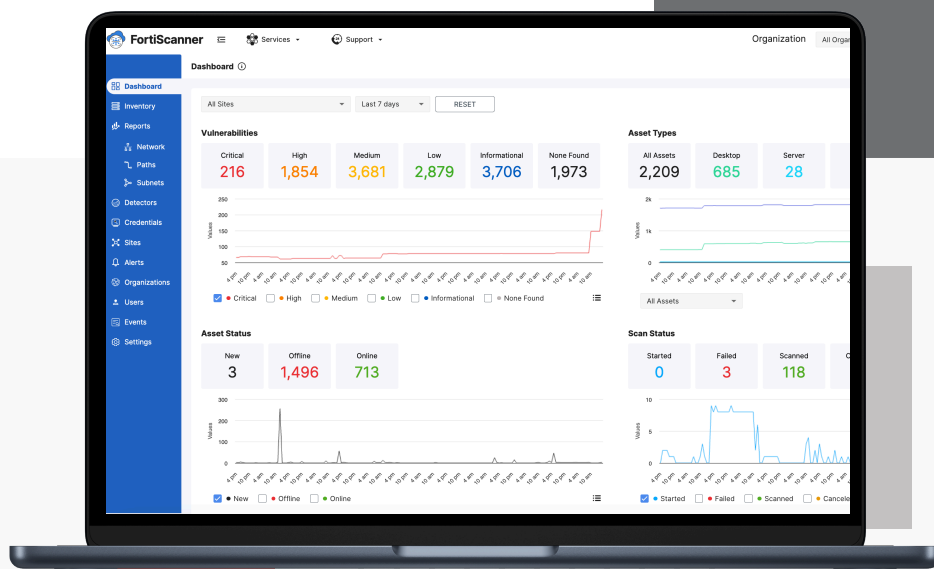


FortiScanner Cloud

Cyber Asset Attack Surface Management Cloud Service



Highlights

- Comprehensive security visibility of corporate networks, with coverage for both managed and unmanaged systems
- Merges asset, network, software, vulnerabilities, and user data from IT and security solutions to give insights into which systems lack essential security measures, and which systems are not included in vulnerability management programs
- Proactively minimizes threats and protects against potential attacks by identifying weaknesses, misconfigurations, and other hazards. In general, FortiScanner could supply organizations with a solid basis for controlling risk and exposure

Minimize threats and protect against potential attacks

FortiScanner is a CAASM—Cyber Asset Attack Surface Management cloud-service platform with a comprehensive security visibility of corporate networks, with coverage for both managed and unmanaged systems. It merges asset, network, software, vulnerabilities, and user data from IT and security solutions to give insights into which systems lack essential security measures and which systems are not included in vulnerability management programs. Organizations can proactively minimize threats and protect against potential attacks by identifying weaknesses, misconfigurations, and other hazards. In general, FortiScanner can supply organizations with a solid basis for controlling risk and exposure.

Use Cases

Available in



Cloud

Governance, Risk, and Compliance

- FortiScanner helps companies adopt the GRC framework
- Identify the risk associated with security vulnerabilities
- Help establish policies and practices to minimize compliance risk

Asset Inventory

- Discover network devices (physical and virtual) connected to the corporate networks
- Detect the applications and services running in the asset devices discovered

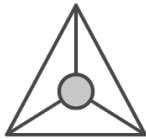
Vulnerability Detection

- Provides the correlation of Assets, Applications, and Vulnerability
- Vulnerability list classification
- Mitigates compliance risk

FortiScanner Cloud Features



Cloud-Managed



Asset
Inventory



Detectors



Network
Scanning



Authentication
Scanning



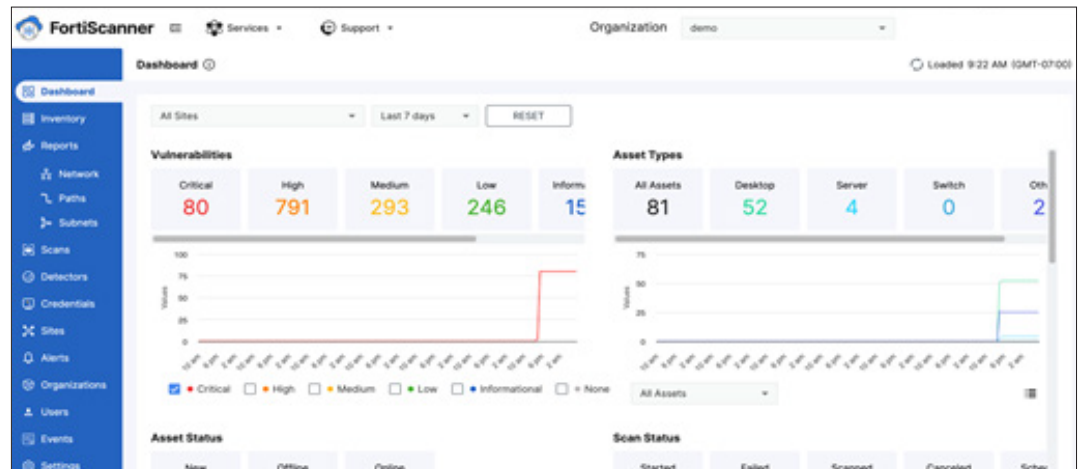
Reports



Multi-Tenancy

Cloud-Managed

- Centralized management in the Cloud and access over the FortiCloud portal
- Discovery assets, vulnerability, and provide the endpoint device inventory tools



FortiScanner Cloud Features

Inventories

Assets, vulnerabilities, software, and services are discovered by the Detectors; one Detector per subnet is mandatory

Organization	Asset Status	Hostname	MAC	IP Address	Site	Type	OS
Research	Online	gy6188	00:50:56:97:b7:57	10.255.253.188	10.255.253.188	Desktop	Windows
Research	Online	gy60-vubuntu	00:0c:29:c5:8e:07	10.255.253.186	186190	Desktop	Ubuntu
Research	Online	www.esxi63.com		10.152.20.163	esxi	Hypervisor	VMware Esxi 7.0.C
Research	Online	gy6188	00:50:56:97:b7:57	10.255.253.188	255.253.188	Desktop	Windows
Research	Online	FortiScan-esxi	08:35:71:19:0a:4b	10.255.253.162	news_30.255.253.0	Hypervisor	VMware Esxi 7.0.C
Research	Online	FortiTester	00:0a:48:91:5e:b7	10.255.253.52	news_30.255.253.0	Desktop	Linux
Research	Online	FortiTester-ESX0	08:35:71:19:0a:4b	10.255.253.163	news_30.255.253.0	Hypervisor	VMware Esxi 7.0.C
Research	Online	FortiTester-ESX0		10.255.253.163	TW-192.168.191.0/24	Hypervisor	VMware Esxi 7.0.C
Research	Online	FortiScan-esxi		10.255.253.162	TW-192.168.191.0/24	Hypervisor	VMware Esxi 7.0.C
Research	Online	FS1048T418000544	00:0c:29:c5:8e:07	10.255.253.186	Lab-255.253.0	Desktop	Ubuntu

Asset Detail

The Asset view shows the following information:

- Asset Details
- Vulnerabilities
- Software
- Services
- Screenshots

Hostname	Asset Status	Site	Type	OS	Service Ports	Notes
AGENT104-PC	Online	1w-192	Server	Windows 7 Professional 7601 Service...	TCP:1, UDP:1, ICMP:1, ARP:1	
MAC, IP	00:0c:29:78:00:99	192.168.191.104				
First Seen	Jun 11 2024 09:40 PM					
Last Seen	Jun 17 2024 01:35 PM					

Detectors

The Detectors can be installed by the user and supports the following OS:

- Windows
- Linux
- MacOS

Download FortiScanner Detector Installer

Latest Available Version: v24.2.0.0016

Note: Each detector is automatically named with its host asset's hostname.

Select the operating system and the CPU type of the asset that will host this detector.

Organization
Default Organization

Host Operating System *
Windows

Host CPU Type *
AMD 64-bit

Minimum Host System Requirements

- Processor running at 2.0GHz or higher
- 1024B of memory
- 1GB of free storage space
- Public network access
- Administrator user access

Detector Installation
Use one of the two methods:

1. Download and run an executable file.
With Administrator access, install the .exe file on the Windows asset that will host the FortiScanner detector.

2. Copy and run command lines.
With Administrator access, run these install commands on the Windows asset that will host the FortiScanner detector.

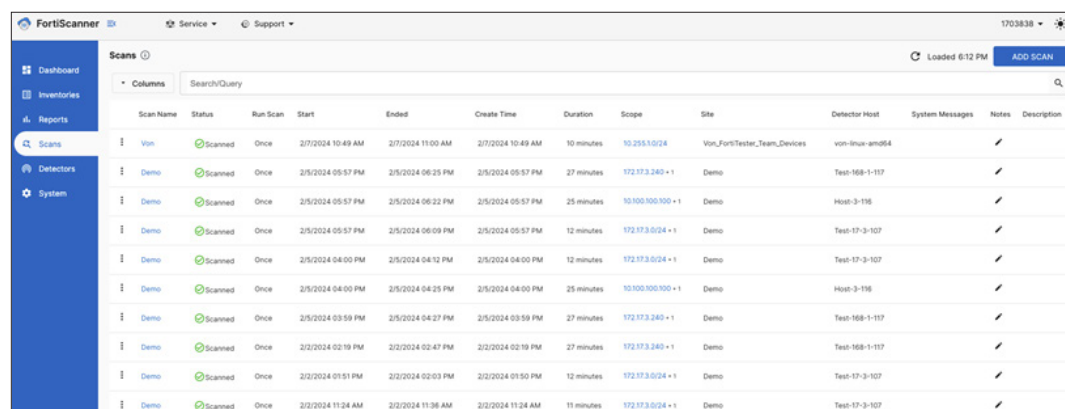
```
curl -o FortiScanner-Detector-Installer-Windows-amd64.exe "https://api-test1.fortiscanner-cloud-ga.com/download/detector/99413827f08b4b5c2a8b639471601785c355e8c832387f94271338533/-1/Installer-Windows-amd64?"; .\FortiScanner-Detector-Installer-Windows-amd64.exe
```

FortiScanner Cloud Features

Scans

Configure scan intervals; every scan setup can be defined by:

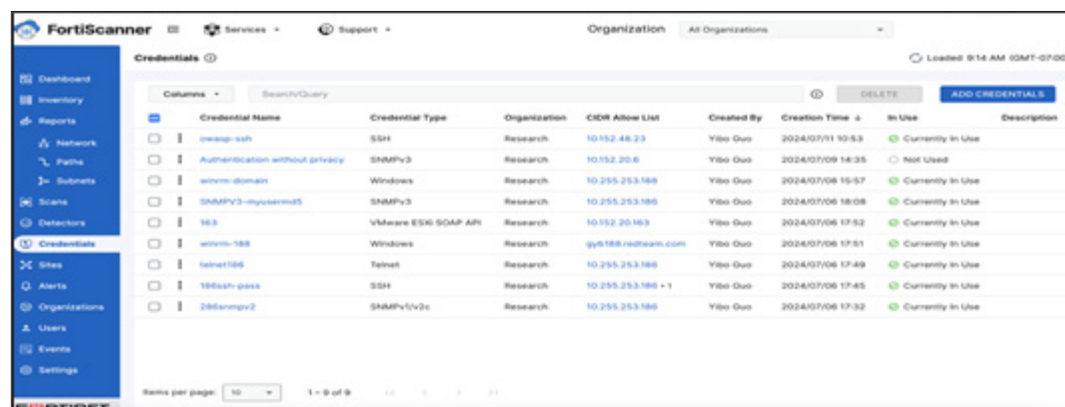
- Site
- Subnet
- Scan Rate
- Hourly, daily, weekly, and monthly



Scan Name	Status	Run Scan	Start	Ended	Create Time	Duration	Scope	Site	Detector Host	System Messages	Notes	Description
Von	Scanned	Once	2/7/2024 10:49 AM	2/7/2024 11:00 AM	2/7/2024 10:49 AM	10 minutes	10.255.10.24	Von_FortiScanner_Team_Devices	von-lvua-amd64			
Demo	Scanned	Once	2/5/2024 05:57 PM	2/5/2024 06:25 PM	2/5/2024 05:57 PM	27 minutes	172.17.3.240 + 1	Demo	Test-168-1-107			
Demo	Scanned	Once	2/5/2024 05:57 PM	2/5/2024 06:22 PM	2/5/2024 05:57 PM	25 minutes	10.100.100.100 + 1	Demo	Host-3-196			
Demo	Scanned	Once	2/5/2024 05:57 PM	2/5/2024 06:09 PM	2/5/2024 05:57 PM	12 minutes	172.17.3.0/24 + 1	Demo	Test-17-3-107			
Demo	Scanned	Once	2/5/2024 04:00 PM	2/5/2024 04:12 PM	2/5/2024 04:00 PM	12 minutes	172.17.3.0/24 + 1	Demo	Test-17-3-107			
Demo	Scanned	Once	2/5/2024 04:00 PM	2/5/2024 04:25 PM	2/5/2024 04:00 PM	25 minutes	10.100.100.100 + 1	Demo	Host-3-196			
Demo	Scanned	Once	2/5/2024 03:59 PM	2/5/2024 04:27 PM	2/5/2024 03:59 PM	27 minutes	172.17.3.240 + 1	Demo	Test-168-1-107			
Demo	Scanned	Once	2/2/2024 02:19 PM	2/2/2024 02:47 PM	2/2/2024 02:19 PM	27 minutes	172.17.3.240 + 1	Demo	Test-168-1-107			
Demo	Scanned	Once	2/2/2024 01:51 PM	2/2/2024 02:03 PM	2/2/2024 01:51 PM	12 minutes	172.17.3.0/24 + 1	Demo	Test-17-3-107			
Demo	Scanned	Once	2/2/2024 11:24 AM	2/2/2024 11:36 AM	2/2/2024 11:24 AM	11 minutes	172.17.3.0/24 + 1	Demo	Test-17-3-107			

Authentication Scanning

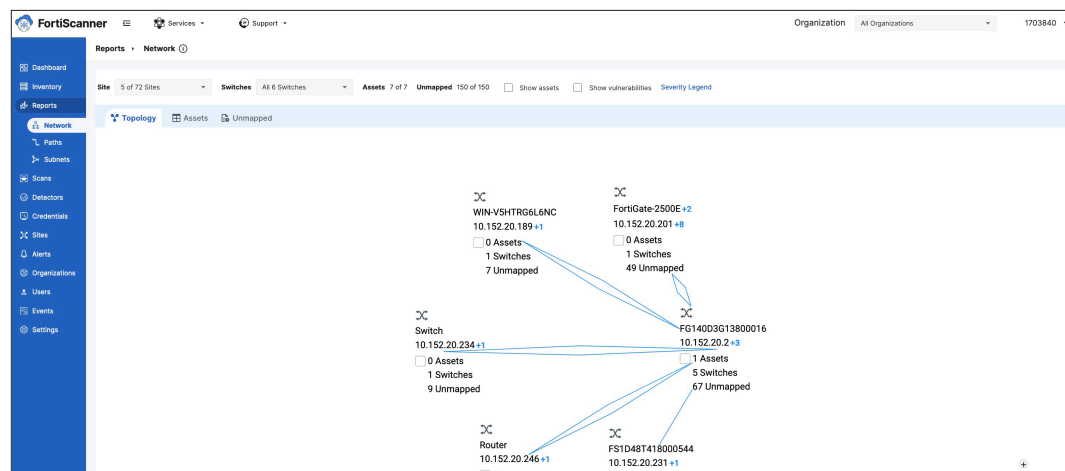
- Perform the scanning against the servers (SSH, SNMP, Telnet, VMware) using the authentication credentials
- Collect system information, applications, and software running; make the correlation with vulnerability analysis



Credential Name	Credential Type	Organization	OWF Allow List	Created By	Creation Time	In Use	Description
winapp-ssh	SSH	Research	10.152.48.23	Yibo Guo	2024/07/11 10:53	Currently In Use	
Authentication without privacy	SNMPv3	Research	10.152.20.6	Yibo Guo	2024/07/09 14:35	Not Used	
winvm-domain	Windows	Research	10.255.253.188	Yibo Guo	2024/07/08 15:57	Currently In Use	
SNMPv3-ryusei@red5	SNMPv3	Research	10.255.253.186	Yibo Guo	2024/07/06 18:08	Currently In Use	
163	VMware ESX SOAP API	Research	10.152.20.163	Yibo Guo	2024/07/06 17:52	Currently In Use	
winvm-188	Windows	Research	gy5188.redteam.com	Yibo Guo	2024/07/06 17:51	Currently In Use	
telnet186	Telnet	Research	10.255.253.186	Yibo Guo	2024/07/06 17:49	Currently In Use	
186ssh-glass	SSH	Research	10.255.253.186 + 1	Yibo Guo	2024/07/06 17:45	Currently In Use	
286snmpv2	SNMPv1/v2c	Research	10.255.253.186	Yibo Guo	2024/07/06 17:32	Currently In Use	

Reports

Reports quickly identify which Asset is compromised with high vulnerability and more information such as Switch and the port the device is connected to



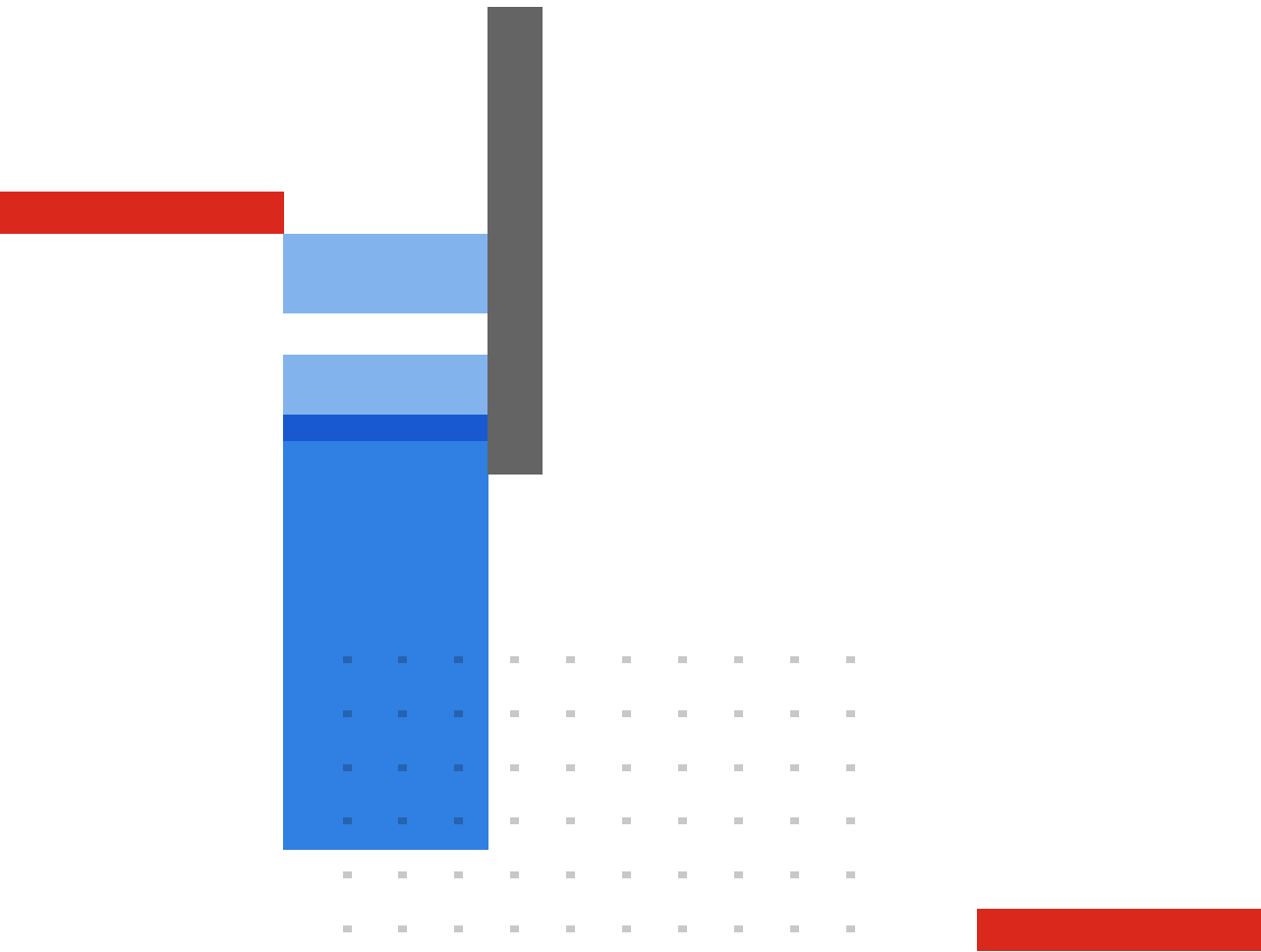
Ordering Information

Product	SKU	Description
FortiScanner Cloud Subscription	FC1-10-SCCLD-1111-01-DD	Annual Subscription for FortiScanner Cyber Assets Attack Surface Management service, for 500 assets, includes FortiCare Premium Services.
	FC2-10-SCCLD-1111-01-DD	Annual Subscription for FortiScanner Cyber Assets Attack Surface Management service, for 1000 assets, includes FortiCare Premium Services.
	FC3-10-SCCLD-1111-01-DD	Annual Subscription for FortiScanner Cyber Assets Attack Surface Management service, for 5000 assets, includes FortiCare Premium Services.

FortiCare Support Service



FortiCare Support Services is per-device support services, and it provides customers access to over 1400 experts to ensure efficient and effective operations and maintenance of their Fortinet capabilities. Global technical support is offered 24×7 with flexible add-ons, including enhanced service level agreements (SLAs) and premium hardware replacement through 200+ in-country depots.



www.fortinet.com

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.