SOLUTION BRIEF

The Fortinet - SecurityMatters Security Solution

Comprehensive Cybersecurity for Industrial and Critical Infrastructure

Executive Summary

The digital trends of Industry 4.0 and Internet of Things (IoT) have improved the way we travel, produce products, power our cities and live our lives. Despite the many benefits of intelligent and interconnected industrial systems, the trend has also presented asset owners and cybersecurity stakeholders with new challenges.

Today, the average security operations analyst must manage and mitigate network misconfigurations, various device malfunctions and potential network policy misuses. Moreover, cyber and ransomware attacks have begun to target industrial control systems (ICS) at an alarming rate. According to Forrester research, 79% of organizations with a SCADA/ICS network have suffered a breach in the past 24 months and 70% of organizations suffer from lack of visibility into their ICS assets. Clearly, the disparity that exists between enterprise security and control systems must be bridged with a comprehensive and holistic approach to cybersecurity.

Joint Solution Description

The joint solution combines SilentDefense's core IP with the advanced threat detection and remediation capabilities of the FortiGate industrial firewall to bring next-generation OT threat monitoring, detection and protection capabilities to customers. Together, the Fortinet-SecurityMatters solution supports a seamless and secure gateway between the OT and IT networks, minimizing threat discovery difficulty and expediting informed remediation of threats.

Joint Solution Benefits

- Extended visibility and monitoring of geo-distributed industrial and enterprise networks
- Improved IT/OT analyst collaboration with central threat detection and monitoring tools
- Better policy and provisioning enforcement due to more accurate asset inventories
- Informed threat prioritization and escalation due to OT-specific threat detection capabilities

FORTINET Fabric-Ready

Fortinet and SecurityMatters have partnered to deliver an industry-leading OT security solution to address these challenges. SecurityMatters SilentDefense integrates to the industry leading open architecture of the Fortinet Security Fabric that is designed around a series of open APIs, Open Authentication Technology, and standardized telemetry data to enable organizations to provide end-to-end security without compromise.

SilentDefense's non-intrusive monitoring capabilities for ICS assets rapidly baseline network behavior and detect malicious and operational threats with an unprecedented degree of detail and accuracy. By integrating with FortiGate, SecurityMatters is able to extend the visibility and utility of the Fortinet Security Fabric even further.

The ability of the SecurityMatters' platform to provide visibility and detailed asset inventories of ICS assets the key reason why SecurityMatters is a valued part of the Fortinet Security Fabric. With SilentDefense and FortiGate working in concert, ICS asset owners are better able to protect their infrastructure from the latest cyber threats, support ambitious preventative maintenance initiatives, minimize downtime and maintain a higher degree of safety for employees and the public.

SecurityMatter SilentDefense

SecurityMatters' SilentDefense is the most advanced and mature real-time network monitoring and intelligence platform for ICS networks. With SilentDefense, customers can monitor and visualize their entire OT network with zero impact on running processes. SilentDefense's deep packet inspection (DPI) and patented threat detection technology empowers customers with the ability to analyze industrial communications in real-time and automatically generate complete asset inventories. SilentDefense provides users with rich device details that include OS version, open ports, device vendor and model, firmware version, serial number, I/O modules and vulnerabilities for all major ICS vendors and industrial protocols.

In addition to its asset inventory capabilities, SilentDefense features a vast threat database called the Industrial Threat Library (ITL), offering users with over 1600 custom threat checks upon deployment. This multi-factor and vector approach to threat detection in extremely effective identifying and prioritizing both cybersecurity and operational indicators of compromise before they become an issue of significance.

Fortinet FortiGate Enterprise Firewall

Complementing SecurityMatters capabilities in the solution is Fortinet's award-winning FortiGate Enterprise Firewall Platform, which provides end-to-end security services across the entire network. This is strengthened by Fortinet's FortiGuard Security Subscription Services which provide the industry's highest level of threat research, intelligence, and analytics. The solution leverages Global Threat Intelligence to protect individual customers, by using FortiGuard to enable visibility and control for next-generation protection against advanced threats, including zero-day attacks.

Use Case: Electric-power

Challenge: RTUs are used by grid operators to control and collect information from remote substations. FortiGate allow asset owners to restrict access to RTUs (e.g. allowing only the Energy Management Systems to communicate with them) and to limit the commands that can be issued to them. Despite these restrictions, it is still possible for an attacker or insider to disrupt operations by issuing a legitimate command with anomalous parameters, like resetting the remote device or worse by putting it in a faulty status until a full power-off power-on cycle is (manually) executed. SecurityMatters has discovered several similar (unknown) vulnerabilities over the years.

Solution: SecurityMatters' SilentDefense automatically generates a network whitelist based on communication patterns down to the commands being sent by observing and inspecting network traffic through complete packet dissection. This whitelist, which can be fully customized by operators, is later used to detect anomalies like an out of range parameter. SilentDefense can be deployed within the main control center, like the Energy Management System, to monitor all the remote connections carried out from a single location or from a remote location, like an electrical substation, to monitor not only incoming connections but also the local traffic from the devices behind the RTU.

Response: SilentDefense can inform and reconfigure FortiGate to block further attempts to access and reconfigure RTUs. In situations where the incident is suspicious, but not clearly malicious, SilentDefense can instruct FortiGate limit the kinds of commands that suspicious device can initiate over ICS protocols such as DNP3, IEC 60870-5-104, or Modbus.

Use Case: Oil & Gas

Challenge: OPC servers are typically used to share process and/or production data between different production and analysis systems. Organizations deploy firewalls to filter out unwanted and unauthorized communications, and only certain OPC message types are actually exposed to the corporate domain. In 2012, a previously unknown vulnerability was found in a widely deployed OPC server. The vulnerability allowed a remote attacker to exploit the ubiquitous OPC authentication interface by sending an anomalous amount of data, to trigger a buffer overflow and possibly execute arbitrary code on the target.

Solution: The accurate network whitelist automatically generated by SecurityMatters' SilentDefense detects anomalous commands and parameters in real-time, like an out of range value that could indicate an attempt to exploit a buffer overflow vulnerability. SilentDefense can be installed at remote sites within Layer 3 networks where OPC servers are typically deployed. As SilentDefense supports a wide range of industrial protocols, including proprietary ones from ABB, Emerson, Yokogawa, Siemens, etc., it can also be deployed within Layer 2 networks as well to detect anomalies and misuses occurring in Process Control Networks.

Response: SilentDefense works in concert with on the Fortinet's FortiGate to block further attempts to access and reconfigure OPC servers. New IPS signatures can be deployed on the FortiGate, and additional solutions of the Fortinet Security Fabric, to provide protections to vulnerable systems until patches can be deployed.

About SecurityMatters

SecurityMatters empowers critical infrastructure and manufacturing organizations with the ability to identify, analyze, and respond to industrial threats and flaws, minimizing troubleshooting costs and unexpected downtime. We leverage ICS-specific knowledge and understanding to provide visibility into critical assets and their activity and detect operational problems and cyber security threats. Our revolutionary network monitoring platform has been successfully deployed by customers worldwide. www.secmatters.com | info@secmatters.com

FORTINET

www.fortinet.com

October 11, 2019 2:38 AM

123456-0-0-EN

D:\Fortinet\Solution Briefs\grey solution briefs\Forescout\sb-the-fortinet-securitymatters-security-solution-v1