SOLUTION BRIEF

Fortinet and Trend Micro Security Solution

SIEM, Security Orchestration, and Incident Response, Together With Endpoint Security Protection

Executive Summary

Trend Micro integrations with Fortinet FortiSOAR and FortiSIEM products offer customers a powerful combination of broad visibility, security analytics, event management, orchestration, automated response, and remediation, together with endpoint protection. Customers can leverage the integrations and the Fortinet Security Fabric platform across an organization's security infrastructure, delivering unparalleled visibility and protection.

Customer Challenges

As digital transformation sweeps through every industry, the attack surface grows dramatically, making security management increasingly difficult. Security teams struggle to keep up with the deluge of alerts and other information generated by their multitude of security devices. And the cybersecurity skills gap only makes this more difficult.

Infrastructure, applications, and endpoints (including Internet-of-Things [IoT] devices) must all be secured. This requires visibility of all devices and all the infrastructure—in real time. Organizations also need to know what devices represent a threat and where.

In addition, organizations need a security automation framework that pulls together all of their organization's tools and unifies operations, eliminating alert fatigue and reducing context switching. This allows organizations to not only adapt but also optimize their security processes.

Joint Solution

Trend Micro and Fortinet have partnered to deliver an integrated security solution that delivers security information and event management (SIEM) and security orchestration, automation, and response (SOAR) capabilities, together with endpoint security protection.

Fortinet FortiSIEM brings together visibility, correlation, automated response, and remediation in a single, scalable solution. It reduces the complexity of managing network and security operations to effectively free resources, improve breach detection, and even prevent breaches. The FortiSIEM architecture enables unified data collection and analytics from diverse information sources including logs, performance metrics, security alerts, and configuration changes. FortiSIEM combines the analytics traditionally monitored in separate silos of the security operations center (SOC) and network operations center (NOC) for a more holistic view of the security and availability of the business.

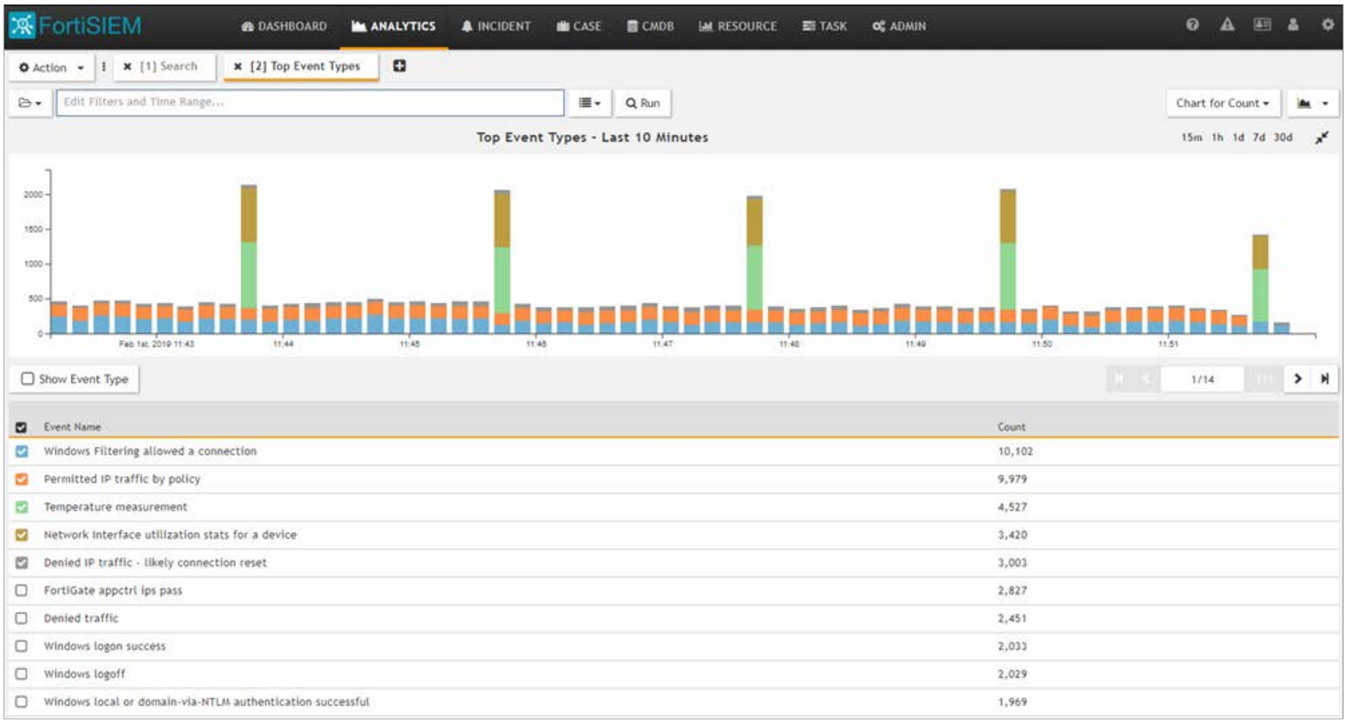
Joint Solution Components

- Fortinet FortiSOAR
- Fortinet FortiSIEM
- Trend Micro Apex Central
- Trend Micro Apex One
- Trend Micro Deep Security
- Trend Micro Endpoint Sensor
- Trend Micro Deep Discovery Analyzer
- Trend Micro Web Security

Joint Solution Benefits

- Unified event correlation and risk management for your entire deployment
- Security and compliance out of the box
- Streamline SOC efficiencies and accelerate incident response
- Eliminate repetitive tasks through automation, correlation of incidents, threat intelligence, and vulnerability data

FORTINET Fabric-Ready

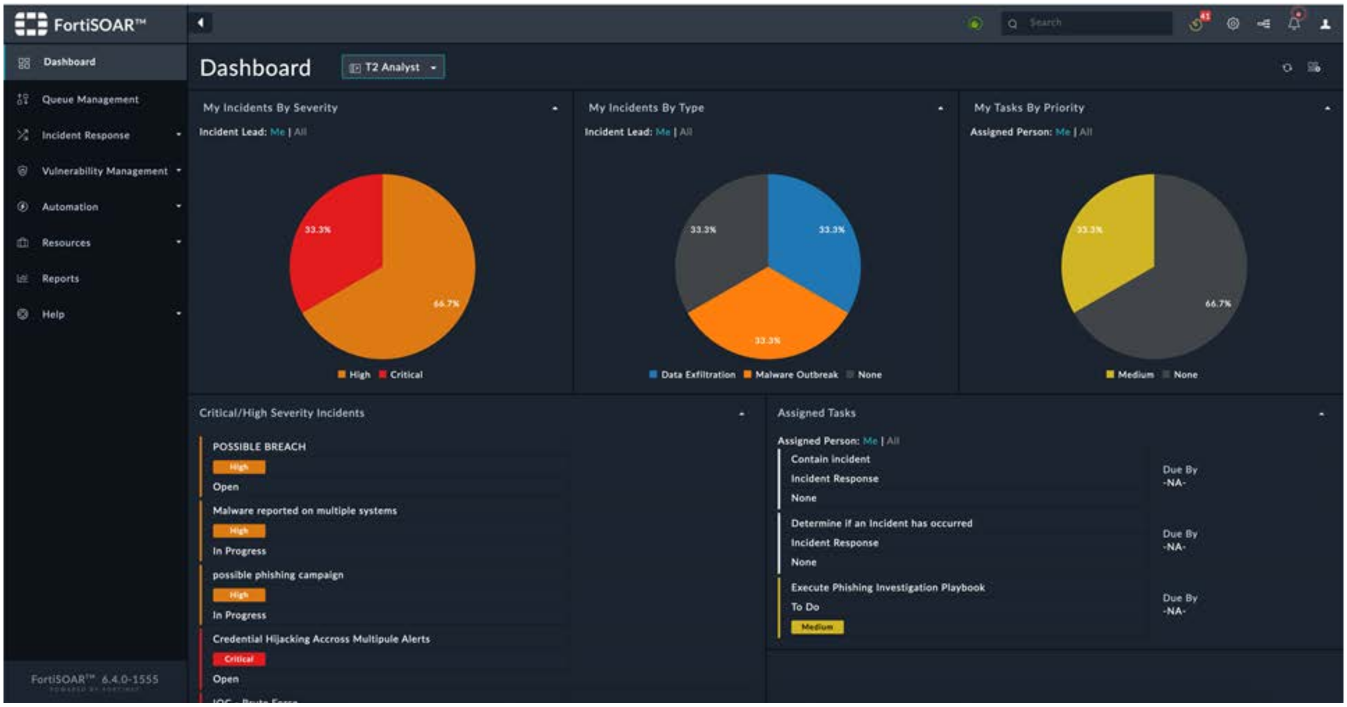


Top Event Types - Last 10 Minutes

☑	Event Name	Count
☑	Windows Filtering allowed a connection	10,102
☑	Permitted IP traffic by policy	9,979
☑	Temperature measurement	4,527
☑	Network Interface utilization stats for a device	3,420
☑	Denied IP traffic - likely connection reset	3,003
□	FortiGate appctrl ips pass	2,827
□	Denied traffic	2,451
□	Windows logon success	2,033
□	Windows logoff	2,029
□	Windows local or domain-via-NTLM authentication successful	1,969

Figure 1: FortiSIEM security analytics.

FortiSOAR is a holistic security orchestration, automation, and response workbench, designed for SOC teams to efficiently respond to the ever-increasing influx of alerts, repetitive manual processes, and shortage of resources. This patented and customizable security operations platform provides automated playbooks, incident triaging, and real-time remediation for enterprises to identify, defend, and counter attacks. FortiSOAR optimizes SOC team productivity by seamlessly integrating with over 300 security platforms and over 3,000 actions. This results in faster responses, streamlined containment, and reduced mitigation times from hours to seconds.



Dashboard

My Incidents By Severity
Incident Lead: Me | All

My Incidents By Type
Incident Lead: Me | All

My Tasks By Priority
Assigned Person: Me | All

Critical/High Severity Incidents

POSSIBLE BREACH
High
Open

Malware reported on multiple systems
High
In Progress

possible phishing campaign
High
In Progress

Credential Hijacking Accross Multipule Alerts
Critical
Open

IOC - Brute Force

Assigned Tasks

Assigned Person: Me | All

Contain incident
Incident Response
None
Due By
-NA-

Determine if an Incident has occurred
Incident Response
None
Due By
-NA-

Execute Phishing Investigation Playbook
To Do
Medium
Due By
-NA-

Figure 2: FortiSOAR dashboard.

The Trend Micro integration with FortiSOAR enables coordination of proactive actions and automated response, which is fundamental to driving customer objectives for security and automation. Integrating solutions that can detect sophisticated cyber threats and automate responses to limit damage from threats through isolation, security orchestration, and remediation is key to preparing, defending, and responding to these types of attacks.

For automation and orchestration of security operations, FortiSOAR connectors integrate with Trend Micro Apex Central (formerly Control Manager), Trend Micro Apex One, Trend Micro Deep Security, Trend Micro Endpoint Sensor, and Trend Micro Deep Discovery Analyzer. This allows security operations teams to optimize and automate their security processes to implement sophisticated response actions.

Trend Micro security products can send security intelligence to FortiSIEM for security event management. FortiSIEM integrates with Trend Micro Web Security, Trend Micro Apex One, and Trend Micro Deep Discovery.

In summary, the Trend Micro and Fortinet integrations benefit customers by linking together different applications within their security environment, to offer a powerful combination of broad visibility, security analytics, event management, orchestration, automated response, and remediation, together with endpoint protection. Customers can leverage the integrations and the Fortinet Security Fabric platform across an organization's security infrastructure, delivering unparalleled visibility and protection.

About Trend Micro

Trend Micro, a global leader in cybersecurity, helps make the world safe for exchanging digital information. Leveraging over 30 years of security expertise, global threat research, and continuous innovation, Trend Micro enables resilience for businesses, governments, and consumers with connected solutions across cloud workloads, endpoints, email, IIoT, and networks. www.trendmicro.com.

FORTINET®

www.fortinet.com

January 15, 2021 6:46 AM

D:\Fortinet\Solution Brief\Grey Solution Brief\Trend Micro\sb-fortinet-and-trend-micro-security-solution-1152021\sb-fortinet-and-trend-micro-security-solution-1152021

881161-0-0-EN