchestration based on policies. Together, we lay the foundation for a universal, unified, and nimble infrastructure for threat detection and response. With this solution, DXL brokers bridge to Cisco pxGrid Controllers for bi-directional, one-to-many communication and shared services between these fabrics. Now, high-speed messaging and automated workflows can maximize the value of contextual, threat, network, and endpoint data by sharing it with any connected application. This ground-breaking integration links two ecosystems and leverages the open source OpenDXL initiative to help enterprises reduce friction, gaps, and delays that hinder effective security operations. Truly, together is power.

McAfee Compatible Solutions

- DXL 4.0 as the messaging fabric
- Cisco ISE version 2.0 or later running pxGrid
- McAfee® ePolicy Orchestrator® 5.3 or higher

Unite Endpoint, Network, and Security Operations

The Data Exchange Layer (DXL) threat intelligence fabric now interoperates with pxGrid, Cisco's open security information grid, to share contextual information and execute threat mitigation actions between and among any application connected to either fabric. The new bridge shares identity and threat intelligence in real time and supports automated threat response workflows across the security industry's largest joint community of vendors and open source applications.

This unified integration fabric provides maximum utility for each application, dramatically increasing the value to customers and vendors of any single product while slashing the amount of time spent developing and maintaining integrations. Through the OpenDXL initiative, open source and in-house developed applications can also share and interact with little effort. Furthermore, organizations can extend the lifespan of existing security and IT systems and add new analytics, monitoring, and response capabilities without uprooting legacy or investing in entirely new systems.

Clear the Integration Hurdle

Enterprises are embracing integration and automation as a way of shortening threat mitigation and response cycles. However, traditional integration models that connect individual applications directly are expensive to create and maintain and become brittle over time as applications change. Few organizations have the time or expertise to get past this obstacle. They are left to manually gather data and implement policy and process updates.

In addition, product boundaries constrain precious event, alert, and threat data that could make the difference between confident action and the risky "wait and see" approach. For example, insight found at the endpoint about a known threat is often not being leveraged at network threat vectors due to manual ticketing processes and operational boundaries. The resulting threat mitigation and remediation experience takes more time, more resources, and is less secure than a fully automated threat defense lifecycle. If the data is available, it traditionally arrives via batch and scheduled processes, after its peak utility.

Thanks to the integration between pxGrid and DXL, now enterprises and service providers can leverage extensible and off-the-shelf integrations and a high-speed messaging fabric to automate and accelerate processes across silos of tools and operations.

Challenges

- Integration cost and barriers slow data sharing and degrade data fidelity
- Manual integration and response increase risk
- New functionality disrupts operations and add complexity
- Stand-alone services reduce visibility and add management overhead

Joint Solution

- Cisco and McAfee have integrated the pxGrid and Data Exchange Layer fabrics to share data and enable end-to-end threat mitigation, between and among any application connected to either fabric at maximum speed across vendors

Results

- Less time and effort spent on integration
- More accurate and immediate decisions with higher confidence than ever before possible
- Reduced response time and manual troubleshooting through use of custom, automated policy actions

Mitigate Threats End to End, Seamlessly

Gain comprehensive visibility

The pxGrid to DXL integration is bi-directional: data flows between the Cisco and the McAfee worlds, plus OpenDXL-integrated applications. Analysts and administrators have unprecedented system-wide visibility to detailed network, user/endpoint privilege level, sensor, and real-time network-attached asset state data. They can improve decision with high fidelity, freshly collected data such as:

- What devices are attached to my network?
- What is a new device's security posture?
- What level of network privilege does it have?
- Is this event likely to be bad?
- Which actions can I take now to reduce or mitigate risk?

In addition to informing the security team, answers to these questions are highly valuable to operations and analytics tools that can incorporate this data in their calculations.

Automate rapid response

The integration extends the options for automated, policy-driven responses by increasing interactions throughout endpoint, network, and security operations. This pervasive expansion from monitoring and detection to active mitigation and containment reduces the vulnerability window and the potential dwell time of an attacker. It makes the best use of the services, their data, and the people that oversee them.

Share services end to end

With this solution, data flows one to many across the messaging bus. Threat response actions published over DXL by McAfee® ePolicy Orchestrator® (McAfee ePO™) software can be picked up by Cisco Identity Services Engine (Cisco ISE) and Cisco Threat Defense platforms, plus pxGrid partners. Services integrated with pxGrid can also direct DXL-integrated products from the McAfee portfolio, the McAfee Security Innovation Alliance, and the OpenDXL community.

For instance, network session telemetry from ISE becomes visible to McAfee ePO software, which can interpret which sessions are legitimate and initiate actions to shut down connections to specific endpoints or issue blocking to IP addresses, domains, or URLs. Or, an unmanaged device detected by Cisco ISE could be added to the McAfee ePO software asset database and quarantined or given only minimal or guest network and data access until it had been brought into compliance.

Containment policies for the new host could include an immediate scan of related endpoints, automatic placement of files in the quarantine portal, software updates, and malware deletion. These steps are traditionally manual, triggered after the user calls the help desk and asks about being kept out or disconnected.

Similarly, an infected or suspicious host flagged by McAfee Endpoint Security could trigger isolation or restricted network access privileges by Cisco ISE. Cisco

DXL/Cisco pxGrid Integration

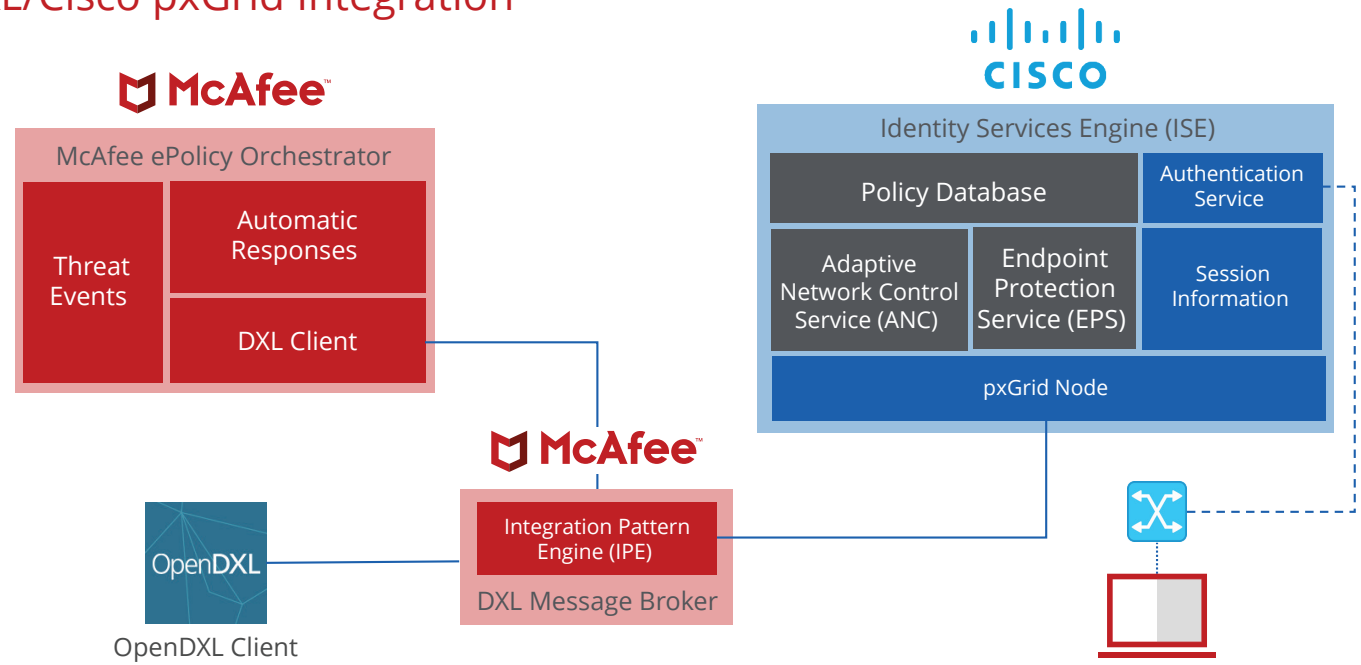

Figure 1. An engine bridges policies across DXL and ISE to connect services across application ecosystems.

response options extend to adjusting dynamic access control lists (ACLs) on switches or increased inspection by network intrusion prevention systems.

Data published to pxGrid and over the DXL bridge can also become part of analytics, indicator of compromise (IoC) hunting, and integrated monitoring within McAfee Enterprise Security Manager. DXL events can be used in a correlation rule or watch list, for instance, to trigger an alarm if a high-sensitivity asset behaves unusually.

Centrally visualize, configure, and monitor services

Data-sharing relationships and automated responses can be defined within the new interactive OpenDXL Console. This new fabric monitor provides an easy way to see available services, invoke requests or responses, and subscribe to or publish an event. To enable the McAfee-Cisco solution, an integrated pattern engine bridges McAfee ePO software policies with pxGrid policies for transparent interoperation.

About pxGrid

Cisco pxGrid is an open framework that enables multivendor, cross-platform network system collaboration among IT infrastructure, such as security monitoring and detection systems, network policy platforms, identity and access management platforms, and virtually any other IT operations platform.

About Cisco ISE

The Cisco Identity Services Engine (Cisco ISE) allows you to see and control network access policy for users and devices connecting to the corporate network. It does all this from a central policy location.

About the Data Exchange Layer

Bringing high-speed messaging to security systems, the Data Exchange Layer provides a universal fabric for exchanging data in real time. It leverages a one-to-many integration model so each application can publish and subscribe to messages over a common communication system.

About OpenDXL

As an open source initiative, OpenDXL increases the variety of services running over Data Exchange Layer. The OpenDXL.com community uses an SDK and their creativity to invent an expanding range of tools, integrations, and applications that overcome the integration hurdles of security software. In addition to many open source and commercial product integrations, a growing set of utilities, including the OpenDXL Console, are featured on opendxl.com.

About McAfee ePolicy Orchestrator

The DXL-pxGrid bridge expands the reach of the McAfee ePO software single-agent and single-console architecture that provides policy-based management for McAfee, third-party partners, and enterprises. In addition to publicizing threat events over DXL, a McAfee ePO software automated response can trigger actions by connected services. To integrate OpenDXL services into McAfee ePO software, the community can use an OpenDXL service wrapper and other tools at OpenDXL.com.

About McAfee Enterprise Security Manager

The foundation of the security information and event management (SIEM) solution from McAfee delivers performance, actionable intelligence, and real-time situational awareness at the speed and scale required for security organizations to identify, understand, and respond to stealthy threats, while the embedded compliance framework simplifies compliance.

To Get Started

- **Enterprises:** View and download OpenDXL integrations from OpenDXL.com, including open source integrations contributed by the community. Download the OpenDXL Console to configure integrations.
- **Developers:** To create new services to run across these fabrics, developers should access the OpenDXL SDK, the OpenDXL Docker Container and other tools, and the Cisco integration via OpenDXL.com.

Learn More

The integration and components are freely available.

www.opendxl.com
www.mcafee.com
cisco.com/go/pxgrid

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com