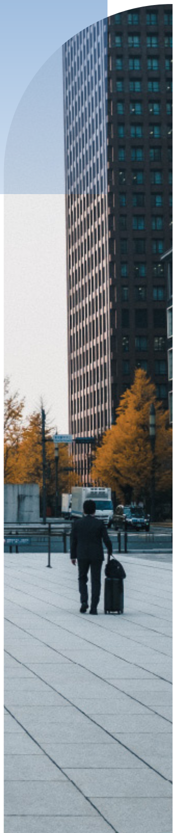
DEPLOYMENT GUIDE

Fortinet and Attivo Networks



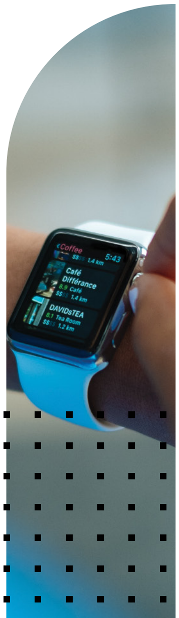


Table of Contents

Overview

Fortinet secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface, and the power to take on ever-increasing performance requirements of the borderless network—today and into the future. Only the Fortinet Security Fabric architecture can deliver security features without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. Fortinet ranks number 1 in the most security appliances shipped worldwide and more than 400,000 customers trust Fortinet to protect their businesses. Learn more at https://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

About Attivo Networks

Attivo Networks is the leader in deception for cybersecurity defense. Founded on the premise that even the best security systems cannot prevent all attacks, Attivo provides the required in-network visibility and substantiated, actionable alerts to detect and analyze cyberattacks, and accelerates defense through integration with prevention systems.

The core solution offered is the ThreatMatrix Deception-based Threat Detection and Continuous Response Platform, which is a comprehensive deception platform for detecting all types of threat vectors in user networks, data centers, and specialty environments of supervisory control and data acquisition (SCADA), Internet of Things (IoT), and point of sale (POS).

Deployment Prerequisites

1. Fortinet FortiGate—Supported versions are 5.2.0 to 5.6.1
2. Attivo Networks—Supported version is 4.0.1.34

For an Attivo BOTsink license, please contact the appropriate channels through Attivo. To request an evaluation of Attivo's Botsink, contact support@attivonetworks.com.

FORTINET FABRIC-READY

Attivo's BOTsink integrates with the Fortinet FortiGate firewall. Through this integration, BOTsink can provide the details of compromised endpoints such that they are immediately quarantined by the Fortinet FortiGate.

Fortinet and Attivo Networks have partnered to deliver an industry-leading security solution that addresses these challenges. The Attivo dynamic deception solution provides organizations with a way to complement their existing security infrastructure by continuously detecting and alerting them to breaches that have bypassed perimeter solutions. Fortinet's award-winning FortiGate Enterprise Firewall Platform provides the industry's highest-performing firewall capabilities and Fortinet's FortiGuard Security Subscription Services provide the industry's highest level of threat research, intelligence, and analytics. Bringing Fortinet and Attivo products together into one integrated solution delivers comprehensive endpoint and network security protection.

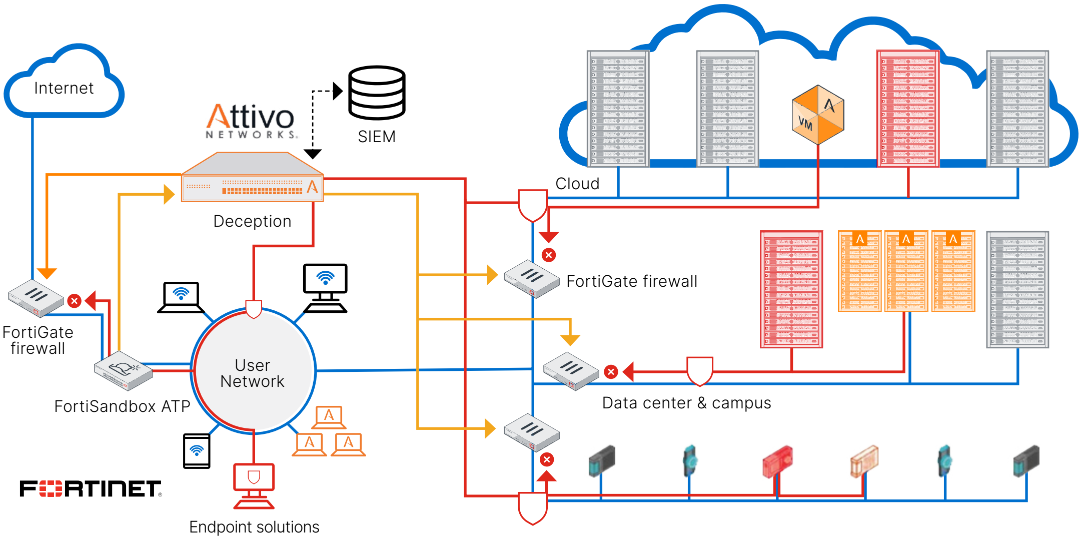
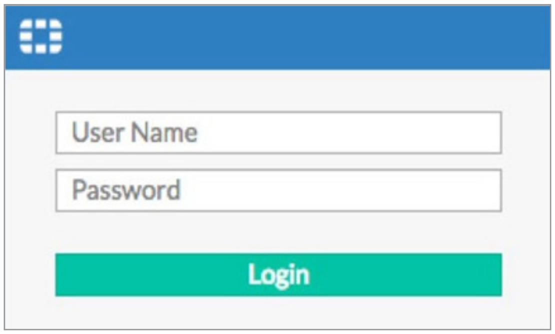


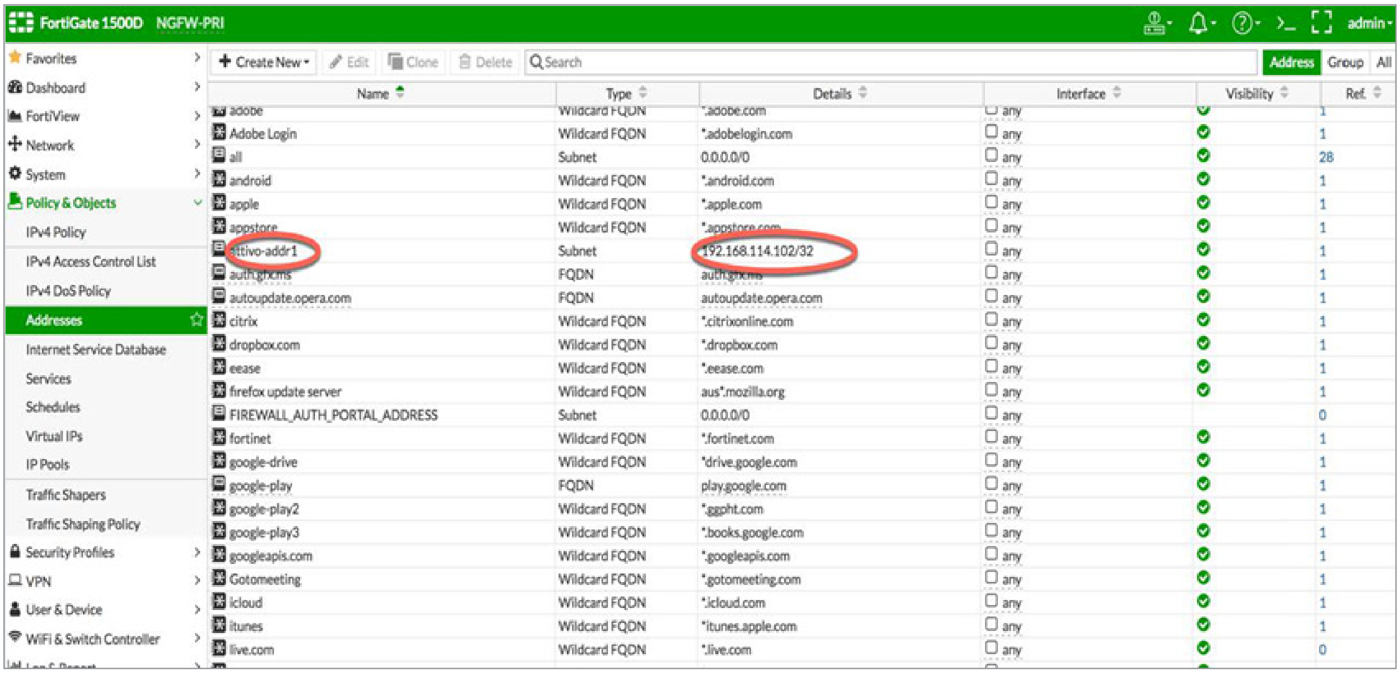
Figure 1: Architecture overview.

Fortinet Configuration

1. Log in to the FortiGate.



2. Whenever endpoint is quarantined from Attivo's BOTsink, it would create a dynamic access rule on FortiGate to block the endpoint. Below is the screenshot:

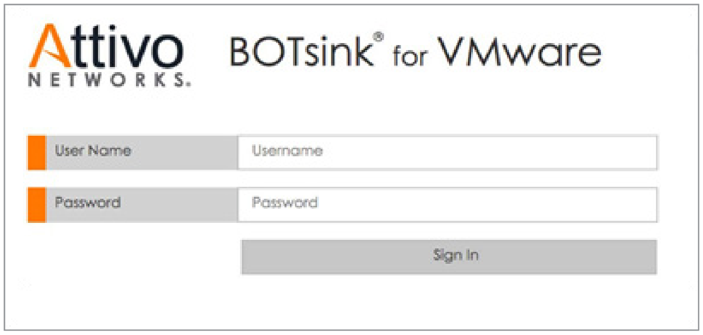


Name	Type	Details	Interface	Visibility	Ref.
adobe	Wildcard FQDN	*.adobe.com	□ any	✓	1
Adobe Login	Wildcard FQDN	*.adobelogin.com	□ any	✓	1
all	Subnet	0.0.0.0/0	□ any	✓	28
android	Wildcard FQDN	*.android.com	□ any	✓	1
apple	Wildcard FQDN	*.apple.com	□ any	✓	1
appstore	Wildcard FQDN	*.appstore.com	□ any	✓	1
attivo-addr1	Subnet	192.168.114.102/32	□ any	✓	1
auth.gfx.ms	FQDN	auth.gfx.ms	□ any	✓	1
autoupdate.opera.com	FQDN	autoupdate.opera.com	□ any	✓	1
citrix	Wildcard FQDN	*.citrixonline.com	□ any	✓	1
dropbox.com	Wildcard FQDN	*.dropbox.com	□ any	✓	1
eease	Wildcard FQDN	*.eease.com	□ any	✓	1
firefox update server	Wildcard FQDN	aus*.mozilla.org	□ any	✓	1
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0	□ any		0
fortinet	Wildcard FQDN	*.fortinet.com	□ any	✓	1
google-drive	Wildcard FQDN	*drive.google.com	□ any	✓	1
google-play	FQDN	play.google.com	□ any	✓	1
google-play2	Wildcard FQDN	*.ggpht.com	□ any	✓	1
google-play3	Wildcard FQDN	*.books.google.com	□ any	✓	1
googleapis.com	Wildcard FQDN	*.googleapis.com	□ any	✓	1
Gotomeeting	Wildcard FQDN	*.gotomeeting.com	□ any	✓	1
icloud	Wildcard FQDN	*.icloud.com	□ any	✓	1
itunes	Wildcard FQDN	*itunes.apple.com	□ any	✓	1
live.com	Wildcard FQDN	*.live.com	□ any	✓	0

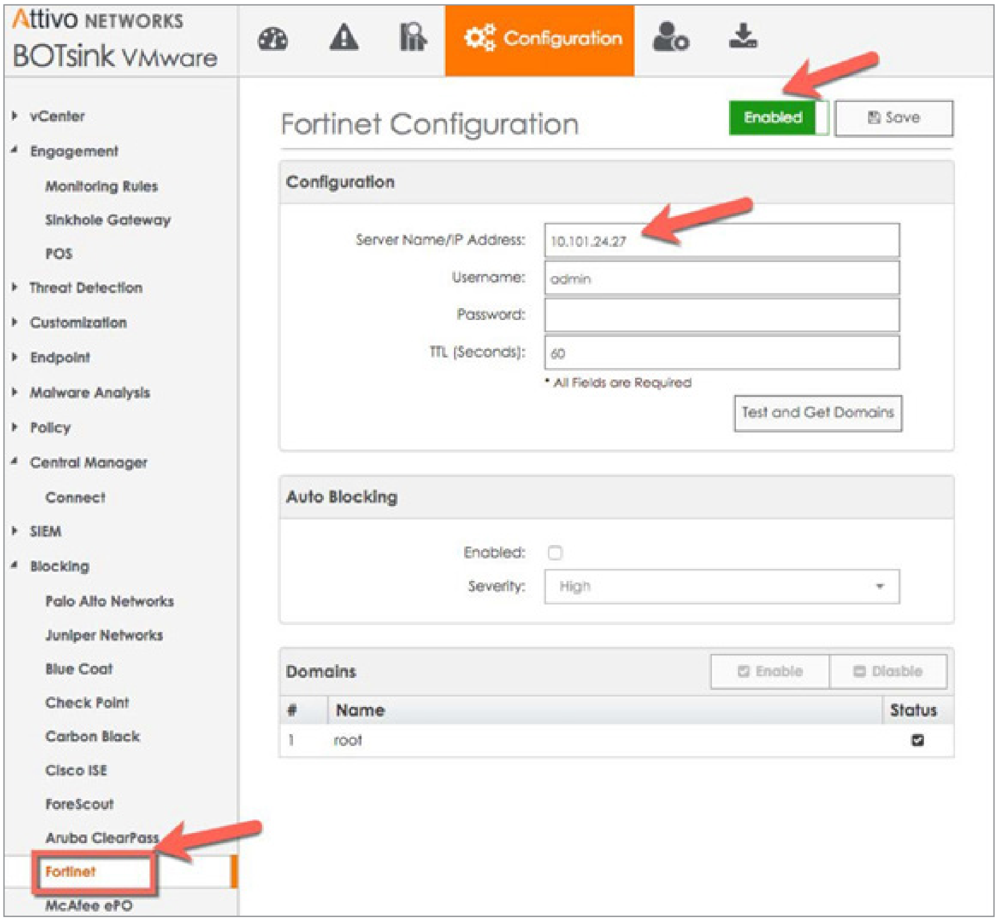
Attivo BOTsink Configuration

1. Log in to the Attivo BOTsink console.

   Note: You will need to log in to Attivo BOTsink using a user with admin privileges.



2. To enable the FortiGate integration, navigate to Configuration → Blocking → Fortinet. Add FortiGate IP in the Server Name/IP Address tab and also place the username as admin and password: FortiGate Password. Save the configuration by clicking Save.



Fortinet Configuration

Configuration

Server Name/IP Address: 10.101.24.27

Username: admin

Password:

TTL (Seconds): 60

* All Fields are Required

Auto Blocking

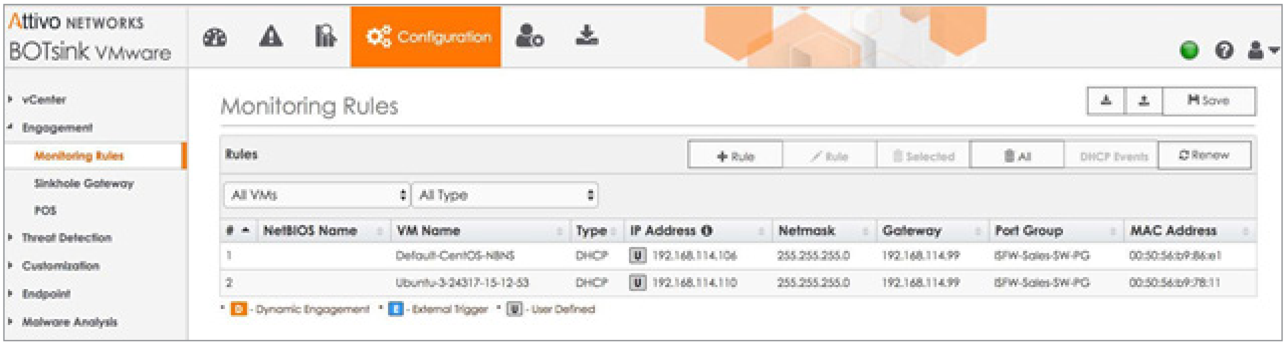
Enabled: □

Severity: High

Domains

#	Name	Status
1	root	☑

3. Create a monitoring rule to deploy an engagement VM in the required subnet. Click the Configuration button, select Monitoring Rules, and click Rule. Click Save in the Monitoring Rules page for the engagement VMs to acquire the configured IP addresses.



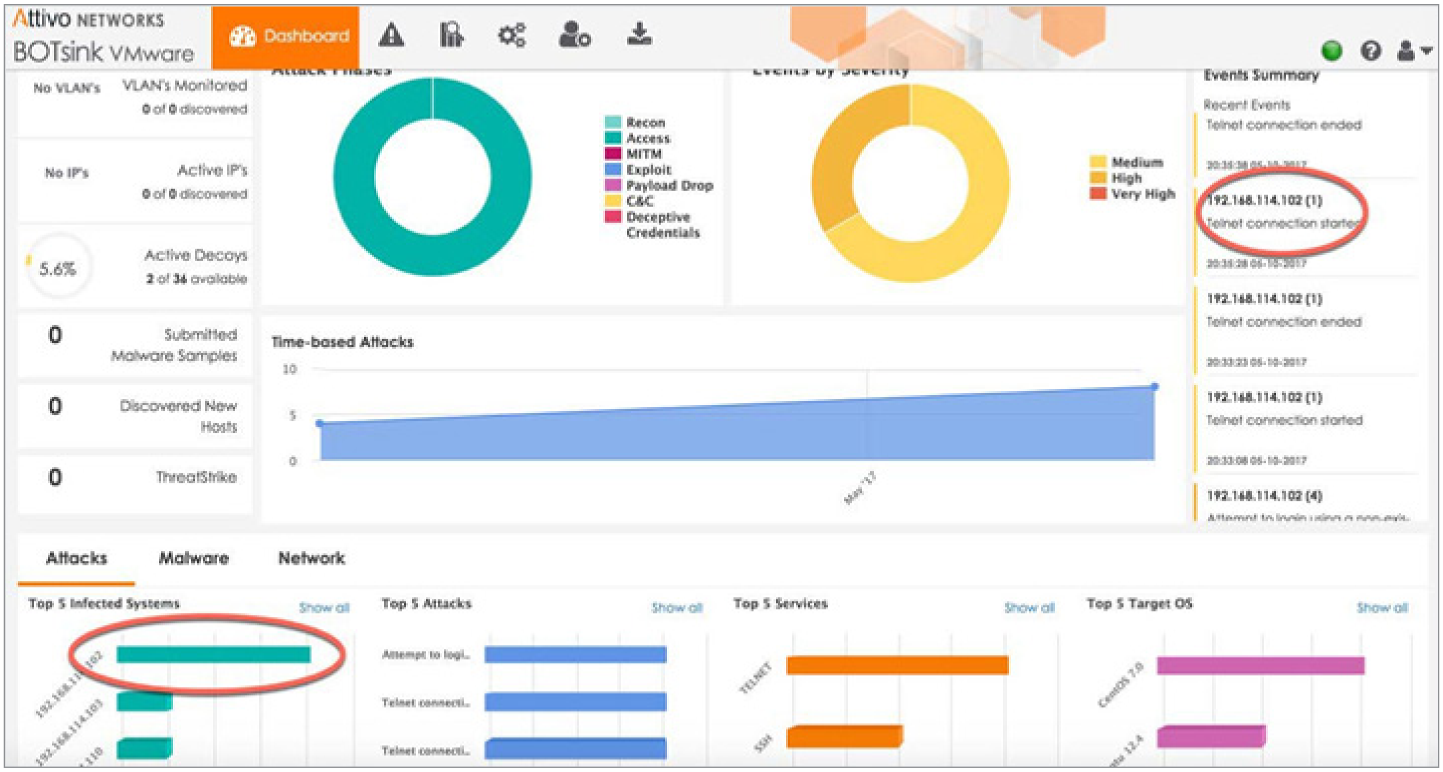
Monitoring Rules

Rules

#	NetBIOS Name	VM Name	Type	IP Address	Netmask	Gateway	Port Group	MAC Address
1		Default-CentOS-NBNS	DHCP	U 192.168.114.106	255.255.255.0	192.168.114.99	ISFW-Sales-SW-PG	00:50:56:b9:86:e1
2		Ubuntu-3-24317-15-12-53	DHCP	U 192.168.114.110	255.255.255.0	192.168.114.99	ISFW-Sales-SW-PG	00:50:56:b9:78:11

* D - Dynamic Engagement * E - External Trigger * U - User Defined

4. The BOTsink dashboard gives Attack Phases and Top 5 Infected Systems.



Events Summary

Recent Events

Telnet connection ended

20:35:38 05-10-2017

192.168.114.102 (1)

Telnet connection started

20:35:28 05-10-2017

192.168.114.102 (1)

Telnet connection ended

20:33:23 05-10-2017

192.168.114.102 (1)

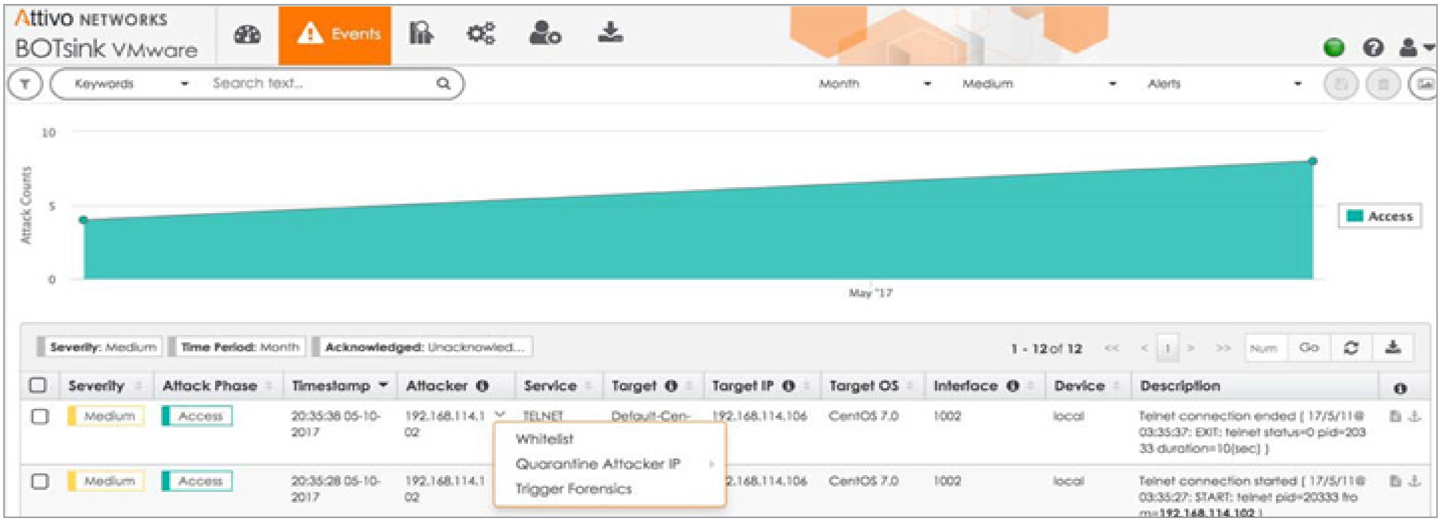
Telnet connection started

20:33:08 05-10-2017

192.168.114.102 (4)

Attempt to login using a non-exis-

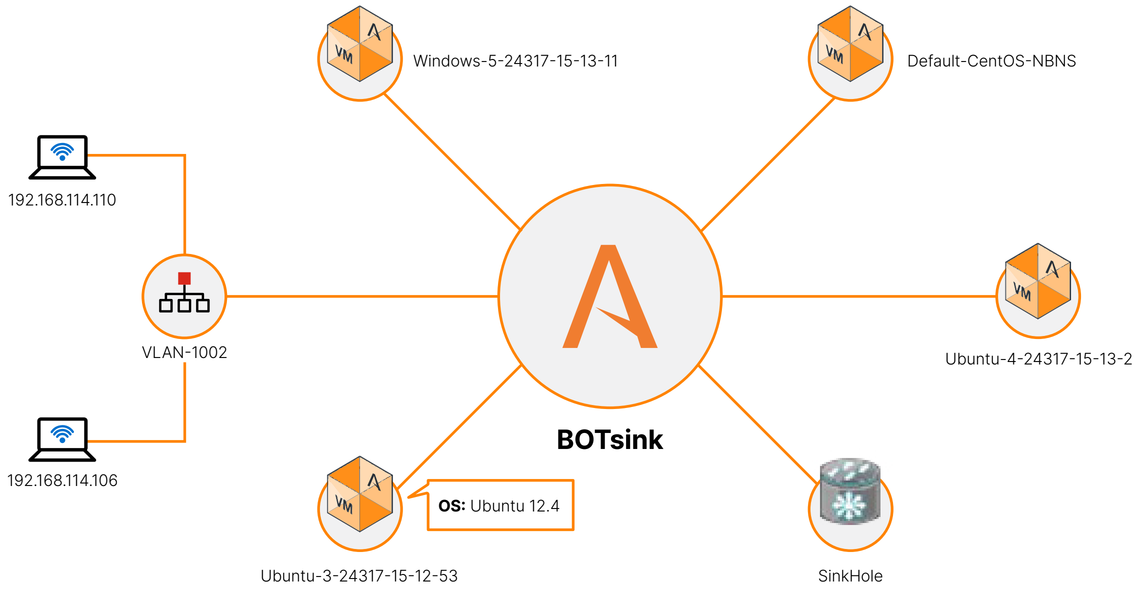
5. Dashboard → Events gives an option to Whitelist/Quarantine Attacker IP/Trigger Forensics.



Severity: Medium | Time Period: Month | Acknowledged: Unacknowled...

	Severity	Attack Phase	Timestamp	Attacker	Service	Target	Target IP	Target OS	Interface	Device	Description
□	Medium	Access	20:35:38 05-10-2017	192.168.114.102	TELNET	Default-Cen-	192.168.114.106	CentOS 7.0	1002	local	Telnet connection ended (17/5/11@03:35:37: EXIT: telnet status=0 pid=20333 duration=10(sec))
□	Medium	Access	20:35:28 05-10-2017	192.168.114.102			2.168.114.106	CentOS 7.0	1002	local	Telnet connection started (17/5/11@03:35:27: START: telnet pid=20333 from=192.168.114.102)

6. A topology diagram is created dynamically on the BOTsink.



Summary

- Access to FortiGate Demo: https://fortigate.fortidemo.com
- FortiGate Administration Guide: http://docs.fortinet.com/fortigate/admin-guides
- Contact support@attivonetworks.com (or your sales representative/sales engineer) if you need any assistance with the Attivo Networks solution or for any guides/documents.

www.fortinet.com