Policy Assurance Monitoring for IoE

Cisco IT Insights

What

As Cisco prepares for the proliferation of devices within the concept of the Internet of Everything (IoE), Cisco IT is focusing on implementing backbone technology and policies to harvest the vast amounts of data being produced by systems, devices, logs, and users. While many initiatives are in flight, the Policy Assurance Monitoring project, a one-year pilot, aims to improve visibility into the implementation of policies and identify where policy monitoring is required to optimize the development hosting environment and realize business value.

“We are implementing governance policies to proactively monitor authorized user behaviors and detect events that indicate policies might have been circumvented,” says Casey Hardy, systems administrator and lead architect for policy assurance monitoring at Cisco. “Our pilot is very specific to the environment we are working in, but the concepts here are challenges that are faced across the business.”

Filling a Security Gap with Policy Assurance Monitoring

Security access monitoring is a means to address policy assurance for the IoE program, whether the policy involves user behavior, asset management, or configuration standard across interconnected systems. With the connecting of multiple systems, extracting useful data is vital to driving business change, and to do that, the organization must ensure that the policies put in place are consistently being governed. Many programs tend to assume that built-in policies are sufficient; however, individual policies may not necessarily communicate critical state information to other policy assurance initiatives within interconnected IoE programs.

We contextualize whether security compliance is an issue by extracting data from operational events (event correlation, behavioral models, and policy compliance). High-level visibility into policy is necessary with engineering, hardware, developer business processes, infrastructure and networking, and information security environments. By enabling policy assurance capabilities for IT IoE operations, we can promote security optimization and continuous improvement in the environments where policies are applied.

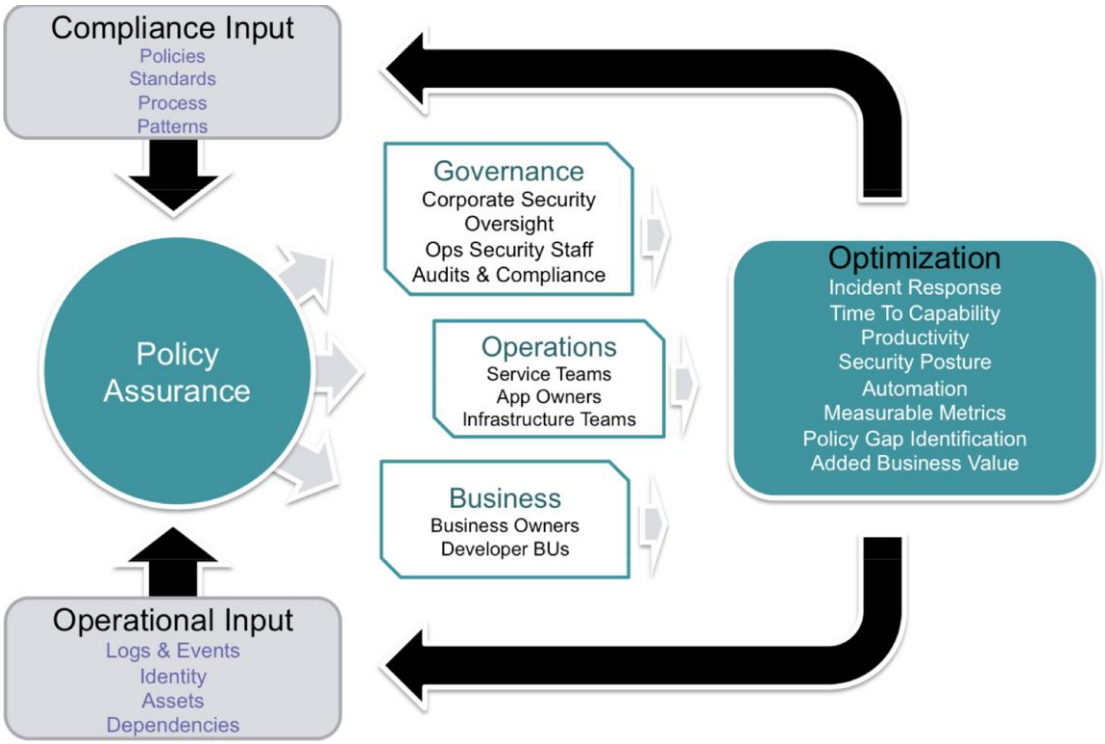
Collaborating with IT

There is a palpable need for this initiative in IT. Establishing new or improving existing policies has the potential to impact several business processes. In a non-IoE environment infrastructure, logs are frequently fragmented, scattered, and lack traceability. Across the board, IoE requires a high level of governance over the implementation of policies. Better logging, alerting, data mining, and response capabilities will allow us to harvest and organize data in more structured and meaningful ways. We are working toward a more holistic approach that will eventually collect data and connect that data to the actual systems on the ground. Currently, these processes are siloed and dependent on the technology where those policies are embedded. We are working to scale the initiative by coordinating within IT.

“Our team also has plans to work in coordination with other groups that collect and make use of policy data, including providing insights to the event correlation team,” says Hardy.

Policy assurance monitoring is integrated as part of a larger organizational architecture, including both workflow and physical components. Policy assurance sits at the center of these larger architectures from a data collection perspective (see Figure 1). To drive policy change and improvement, data from within the data center hosting space (applications, logs and event hosting, infrastructure data and performance information, and storage) needs to be centralized.

Figure 1. Overview of Policy Assurance Monitoring



Why

Most businesses face challenges around defining what information is important and connecting it to other activities that are related to business processes, compliance, and productivity.

“It’s really more of a visibility problem that we’re trying to solve than a technology problem, because the data collection and interpretation has to be flexible enough for all the technologies,” says Hardy. “Everything has a policy around it, but do you know how relevant that policy is to your business goals, and are you compliant with the policies that interact with it? At the core, that’s the problem that we are trying to solve.” Fractured policy compliance data leaves gaps in IT security, IT operations, and Cisco® intellectual property protection.

The main four gaps that we’re trying to close up fall within the visibility spectrum, including:

- Improving forensics confidence and investigation through centralizing a secure-logging framework
- Enabling predictive analytics through the large-scale collection of virtual and physical hardware instrumentation
- Revealing unknown dependencies among the application portfolio through data mining application interactions
- Establishing baselines to enable more accurate value statements for future investments

We envision benefits specific to the technologies in the pilot project, including the following:

- Log integrity: Highly sensitive logs are collected to a secure, access-controlled central location and do not persist in a local, corruptible store.
- On-demand data mining: Logs can be mined in near real time to associate real user activities with activities taken while acting as generic accounts or other users.
- Automated alerts and remediation: Enables future ability to trigger administrative alerts or automatic action when inappropriate activities appear in logs.

- Root cause analysis and investigation: Improves accuracy of root cause analysis for security incidents and enables better collaboration with corporate security investigators.

Overall, the policy assurance monitoring initiative aims to reduce the root configurations that cause policy violations. “If our policy implementation is not appropriate to the environment, there will be a lot of exceptions occurring that we can’t see or manage. We need this data to make our policy implementation better conform to the actual needs in the environment,” says Hardy.

The initiative has the potential to reduce incidents and interruptions to workflow, and reduce overall time spent to correct and fix configurations that have resulted from the inconsistent implementation of policies.

For More Information

To read additional Cisco IT case studies about a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT.

To view Cisco IT webinars and events about related topics, visit Cisco on Cisco Webinars & Events.

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described. Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties; therefore, this disclaimer may not apply to you.

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.