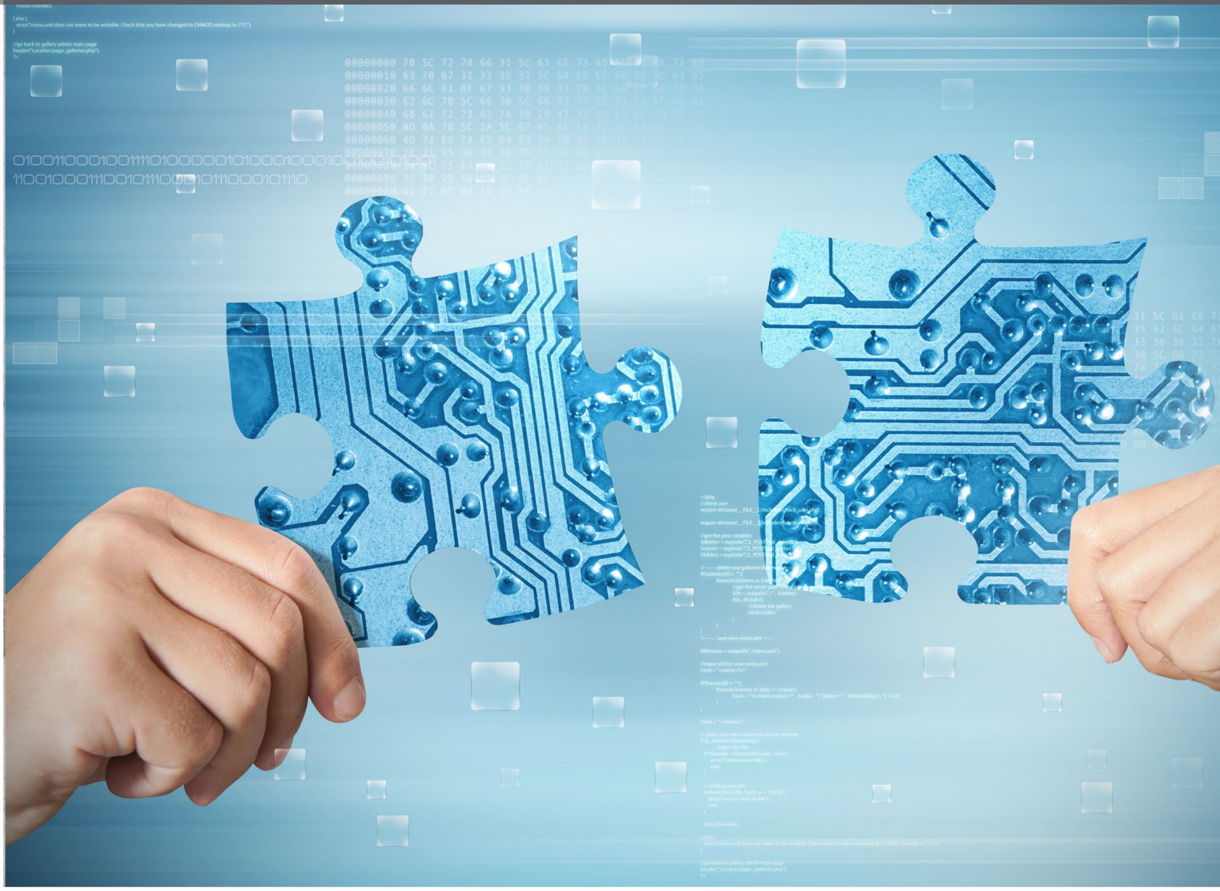
SAINT®

Integration with Cisco ISE



SAINT Integration with Cisco Identity Service Engine

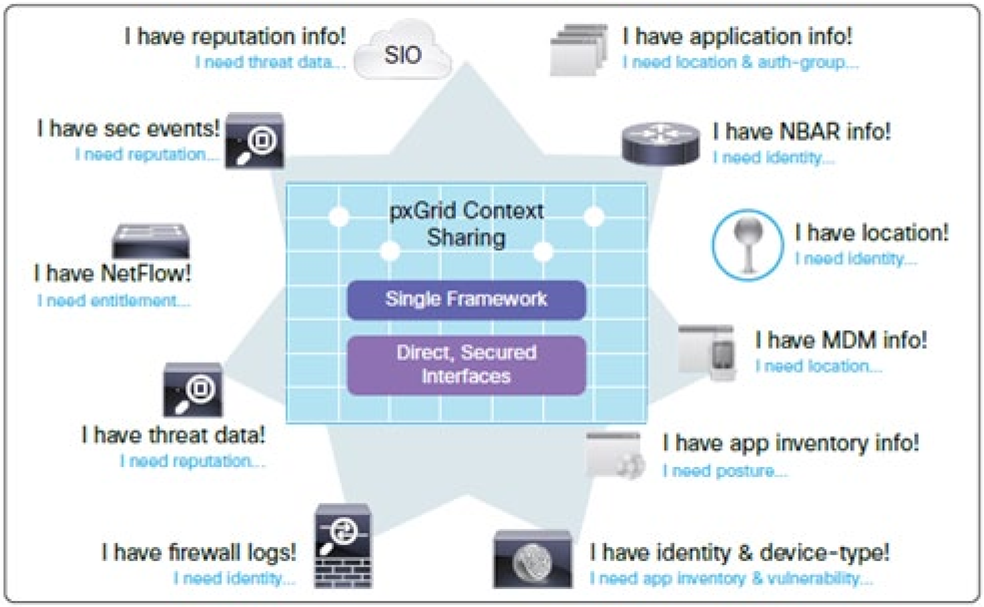
An effective solution must work across the entire technology eco-system.

The complexity of today's modern IT infrastructures demands extremely robust and secure technology solutions to facilitate business operations while ensuring the confidentiality, integrity and availability of content. Technology must be able to communicate across disparate platforms while maintaining operational control and integrity of various components such as security monitoring, assessment, detection and mitigation resources, policy platforms, asset configuration management systems and access management platforms. The key to executing such a complex and effective solution is choosing solution providers that understand the scope of the problem, and deliver solutions that work across the entire technology ecosystem rather than creating one-off solution silos to be maintained outside of the broader framework.

Cisco Platform Exchange Grid (pxGrid) and Identity Services Engine (ISE)

Cisco® Platform Exchange Grid (pxGrid) enables multi-vendor, cross-platform network system collaboration among parts of the IT infrastructure such as security monitoring and detection systems, network policy platforms, asset and configuration management, identity and access management platforms, and virtually any other IT operations platform. When business or operational needs arise, ecosystem partners can use Cisco pxGrid to share contextual information with Cisco platforms that use Cisco pxGrid as well as any ecosystem partner system that uses Cisco pxGrid.

Cisco Platform Exchange (pxGrid) Framework



The Cisco pxGrid controller orchestrates connections between platforms and authorizes what contextual information gets shared between those platforms. This control function is provided by Cisco Identity Services Engine (ISE). The Cisco pxGrid platform thus provides a conduit for ecosystem partner platforms to execute network actions within the Cisco network infrastructure on users and devices via Cisco ISE. For more information on Cisco pxGrid and the Identity Services Engine (ISE), go to http://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/at_a_glance_c45-728420.pdf

SAINT Security Suite provides the capability to communicate to ISE that an asset has been found to be of high risk to threat exposure.

SAINT Security Suite

As a security solution, SAINT Security Suite provides authenticated and unauthenticated scanning and assessments of a wide range of network-based hosts, to gain insight into security risks that impact the confidentiality, integrity, authenticity and availability of critical information and IT infrastructure. SAINT Security Suite identifies risks across the ecosystem from host vulnerabilities and configuration weaknesses, exposure of sensitive content, risks to web applications and servers, as well as risks propagated as a result of the actions of the users that expose sensitive content or critical assets. SAINT extends the value of its solutions by providing integration and interoperability with other security investments through SAINT's API and solution partner alliances. This ensures security practitioners and asset managers can quickly, easily and effectively identify and remediate risks before they are exposed to internal or external threats. For more information about SAINT Security Suite, go to http://www.saintcorporation.com/products/SAINT8.html.

The Partner Solution

As a Cisco Solution Partner, SAINT is a member of the Cisco Security Technical Alliance program—an ecosystem of complementary technologies to help customers gain better security, faster resolution of critical events, and increase return on investment (ROI). Partners in this program have developed a proven integration capability with the Cisco Security product portfolio's open and proprietary APIs and other integration points. SAINT Security Suite is part of this ecosystem—providing interoperability with CISCO's Identity Services Engine (ISE) within the Cisco Platform Exchange Grid (pxGrid), as well as Cisco's FireSIGHT Management Center.

Cisco ISE leverages Cisco pxGrid technology to integrate with Cisco FireSIGHT so it can collect identity contextual information from ISE for identity-based event

Staff can quickly and effectively work to reduce risk to the organization.

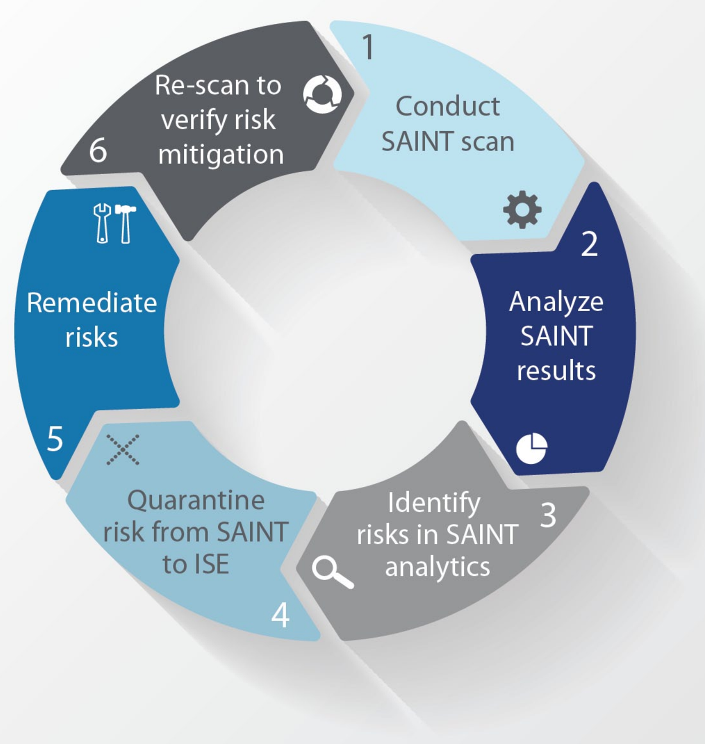
logging as well as specifying quarantine actions for remediation. Simply put, when a Cisco Advanced Malware Protection (AMP) for Endpoints malware detection appears in Cisco FireSIGHT, it dynamically instructs ISE to quarantine the infected endpoint.

What can a security expert do to reduce the possible risk of exposure determined through your vulnerability management program? Using SAINT's ISE integration, you can make that determination as part of your vulnerability analysis inside of SAINT Security Suite, and trigger ISE to quarantine the risky asset until actions can be taken to remediate the vulnerabilities and validate the remediation through a re-scan.

How it Works

The Cisco pxGrid ISE Management Center provides command and control over the platform exchange framework. Cisco works with relevant industry organizations to drive context-sharing standards applicable to Cisco pxGrid and facilitate platform-to-platform communications to enable more efficient and effective network and IT operations. This exchange framework and content sharing is made available to ecosystem partners to support integration between ISE and the capabilities of partner solutions.

Using our SAINT Security Suite investment, you can communicate directly within this exchange framework, and facilitate real-time risk mitigation and reduce your threat attack surface.


1
Conduct SAINT scan
2
Analyze SAINT results
3
Identify risks in SAINT analytics
4
Quarantine risk from SAINT to ISE
5
Remediate risks
6
Re-scan to verify risk mitigation

This diagram illustrates how SAINT Security Suite can be used to communicate to ISE that an asset has been found to be of high risk to threat exposure from an analysis of the scan results. The risky asset should be quarantined from all inbound or outbound communication across the environment until the risks have been investigated and remediated.

These risks can be a result of known platform or application vulnerabilities, exposure of sensitive content, unauthorized services running on a host, a configuration identified as out of specification with local configuration management (CM) policies, or even identification of a default or easy-to-guess password to a critical resource.

The key benefit in this example is that staff given the responsibility of managing the security program within the ecosystem can quickly and effectively work with asset managers to reduce the threat potential as a result of an identified risk, and work collaboratively to reduce risk while maintaining operational control over the environment.

See more information about the integration between SAINT Security Suite and Cisco's ISE at https://marketplace.cisco.com/catalog/companies/saint-corporation/products/saint-security-suite-cisco-ise-module.

To learn more about the SAINT Security Suite, contact us at:
(800) 596-2006 or
sales@saintcorporation.com

About SAINT Corporation

Since its inception in 1998, SAINT has been developing innovative software solutions. SAINT's customers include high-level government agencies, top colleges and universities, and major financial institutions. Industries and governments all over the world are using SAINT products and services to manage IT security risk and compliance. SAINT Security Suite enables customers to:

- Identify security vulnerabilities on network devices, operating systems, desktop applications, web applications, etc.
- Detect and fix possible network security weaknesses before they're exploited by intruders.
- Anticipate and prevent common system vulnerabilities
- Demonstrate compliance with current government and industry regulations, such as PCI DSS, NERC, and FISMA.

For more information about SAINT as a Cisco partner or other SAINT solutions, please call us at 800-596-2006; e-mail us at sales@saintcorporation.com; or visit *www.saintcorporation.com*.

Copyright © 2015
SAINT Corporation