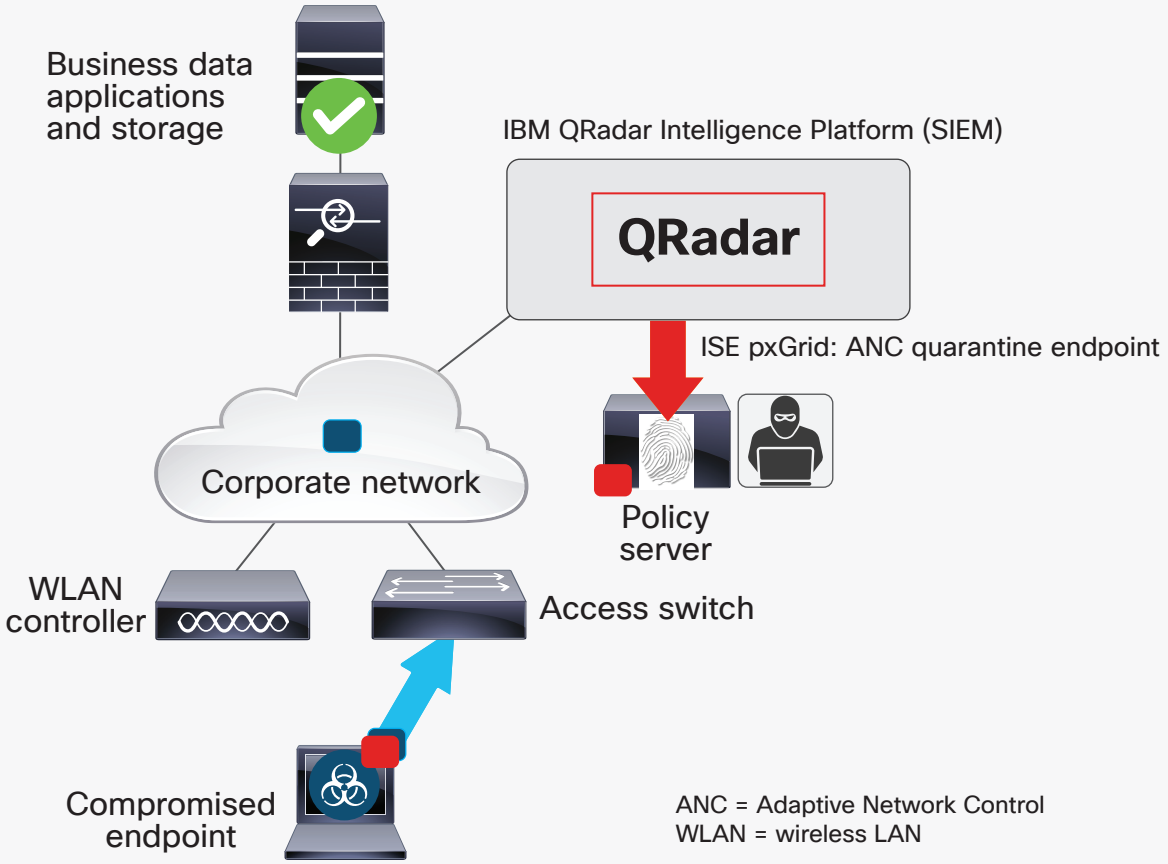
Prevent and Contain Threats with the Cisco ISE pxGrid app for IBM QRadar

What if you could streamline the enforcement of user and device policies, contain threats, and accelerate incident investigations? The Cisco Security and IBM partnership provides security analysts with the tools to streamline security operations.

Benefits

- **Detect, contain, and remediate insider threats** by identifying "at-risk" users and devices
- **Enforce policies and contain threats everywhere** from the network to the endpoint and cloud
- **Gain full visibility of all users and devices** and see authentication and remediation data in a single interface
- **Eliminate blind spots** created by unknown or unmanaged devices roaming on the network, including Internet of Things devices
- **Simplify remediation efforts** in complex security deployments by implementing quarantine actions directly from the QRadar interface

Architecture of the ISE pxGrid and QRadar integration



Overview

The Cisco® ISE pxGrid app consumes contextual data from the pxGrid node. Details are displayed as user and device activity in the QRadar dashboard. Security analysts gain a holistic view that helps them expedite their investigation of, and subsequent actions on affected devices.

The pxGrid and QRadar integration gives you deeper insights into risky user behavior. It analyzes user and device activities in the network data, on endpoints, and in the cloud. It provides details such as user name, IP address, MAC address, and device type, among other information, and displays the data in the QRadar dashboard.

Downloadable through the IBM Security App Exchange, the pxGrid app helps security analysts use QRadar to quickly assess the significance of user-centric events. It correlates contextual data such as identities, privilege levels, locations, services being used, and device types (for example, mobile and personal devices).

This integration helps streamline security operations, so teams can quickly investigate and remediate threats.

Security Outcomes

Get answers faster

With this integration, you can organize all relevant threat information on one analysis platform instead of conducting lengthy investigations and traversing from system to system. It's easier to see and understand threats and vulnerabilities on a single product.

Stop attacks faster

When you've recognized a security event, you can take immediate action to stop it by directing ISE to contain the device from QRadar. With integrated network access control technology, you can change your users' access privileges when suspicious activity, a threat, or vulnerabilities have been discovered. Devices that are suspected of being infected can be denied access to critical data while their users can keep working on less critical applications.

Key Capabilities

With its deep network visibility, and its secure access control capabilities, ISE pxGrid controls who gets onto your network all through the QRadar SIEM console.

ISE uses **Cisco Platform Exchange Grid (pxGrid)** technology to share rich contextual data with the IBM QRadar Security Intelligence platform. pxGrid is an Internet Engineering Task Force (IETF) standards-based way to accelerate your ability to identify, mitigate, and remediate security threats across your extended network.

Construct a software-defined segmentation policy to contain network threats. Use Cisco TrustSec technology to enforce role-based access control at the routing, switching, and firewall layer. Dynamically segment access without VLAN complexity or the need for network redesign.

Share user and device data with partner network and security solutions. Improve their overall efficacy and accelerate the time to containment of network threats. Affected users and devices are displayed in the QRadar dashboard.

The Cisco Security and IBM advantage

The ongoing collaboration between IBM Security and Cisco is helping organizations strengthen their posture against increasingly sophisticated cyberattacks. Rather than working in silos, as is the industry norm, these two leading security providers are collaborating to build solutions and share threat information that will empower clients to see a threat once, act at extreme speed and scale, and protect everywhere.

Call to Action

Next steps

For additional information, visit: http://cs.co/ibmsec.

For opportunities and connections email:
IBM: cisco-ibm-security@us.ibm.com
Cisco: cisco-ibm-security@cisco.com

Download the app for free at https://www.ibm.com/security/community/app-exchange.

C22-740603-00 05/18