FORTINET | cyber OBSERVER

SOLUTION BRIEF

Fortinet and Cyber Observer Security Solution

Cybersecurity Orchestration, Management, and Awareness

Executive Summary

Even the best security product can be circumvented if the security policy is not well-defined. Several recommendations for creating a well-defined security policy exist. One is the Critical Security Controls from the Center for Internet Security. This is a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. A principal benefit of the Controls is that they prioritize and focus a smaller number of actions with high pay-off results. The Controls are effective because they are derived from the most common attack patterns highlighted in the leading threat reports and vetted across a very broad community of government and industry practitioners.

Cyber Observer's partnership with Fortinet enables CISOs and their security teams to manage and monitor their cybersecurity posture across the entire network ecosystem. The solution monitors the FortiGate enterprise firewall rules, policies, and settings, and alerts on key aspects and issues that could affect the entire organization. This offers executives a single-pane-of-glass view into the effectiveness of their security policy, as well as a validation with respect to compliance and controls that apply to the organization, empowering management to effectively drive posture and maturity forward.

Solution Description

The award-winning Fortinet FortiGate enterprise firewall platform offers protection from a broad array of threats. FortiGate provides high-performance, layered security services and granular visibility for end-to-end protection across the entire enterprise network. FortiGate is a key part of the Fortinet Security Fabric, which enables security components to collect and

share intelligence between devices, systems, and partners, support unified management, and synchronize and automate responses to threats. The open, end-to-end fabric of security

solutions—woven together to scale and adapt as business demands change—enables organizations to address the full spectrum of challenges they currently face across the expanding attack surface. The FortiGate platform also leverages global threat intelligence to protect individual customers, by using Fortinet FortiGuard Security Subscription Services to enable visibility and control for next-generation protection against advanced threats, including zero-day attacks.

Cyber Observer's partnership with Fortinet enables CISOs and their security teams to orchestrate and manage their cybersecurity ecosystem and receive alerts from Cyber Observer regarding key aspects of FortiGate enterprise firewalls including

Joint Solution Components

- Fortinet FortiGate
- Cyber Observer

About Cyber Observer

Cyber Observer produces a holistic posture management & awareness solution for CISOs, CIOs & senior managers that integrates easily and quickly to provide an unprecedented & comprehensive representation and analysis of an enterprise's entire cybersecurity ecosystem.

Learn more at:

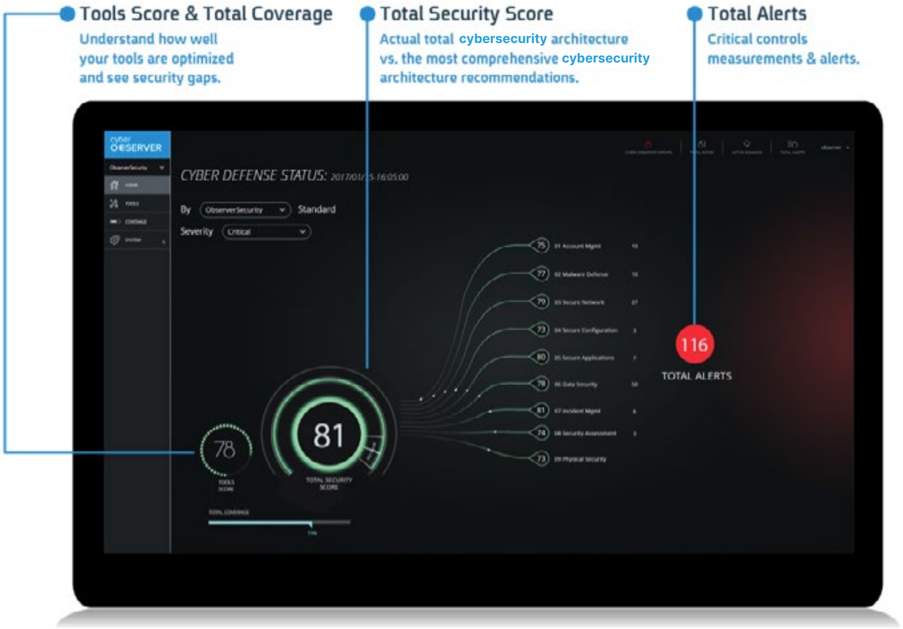
www.cyber-observer.com

FORTINET FABRIC-READY

configuration, rules, and policies. The joint effort helps enterprises manage their cybersecurity environment while continuously monitoring their cybersecurity ecosystem posture.

Cyber Observer is automatically deployed in the corporate network in a matter of a few hours, predefined with FortiGate enterprise firewall Critical Security Controls (CSC) measurements to deliver the following:

- Current configuration implementation status (features, updates, etc.) based on the vendor's and security standards best practices
- Current security status (rules, policies, etc.) based on the vendor's and security standards best practices
- Alerts on deviation from daily normal behavior in terms of the firewall's implementation and effectiveness as well as continuously monitoring relevant security issues in near real time
- Recommended steps for improvement



Solution Benefits

The plug-and-play integration between Cyber Observer and Fortinet offers powerful security effectiveness and resilience visibility, as well as compliance validation and controls for securing and monitoring FortiGate firewalls from a management perspective in an unprecedented manner. The joint solution delivers the following benefits:

- Provides organizations with the best indicators as to the types of cybersecurity applications and tools that are misconfigured, malfunctioning, or need to be deployed.
- Reveals security gaps that exist in each security domain and delivers continuous proactive recommendations that need to be closed, leading to greatly improved security.
- The Cyber Observer machine learning analytics engine continuously calculates on-line measurements that represent normal behavior; it then alerts in case of deviation from normal behavior.
- The solution leverages the industry's best validated security protection offered by Fortinet's award-winning FortiGate network security platform to protect againstsophisticated cyber threats.

FORTINET

www.fortinet.com

August 27, 2021 4:59 PM

Macintosh HD:Users:austin:Dropbox (Red Rider):Clients:Fortinet:Solution Brief Updates:Working Group 2:sb-fortinet-cyberobserver:sb-fortinet-cyberobserver_2021

429118-A-0-EN