

Cisco pxGrid: Automate Multi-Platform Communications through a Unified Architecture

What You Will Learn

IT Environments are drowning in a deluge of network and security information, adding complexity to security operations and deploying threat response. Traditional APIs are too limited, insecure and platform specific to provides a practical solution. Cisco Platform Exchange Grid (pxGrid) provides a way for all of the diverse multivendor platforms in the environment to exchange information securely, in a tightly controlled bi-directional manner. This occurs automatically in real time, without relying on platform specific APIs.

This paper discusses:

- The operational challenges customers face today when dealing with multiple security systems that don't communicate or interoperate
- How Cisco Platform Exchange Grid (pxGrid) enables immediate, automated inter-system communications
- The Cisco Platform Exchange Grid (pxGrid) architecture and operations
- How developers can start integrating their platforms with pxGrid today to enable context exchange between their platforms and Cisco security products, as well as well as with other pxGrid enabled development partners

A Growing Security and Operational Challenge

To keep the IT environment secure and running smoothly, businesses already use a wide range of tools and platforms, often from different vendors. These can include identity and access management (IAM) platforms, policy platforms, security information and event management (SIEM) systems, threat defense systems, and many others. All of these tools are critical to protect the business and safeguard their operations. But they don't talk to each other, creating multiple "silos" of information and a huge operational challenge.

Swiveling from one tool to another adds a lot of complexity - and cost - to security operations effort. It also reduces the overall effectiveness of IT security, because it can take a long time, and a great deal of manual effort, to get the information needed from each of these tools to take the appropriate security action or respond to a threat. That's time that businesses can't afford when an advanced attack is seeking to burrow deeper into the environment or exfiltrate sensitive data.

The traditional answer to this problem was to use platform APIs to help platforms share information. But in modern IT environments, this approach doesn't scale. APIs are historically specific, single-purpose integrations between one system and another. The number of platforms that need to share information today is just too large; businesses can't realistically implement single-purpose APIs linking every tool to every other tool.

In the first place, those APIs just don't exist. The on-going development effort for vendors to maintain dozens of single-purpose APIs, and to retest all of them for every minor software update, would be enormous. And even if they were able to do so, businesses would quickly be overwhelmed with information. APIs work on a basic polling model, just sending requests for information over and over again. This type of communication might be fine for one or two systems communicating this way. But 20 systems doing that at the same time would create a huge performance and scalability problem.

APIs are also usually not secure. Often, they rely on simple (and relatively weak) username-and-password authentication. They typically don't offer authorization capabilities over how that data is used. Once an API opens a doorway into a system, other systems can get access to that information and do what they want with it.

Businesses are left with a difficult security operations challenge that they can't afford to lose, and no easy way to address it. Wouldn't it be better if all the diverse tools in the IT environment could talk to each other? What if platform vendors could draw contextual information and capabilities from the other systems in the environment and give the operations staff everything they need to solve real-world problems and respond to threats faster?

That's exactly what Cisco pxGrid provides.

Introducing pxGrid

pxGrid provides a common transport language between the various network and security systems in the IT environment. Instead of each system having to rely on single-purpose APIs, they can all be integrated once with pxGrid to share contextual information with each other. Intersystem communications can now happen automatically and immediately, with no manual intervention required.

pxGrid enables multivendor, cross-platform network system collaboration among multiple parts of the IT infrastructure. These can include security monitoring and detection systems, network-policy platforms, asset and configuration management, identity and access management platforms, and virtually any other IT operations platform. IT and security vendors can use pxGrid to share context with Cisco platforms that use pxGrid, as well as with systems from any other pxGrid ecosystem partner. With this unified framework, they can share context bidirectionally with many other platforms without the need for platform-specific APIs. And they can implement pxGrid once, and then use it again and again to integrate any pxGrid-enabled platform.

pxGrid is fully secured and customizable. Partners can share only what they want to share and consume only the information from other platforms on the grid that is relevant to them. This level of customizability, along with the pxGrid publish-subscribe-query architecture, makes it easy to scale this context sharing, even when communicating with multiple systems. Furthermore, pxGrid enables ecosystem partner platforms to execute network actions with Cisco network infrastructure. Not only can security operations teams gather the relevant threat information faster, but they can also take responsive action immediately.

pxGrid is information model and data format agnostic, as it focuses on transport of security context data. As a result, it is flexible and can work with a variety of data types as needed to suit a wide range of use cases. Ultimately, these context-sharing and network-control capabilities make it possible for IT infrastructure providers to address more use cases, undertake their functions more effectively, and extend their reach deeper into the network infrastructure.

Capabilities and Benefits

pxGrid provides:

- **A single framework for multiple systems to share context:** With pxGrid, any partner platform can connect with other platforms in the IT environment (including both Cisco and third-party platforms that use pxGrid). to share relevant context. This can include real-time operation status, historical event information, operational telemetry, usage statistics, or any other information that an IT platform may need to share or consume.
- **Total control over what context is shared and with which platforms:** Because pxGrid is fully customizable, partners can “publish” only the specific contextual information they want to share and can control which partner platforms that information gets shared with.
- **Bidirectional, many-to-many context sharing:** pxGrid enables platforms to both share and consume context with other connected platforms, with all communication orchestrated and secured centrally by the grid and delivered to each platform in its native data format.
- **Scalable simultaneous connectivity with multiple platforms:** pxGrid enabled platforms to publish only the context data relevant to partner platforms. Numerous “topics” can be customized for a variety of partner platforms, yet always shared through the same reusable pxGrid framework. Furthermore, by sharing only relevant data, platforms that are both publishing and subscribing can easily scale their sharing by eliminating irrelevant data.
- **Integration with Cisco platforms:** pxGrid provides a unified method of publishing and subscribing to relevant context with a growing number of Cisco platforms that use pxGrid for third-party integrations.
- **Automated network threat response:** With pxGrid’s network instrumentation, pxGrid-enabled platforms can take network threat-response actions by simply making a call to pxGrid - even if the platform making the call itself has no network topology or control awareness.

A Superior Mechanism for Cross-Platform Communication

pxGrid provides a much better way to share information than conventional APIs, for several reasons. First, its ability to implement “many to many” communication among diverse network platforms means that it’s innately scalable, much more so than architectures based on polling.

Second, it allows for far more detailed customization. It doesn’t make sense for each tool to pull all the information generated by every other system. that won’t scale either. But unlike APIs, which don’t allow for much customization in what and how the systems communicate, pxGrid lets each connected system pull only the specific information it needs from other systems and share only the specific information that’s relevant to the other systems they’re communicating with.

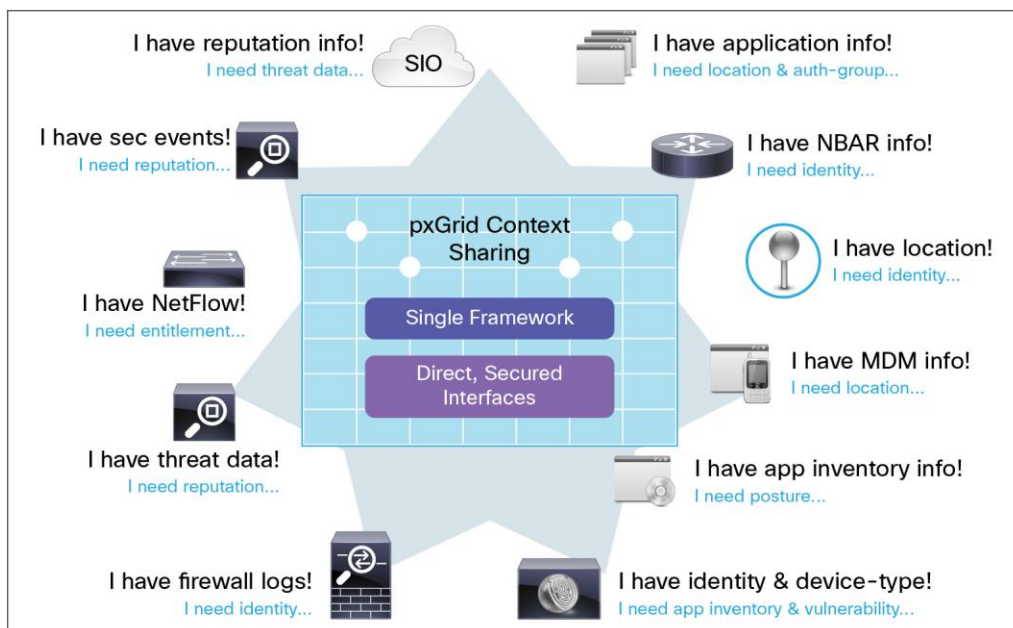
Finally, pxGrid provides stronger security and control. It preserves the integrity of each system’s data far more effectively than APIs by providing tightly controlled access, authentication, and authorization for each system on the grid. Just as users can be authorized on the network to access some resources but not others, IT vendors can authorize systems connected to the pxGrid to access the information they need from their platform, but nothing else.

How pxGrid Works

The basic architecture of pxGrid comprises a central pxGrid controller with multiple systems (nodes) connected to it through a client library. The controller acts as a kind of switchboard operator for the grid, communicating with each node's agent to allow each connected system to share and consume authorized context information with other nodes.

Figure 1 shows a high-level example of pxGrid in action. Here, you can see the diversity of platforms involved in security operations for a typical business. Each has an important role to play, but each needs information from other systems to do its job effectively.

Figure 1. pxGrid Context Sharing



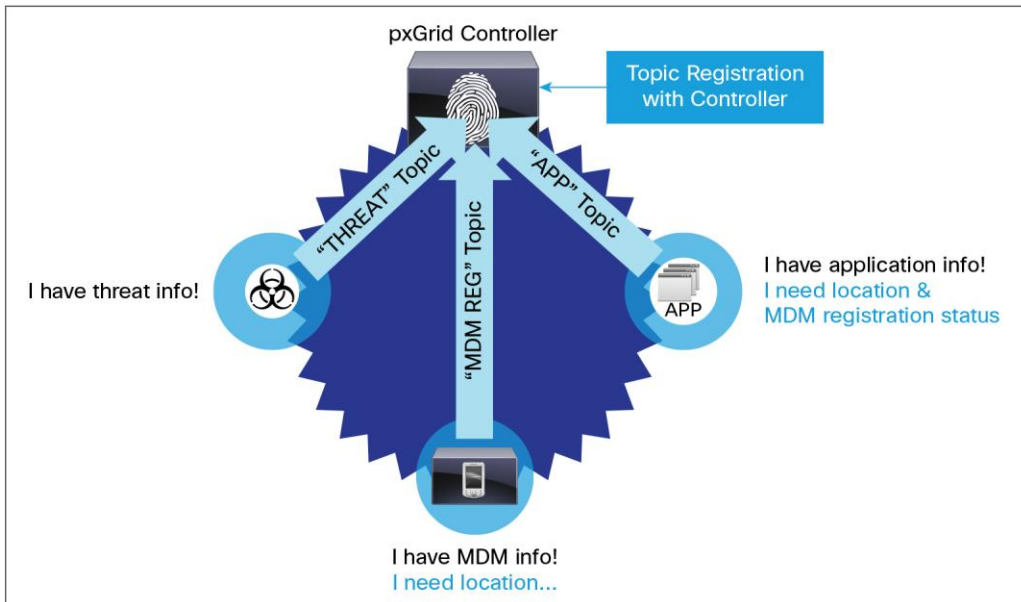
As a simple example, imagine a bring-your-own-device (BYOD) use case, where a business wants to implement different levels of access privileges based on the devices its employees are using and the locations of the users. Doing this requires information from three components: an identity and access management (IAM) platform to provide application permissions, a mobile device management (MDM) platform to check the registration status of the device, and a SIEM platform to assess and inform about the threat risk associated with the employee.

Here's how pxGrid implements interplatform communication to simplify this process:

First, each platform independently authenticates with pxGrid. pxGrid also handles the authorizations, controlling which platforms can publish, which can subscribe, and which can query, as well as which specific context information may be shared with other platforms on the grid. This is done through a "pub/sub" model. Each connected platform publishes specific "topics" to the grid, and/or subscribes to topics that are relevant to the use cases it handles. Each topic is registered in the pxGrid topic directory so that it can be cataloged and found by platforms interested in that topic. Platforms may subscribe to all real-time updates to a topic, query for specific attributes on demand, or do bulk downloads of information from that topic.

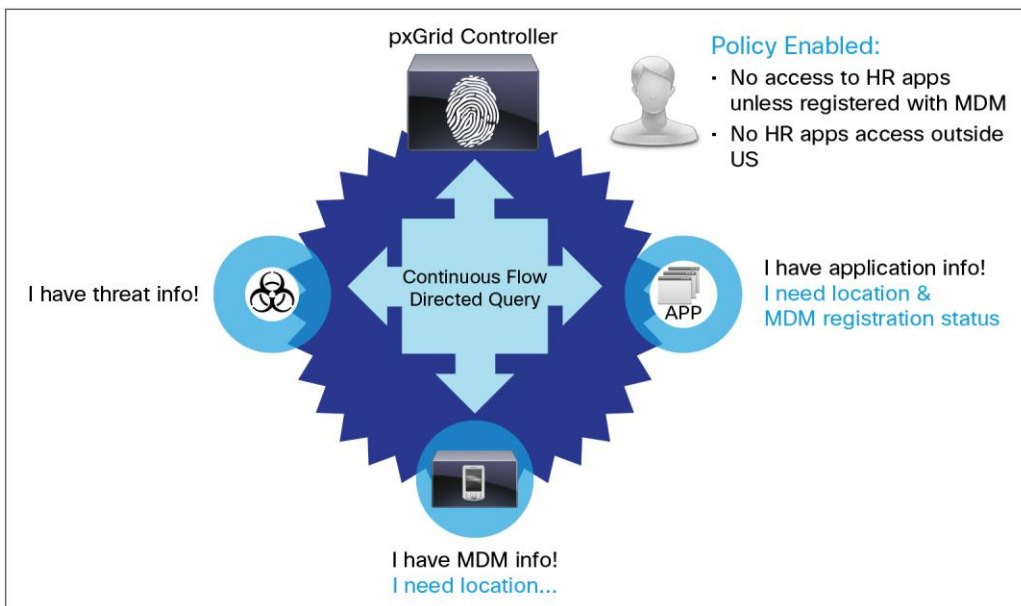
So in the BYOD case, the IAM platform publishes an Applications topic, providing application permissions for users. The MDM platform publishes an MDM Registration topic, providing information about the registration status of a given device. The SIEM publishes an Employee Threat Risk topic, providing the threat risk associated with a given user. (See Figure 2.)

Figure 2. pxGrid Context Sharing for BYOD and Threat Defense



At the same time, each platform on the grid subscribes to topics relevant to its specific operations. The IAM platform can subscribe to the MDM Registration and Employee Threat Risk topics. The MDM platform can subscribe to the Application topic. The SIEM publishes Employee Threat Risk information for consumption by both MDM and IAM platforms. Once this framework is established, each platform can continually pull or ad-hoc query the information it needs from other platforms on the grid, in the appropriate data format, to fulfill its role in allowing or denying access to BYOD users (Figure 3).

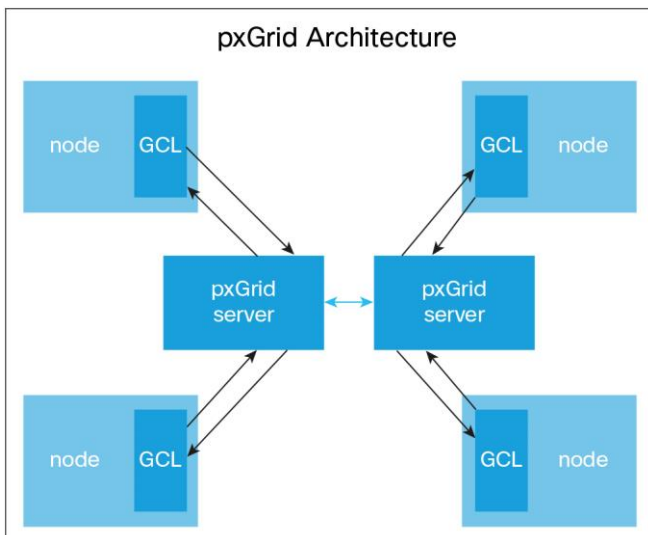
Figure 3. Using pxGrid to Simplify BYOD Security



The pxGrid Architecture

At the heart of pxGrid is a controller and participating nodes, as shown in Figure 4. In a typical customer deployment, nodes reside on separate hosts but within same network. However, they may also be federated across multiple customer environments. As discussed, each node goes through authentication, registration, and authorization to communicate over pxGrid and can establish itself as a provider or consumer of topics for sharing information. The pxGrid server provides message routing and control based on the context data being shared and a participating node’s authorization. It supports queries, notifications, and bulk downloads of context data. Depending on the context, pxGrid can establish an out-of-band channel for a bulk download.

Figure 4. High-Level pxGrid Architecture

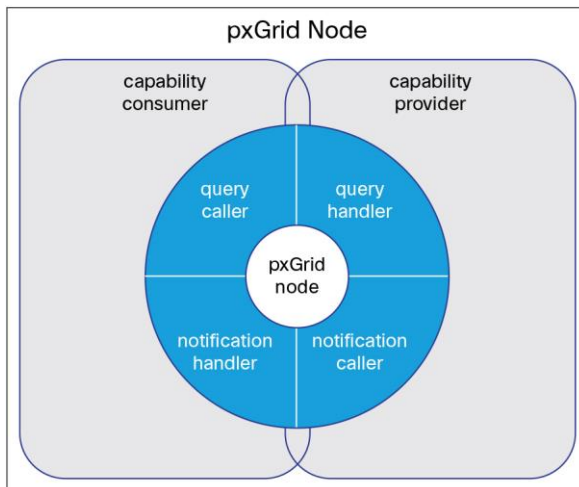


Nodes don't communicate directly with pxGrid. Instead, nodes make programmatic calls to the Grid Client Library (GCL), which in turn connects and communicates with pxGrid. Depending on the use case, one deployment may have only a few nodes, while others may have thousands. pxGrid is designed to scale upward.

Bidirectional Communications

pxGrid enables bidirectional communication between pxGrid nodes. Nodes can be both providers and consumers of capabilities, assuming they are authorized by the pxGrid controller for both functions (Figure 5). As the provider of a capability, a node handles queries, generates notifications, or both. As the consumer of a capability, a node initiates queries, receives notifications, or both. (Note: "Capability" here refers to information channels or topics for sharing contextual information. pxGrid uses information models to define the context data, interfaces, or operations for capabilities associated with that model. For instance, an Identity model could include a Session Directory capability consisting of interfaces for consuming information related to session logins in the network.)

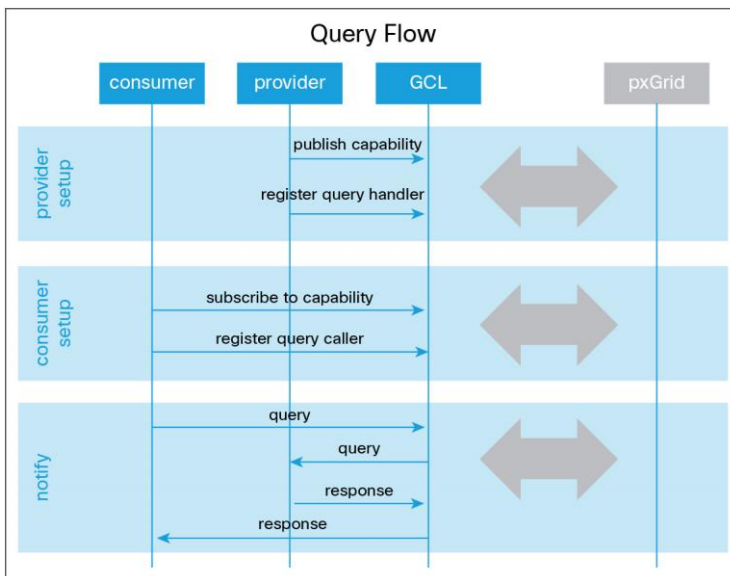
Figure 5. Bidirectional Communications in a Node



Queries

A query is a synchronous call initiated by a consumer and serviced by a provider (Figure 6). Using the GCL, the consumer utilizes a query caller to initiate the communication. The provider implements a query handler to programmatically process requests and generate responses. pxGrid passes the request through the consumer GCL and into the provider GCL, likely on another node in the network. Using custom code implemented by the developer in a query handler, the provider generates a response that pxGrid then sends back to the consumer. The consumer waits until the response is received.

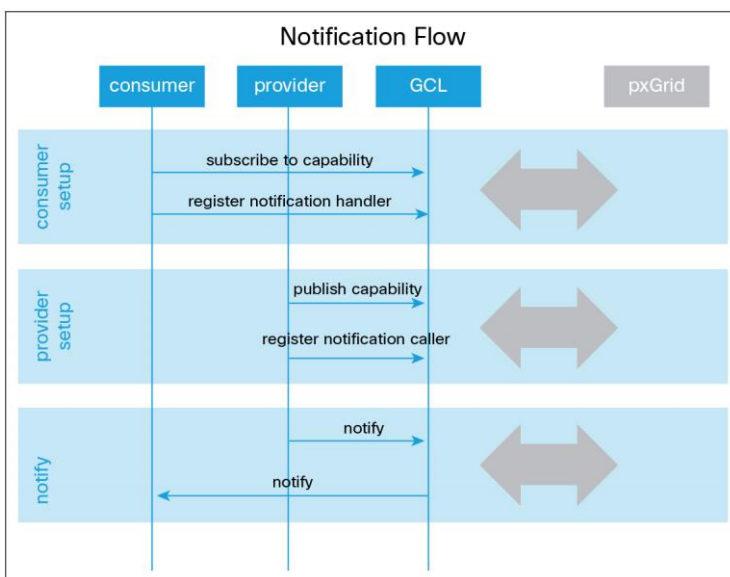
Figure 6. Query Flow



Notifications

A notification is an asynchronous message generated by a provider and received by a consumer. The consumer must first register interest in an information topic. Using messaging terminology, consumers subscribe to a topic and providers publish to the topic. The GCL handles communication with pxGrid, so the consumers and providers can focus on writing code to consume and provide the information. Consumers do not wait for information as they do in a query flow. The GCL uses a separate thread to invoke a notification handler supplied by the consumer. Figure 7 details the flow.

Figure 7. Notification Flow

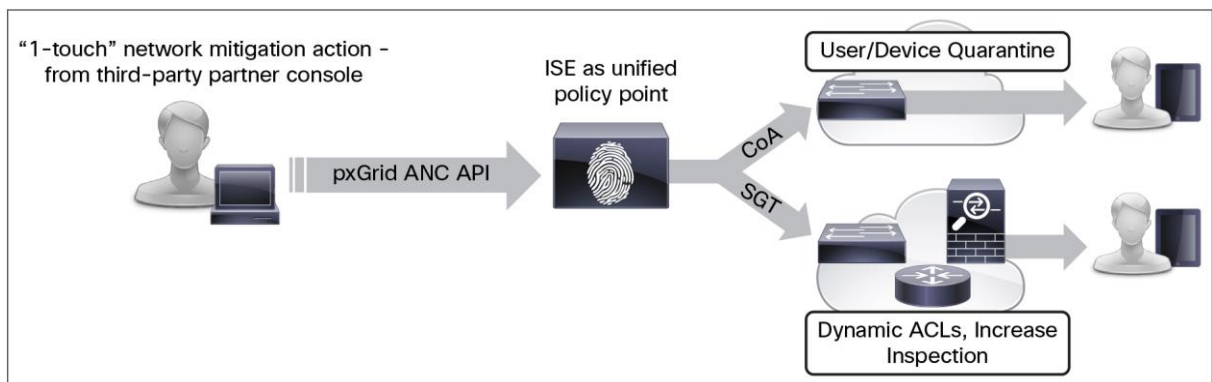


Automated Network Threat Response

pxGrid also provides pxGrid-enabled platforms with the capability to take network threat-response actions on users or endpoints directly from the partner platform. For example, in a SIEM platform an operator may quarantine users or devices or take investigative actions by rerouting traffic. With pxGrid, all this can be done from the SIEM console, using the same pxGrid framework used for sharing or consuming context. In this scenario, the system calls a threat-response API within the pxGrid framework. It can then use threat-response capabilities that are already instrumented in platforms like the Cisco Identity Services Engine to carry out the response action. With this architecture, pxGrid-enabled platforms don't need to understand how to take a response action. They just make a call through pxGrid to a platform, like the Identity Services Engine, that understands the network and has the instrumentation to carry out the requested action.

Figure 8 outlines the Adaptive Network Control (ANC) capabilities on the Identity Services Engine as invoked by a pxGrid-enabled platform making a call to the threat-response API. The engine carries out a change of authorization and issues a security group tag.

Figure 8. pxGrid Threat Response



How XMPP Is Used in the Grid

pxGrid uses the Extensible Messaging and Presence Protocol (XMPP) as the foundation protocol for exchanging security data between systems across the grid. Based on XML, XMPP uses a decentralized client-server architecture, where clients safely connect to servers, and the messages between the clients are routed through the XMPP servers deployed within the cluster. XMPP has been used extensively for publish-subscribe systems in a wide range of file transfer, video, Internet of Things, and other collaboration and social networking applications.

XMPP offers several important advantages for exchanging security data in pxGrid. It provides:

- **An open and standards-based communication framework**, with a decentralized and federated architecture that has no single point of failure
- **Strong security** with support for highly secure domain segregation and federation using Simple Authentication and Security Layer (SASL) and Transport Layer Security (TLS) mechanisms
- **Real-time information exchange and event management** using pub-sub notifications
- **Flexibility and extensibility** as an XML-based framework that can easily adapt to new use cases and support custom functionality
- **Support for multiple information-exchange mechanisms** between participating clients

- **Support for both on-demand and directed queries between clients**, communicated through the XMPP server
- **Support for out-of-band file transfers and direct communication** between participating clients
- **Bidirectional communication**, eliminating the need for firewall tunneling or opening up a new connection in each direction between client and server
- **Scalability**, with support for cluster mode deployments with fan-out and message routing, and peer-to-peer communications
- **Easy deployment** through a straightforward XMPP framework for nodes to detect the presence, availability, and service capabilities of other participating nodes in the system

To simplify the integration with diverse partner platforms, pxGrid defines an infrastructure protocol that hides the nuances of the XMPP data plane protocol and makes information-sharing models extensible with simple and intuitive APIs. pxGrid nodes connect to the grid using this pxGrid protocol, which uses the XMPP transport protocol and introduces an application-layer protocol that uses XML and XMPP extensions. Partners providing platforms for the grid can extend the pxGrid protocol infrastructure model and define capability-specific models and schemas. And they can take advantage of a clean separation between infrastructure and the capabilities that can run on that infrastructure.

Enabling Secure Information Exchange

pxGrid enables secure information exchange between nodes on the grid in three ways. First, it goes beyond the basic username and password to provide strong public key infrastructure (PKI)- and certificate-based authentication for every platform sharing or consuming information on the grid.

Second, pxGrid provides a detailed authorization framework to control what each connected platform can and can't do on the grid. For example, operators can specify which individual topics a platform can share or consume, authorize some nodes to subscribe to topics but not publish (or vice versa), or specify that certain platforms can do bulk downloads but others can't.

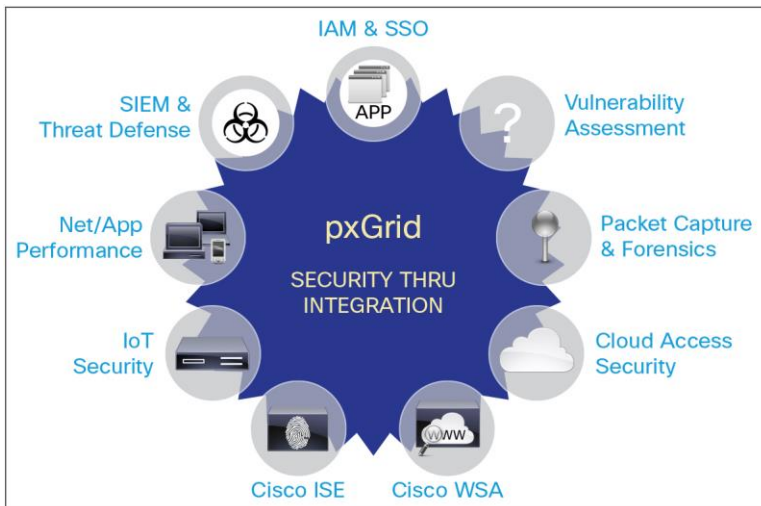
Finally, all data shared over pxGrid is encrypted. Communications are always private and protected from being intercepted by a "man in the middle" attack. Together, these tools allow for much stronger security and control in cross-platform communications than APIs do.

The pxGrid Ecosystem in Action

pxGrid can provide a powerful framework to allow cross-platform communication in IT environments with more security and scalability than anything that businesses have used in the past. But the grid is only as valuable as the platforms that take advantage of it. How much can you actually do with pxGrid today? In fact, quite a lot.

A large and growing number of IT and security vendors are already building pxGrid integration into their solutions. Current ecosystem partners include providers of industry-leading solutions for SIEM and threat defense, network and application performance acceleration, cloud and IoT security, and many others (Figure 9).

Figure 9. pxGrid Ecosystem Partners



Right now, ecosystem partners are using pxGrid to:

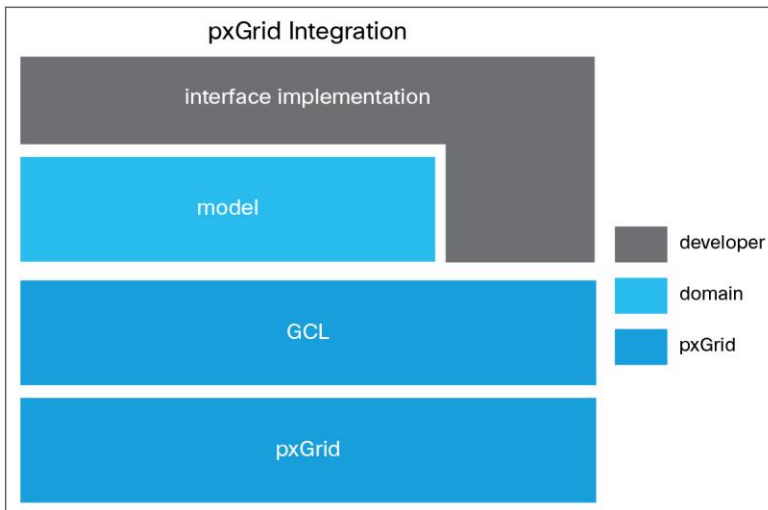
- Accelerate threat response by integrating their SIEM and threat-defense solutions with the Identity Services Engine
- Provide more in-depth network vulnerability assessments by drawing on user identity and authorization, access method, security posture, and other contextual information
- Simplify complex IAM processes to enable single sign-on for multiple cloud applications
- Attribute users and network privilege to cloud security monitoring events and analytics
- And much more

How to Integrate with pxGrid

Cisco makes it easy for partners to integrate their solutions with pxGrid and capitalize on bidirectional communication with other security platforms to bring new capabilities and business benefits to their customers. We provide a complete technical overview and tutorial on [Cisco DevNet](#), along with a full software development kit (SDK) with all of the necessary Java and C client libraries for developers to integrate their nodes with the pxGrid server. The SDK includes a full testing environment, as well as all the necessary instrumentation to quickly integrate with the grid and begin publishing and subscribing to topics and taking network actions.

Figure 10 shows the high-level relationship between pxGrid, the GCL, the model for a particular domain, and custom code written by the developer. The model, as discussed earlier, consists of entities and interfaces common to the domain (security, for example). “Interface implementation” refers to the actual functionality for how a node will behave. The developer extends this model’s interfaces and uses existing classes in the GCL to implement this functionality.

Figure 10. pxGrid Integration



To download the SDK, visit <http://cisco.com/go/pxgrid>. The SDK includes:

- pxGrid technical overview, tutorial, configuration and testing guide, and other relevant documents
- The GCL in Java and C that will be integrated with the platform connecting to pxGrid
- Identity Services Engine virtual machine and setup documentation that can be used as a pxGrid controller for testing pxGrid client implementations
- Information on how to access the cloud-hosted pxGrid test bed to test your integration if you prefer to not install a local testing instance
- Sample pxGrid session output to test a system's capability to consume pxGrid data
- RADIUS session emulator to generate live user and device session data to test pxGrid-integrated systems

Conclusion

As network threats grow more sophisticated and harder to detect, speed will become an increasingly critical element in effective threat response. Having to swivel between the diverse network security solutions in an environment, or trying to patch together multiple platform-specific APIs, will no longer suffice.

Cisco pxGrid provides the framework to accelerate and automate complex security processes in the modern enterprise. Any security platform can share information with any other system in the environment in real time, in a highly scalable and tightly controlled manner, without relying on platform-specific APIs. For security vendors, pxGrid provides an easy-to-implement framework to extend and enhance the capabilities of their solutions and deliver more value to their customers.

For More Information

To learn more about Cisco pxGrid - and even download the SDK and start using it today - visit <http://www.cisco.com/go/pxgrid>.




Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)