SOLUTION BRIEF

Digital Defense, Inc. and Cisco® offer Integrated Solution to Evaluate New and Unknown Assets and Restrict Access Based on Risk

Frontline.Cloud™ asset discovery, and vulnerability and threat risk assessment combined with Cisco® Identity Services Engine (ISE) access control to protect network from high-risk assets.

BUSINESS PROBLEM

Cisco ISE is a market leading technology for network access and policy control for onboarding of authorized users and devices, while disallowing unauthorized assets and users onto the network. However, even an authorized asset and user may introduce great risk to the organization.

It is critical to understand how exposed, unpatched, and/or infected an asset is before introducing it into the network and make a policy decision based on that risk. All it takes is a single infected host to enable an attacker to methodically take over an entire network or find where the crown jewels are for exfiltration regardless of whether security policy would normally allow that user and host access.

The fact is allowing any device to connect without a true understanding of overall risk, including if the asset is already compromised, astronomically increases the potential of an organization getting breached. With the growth and dynamic nature of mobile workers, IoT/ICS technologies, and cloud technologies, security professionals struggle with tracking, understanding the risk posture, and prioritizing patching of critical assets. The ability to restrict access based on risk posture through automation can give security admins confidence in protecting the organization while addressing high-risk assets requesting access to network resources.

DIGITAL DEFENSE FRONTLINE.CLOUD™

Digital Defense's Frontline.Cloud platform has been purpose-built to be deployed and operate in today's hybrid cloud enterprise environments. Frontline.Cloud is hosted on Amazon Web Services (AWS) and incorporates Digital Defense's patented and proprietary technology that supports multiple software security modules focused on pro-actively protecting business critical assets. The Frontline.Cloud Software as a Service (SaaS) platform supports Frontline Vulnerability Manager™ (Frontline VM™), Frontline Web Application Scanning™ (Frontline WAS™), and Frontline Active Sweep™ (Frontline ATS™), leveraging multiple patents that eliminate the deficiencies in similar solutions that are also traditionally based on hardware appliances.

Frontline.Cloud is the only solution in the market that can scale to operate on premise, in the cloud or in hybrid network-based implementations to fit the needs of organizations of any size, including even the largest financial, government, healthcare, retail and utility providers in the world.

SCAN
Quickly, comprehensively and accurately assess your network for vulnerabilities.

ANALYZE
Identify which assets are at risk and receive actionable intelligence.

SCORE
Benefit from a clear, easy-to-understand metric to determine your organization`s security posture.

AUTOMATE
Seamlessly integrate Frontline vulnerability finding into my security workflow.

CISCO ISE AND pxGRID

The Cisco Identity Services Engine (ISE) allows for the creation, management and enforcement of network access policies for the various devices connected to an organization's network based on advanced profiling of users and devices. ISE is able to leverage important security context through Cisco's Platform Exchange Grid, (pxGrid), which consumes information from Frontline.Cloud to be incorporated into Cisco ISE, allowing for an improved security context in which to create and modify policies and automate access control based on vulnerability and threat risk.

SOLUTION SUMMARY

Cisco® Identity Services Engine (Cisco ISE)/pxGrid combined with Digital Defense's Frontline.Cloud vulnerability and threat assessment platform, extends traditional network access control and policy management to identify high-risk assets, that are highly vulnerable to exploits, remain unpatched or have already been infected. With that knowledge, Cisco ISE can make intelligent, potentially automated, policy decisions to restrict access and protect the network and resource from a potential compromise or attack.

INCREASE VISIBILITY, IDENTIFY RISK, IMPROVE THREAT DETECTION, AND ACCELERATE REPONSE

Visualize

- Discover devices instantly without requiring agents
- Profile and classify devices, users, applications and operating systems
- Continuously monitor corporate, BYOD and IoT endpoints

Control

- Allow, deny or limit network access through Cisco ISE based on device risk posture and security policies
- Assess, prioritize and remediate malicious or high-risk endpoints
- Improve compliance with industry mandates and regulations

Automate and Orchestrate

- Share endpoint context from Cisco ISE via Cisco pxGrid with Frontline VM
- Create actionable workflows to have Cisco ISE automatically restrict access based on Frontline scans and associated risk assessment
- Create dynamic policy changes in system-wide response to quickly mitigate risks

SOLUTION DESCRIPTION

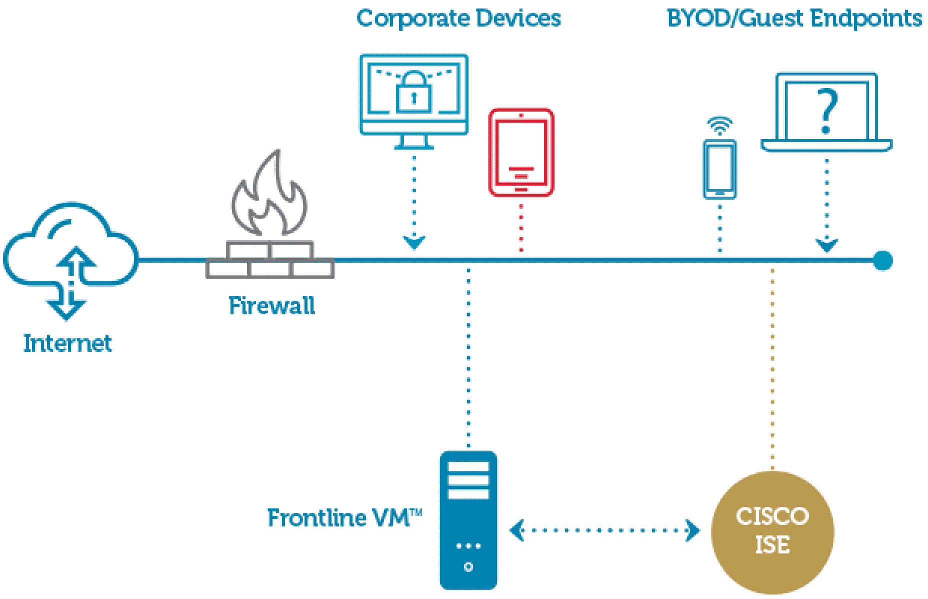
Prioritization and Automation Optimize Workflows

Digital Defense's Frontline.Cloud digitally fingerprints the hosts as contiguous entities, reconciles asset changes from scan to scan utilizing patented correlation algorithms (helping to minimize duplicates or unknown devices), prioritizes vulnerabilities, and automates workflow across the hybrid network to make better risk management decisions, quickly. Frontline.Cloud delivers unparalleled accurate network and host assessments all the way to intelligent integration with Cisco ISE, for automating security workflows and policies.

Restricts Devices that May Introduce Risk

Cisco ISE/pxGrid reduces risks and contains threats by dynamically controlling network access. ISE can assess vulnerabilities from Frontline.Cloud and apply threat intelligence. ISE monitors and denies network access to any device based on known information. United, Cisco ISE will use the vulnerability intel and Frontline Security GPA® scoring intelligence as part of its access decision policies. Providing Cisco ISE with Frontline. Cloud scanning intelligence data allows it to take more granular action by restricting access of a device that may potentially introduce risk into the network.

The integration offers a policy to allow ISE to request an immediate vulnerability scan when a new device, which has not yet been assessed by Frontline.Cloud, comes onto the network.. That same policy can restrict access for the given device, until ISE has received the data from Frontline.Cloud, whereupon it would then fall to other policies to determine what actions to take based on the findings.



INTEGRATION PROCESS & BENEFITS

The integration offers a more holistic approach to network access security:

Visibility

- As an endpoint attempts to connect to the network, ISE is immediately aware of it
- ISE requests the most recent scan results for the endpoint from Frontline VM
- Based on not having seen the device before, ISE can request Frontline VM to scan endpoint for vulnerabilities

Automated Scanning

- ISE can launch a scan from the scan repository based on a condition [i.e. has not seen the pre- existing device in 3 days on the network]

Policy Enforcement

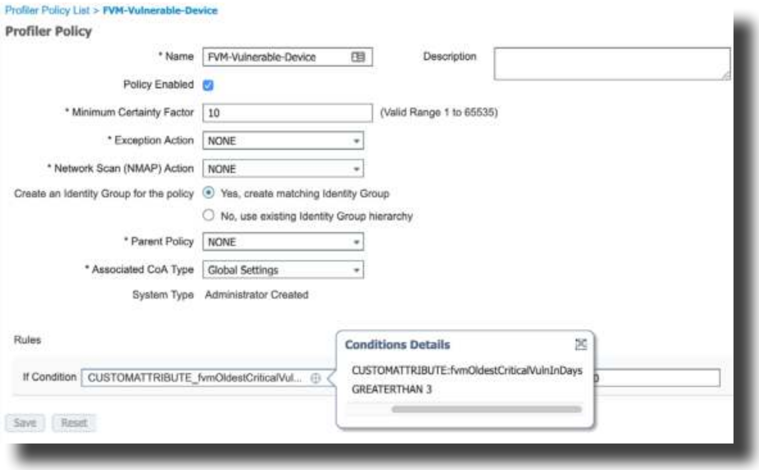
- If critical vulnerabilities exist, ISE will quarantine or block the device so it does not become a launching point for advanced threats
- If vulnerabilities are present on the network for an extended time [e.g. 3 months], an ISE policy may quarantine or block the device

LEARN MORE

To learn more about the advantages of the Digital Defense, Inc. Frontline.Cloud Platform with Cisco ISE/ pxGrid certified integration:

Sales can be reached at: sales@digitaldefense.com

Technical support questions can be directed to: integrations@digitaldefense.com



Profiler Policy List > **FVM-Vulnerable-Device**

Profiler Policy

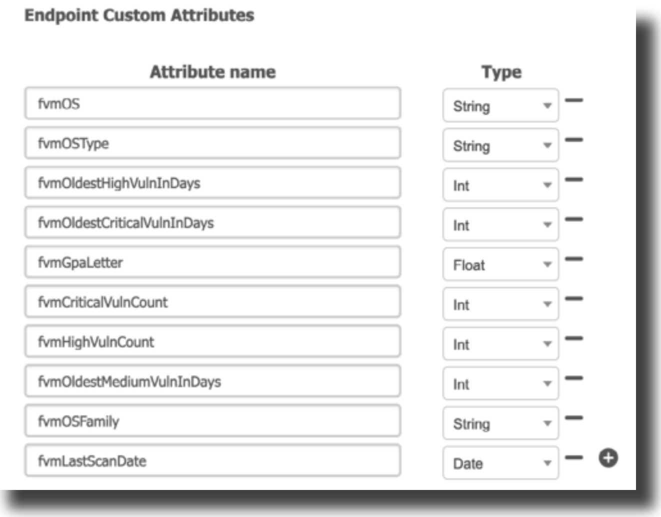
* Name	FVM-Vulnerable-Device	Description
Policy Enabled	☑	
* Minimum Certainty Factor	10	(Valid Range 1 to 65535)
* Exception Action	NONE	
* Network Scan (NMAP) Action	NONE	
Create an Identity Group for the policy	● Yes, create matching Identity Group ○ No, use existing Identity Group hierarchy	
* Parent Policy	NONE	
* Associated CoA Type	Global Settings	
System Type	Administrator Created	

Rules

If Condition CUSTOMATTRIBUTE_fvmOldestCriticalVul...

Conditions Details

CUSTOMATTRIBUTE::fvmOldestCriticalVulnInDays GREATERTHAN 3



Endpoint Custom Attributes

Attribute name	Type
fvmOS	String
fvmOSType	String
fvmOldestHighVulnInDays	Int
fvmOldestCriticalVulnInDays	Int
fvmGpaLetter	Float
fvmCriticalVulnCount	Int
fvmHighVulnCount	Int
fvmOldestMediumVulnInDays	Int
fvmOSFamily	String
fvmLastScanDate	Date

*Integration supported for Cisco ISE 2.4 Plus

About Digital Defense

Founded in 1999, Digital Defense, Inc. is an industry recognized provider of security assessment solutions. Digital Defense provides vulnerability and threat assessment Software-as-a-Service (Saas) solutions and services purpose-built to operate in today's hybrid cloud enterprise environments. Digital Defense's proprietary platform, Frontline.Cloud, incorporates patented technologies and offers multiple software security systems focused on pro-actively hardening business critical assets from being compromised and breached. The Frontline. Cloud platform supports Frontline Vulnerability Manager™ (Frontline VM™), Frontline Web Application Scanning™ (Frontline WAS™), and Frontline Active Threat Sweep™ (Frontline ATS™) that provide agent-less discovery, vulnerability and threat assessment of dynamic assets, while eliminating manual processes and integrating with market-leading 3rd party security and IT offerings to eliminate gaps in visibility and enable faster remediation. Frontline.Cloud is the only solution in the market that is built to be scale across any size organization and operate on premise, in the cloud or in hybrid network-based implementations.

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide leader in IT that helps companies transform the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected. The Cisco Identity Services Engine (ISE) improves operations and network defense capabilities with user and device contextual data, access policies, and enforcement. Cisco ISE is helping companies consolidate their security operations through open integration with partner technologies. ISE shares its wealth of contextual identity information and allows partner technologies to block network access.