# ENERGY COMPANIES BENEFIT FROM INNOVATIVE SIEM-BASED SECURITY-AS-A-SERVICE FROM STRATEJM

*"FortiSIEM allows Stratejm to provide comprehensive end-to-end protection across highly complex environments. Coupling the unique capabilities of FortiSIEM with our expertise and experience has enabled us to create a compelling value proposition"*

– *John Menezes*
*CEO*
*Stratejm*

Canadian managed security services provider (MSSP) Stratejm is a proponent of the benefits of implementing a strategy based on detection and response to address today's threats. Founded in 2013, and located in Mississauga, Ontario, the company developed Canada's first Security-as-a-Service platform to enable North American customers to proactively manage cyber security risks in an intuitive, structured and cost-effective manner.

### TRADITIONAL SECURITY MEASURES CAN'T KEEP UP

John Menezes – Stratejm's founder, President and CEO – elaborated, "Customers often spend a lot of money on compartmentalized technology and even more on implementation: Their time-to-value was way too long and their effectiveness too short given the pace at which threats are evolving."

Menezes saw the opportunity to create an agile set of cloud-based services that could be scaled and configured to accommodate the dynamic needs of his customers. He and his team architected a framework based on identifying a highly flexible security incident and event management (SIEM) solution capable of delivering a rich feature set across a diverse selection of client environments.

### SECURITY AND NETWORKING PROWESS

"The Fortinet FortiSIEM platform has a unique ability to integrate security and network functions," said Menezes. "We conducted extensive lab testing to verify performance and features, and quickly realized that FortiSIEM is much more than a traditional SIEM. It had what we were looking for from the security operations center [SOC] perspective but it also had significant network operations center [NOC] capabilities. The combination delivers better overall protection and control; enabling us to achieve an accelerated time to value for both ourselves and our clients."

He added, "We saw how the multi-tenant architecture would provide us with the ability to manage many different customer domains – both physical and logical – and discrete systems and networks from a single console. We committed to utilizing FortiSIEM as the cornerstone of our Security-as-a-Service portfolio to deliver a compelling set of offerings to our clients at unrivalled price points."

Available as a virtual or physical appliance, Stratejm opted for a cloud-based FortiSIEM deployment to allow its own clients to select the exact combination of features, performance and coverage to fulfil their

## DETAILS

**PARTNER:** Stratejm

**CUSTOMERS:** Canadian Utility Customers

**INDUSTRY:** Energy

**LOCATION:** Ontario, Canada

## BUSINESS IMPACT

- Reduces complexity and resource requirements, accelerates integration and time to value
- Provides dynamic, context rich views of IT & OT environments
- Facilitates cloud-based 'consumption' delivery model
- Enables rapid onboarding of new clients

## SOLUTIONS

- FortiSIEM

precise needs: "We're able to offer a 'consumption' model to meet the specific individual requirement of every company that we work with," noted Menezes.

## UNIFYING THE WORLDS OF IT AND OT

A unique feature of FortiSIEM is its ability to span information technology (IT) and the control systems found in operational technology (OT) domains. "Traditionally, IT and OT infrastructures were totally separate but we are now seeing the two rapidly converge. With FortiSIEM, we're able to offer a unified solution that protects the entire environment," commented Menezes. "This is proving extremely attractive to clients, especially those designated as 'critical infrastructure' owners."

A Stratejm client – a power-distributor in Canada – concurred, "We started looking at alternatives once it became clear that our existing SIEM couldn't scale to meet our growth needs," explained the company CIO. "Stratejm's use of FortiSIEM to consolidate our IT and OT domains, along with combining world-class security and networking capabilities, is very compelling for us. The holistic approach gives us continuous visibility across our entire infrastructure and unifies what were traditionally siloed perspectives."

## REAL-TIME DISCOVERY AND MONITORING

The ability of FortiSIEM to perform real-time discovery across even the largest, most complicated environments has proven to be a key differentiator for Stratejm. Fortinet has developed an intelligent infrastructure and application discovery engine that identifies and maps all pertinent elements throughout each enterprise. The information is stored in a centralized management database (CMDB) and used to provide rich contextual insights that enhance the detection and remediation of potential threats.

"The CMDB is a unique capability that gives us an advantage over our competitors," recounted Menezes, "FortiSIEM provides our intelligence analysts 360-degree visibility into each of our clients' environments, encompassing assets such as endpoints, applications, storage, and network components. When an alert is generated, we're instantly equipped with contextual information that a typical security analyst could never get from a traditional SIEM."

## EXPEDITED ONBOARDING

The auto-discovery capabilities of FortiSIEM provide the ability to do rapid onboarding; assimilating new environments with ease. Another utility customer – a Canadian power company with over 2,000 devices – was up and running on FortiSIEM in remarkably short time. A company spokesperson confirmed, "We were expanding our operations and had two years left on a legacy SIEM contract, but we just couldn't scale or get the implementations times down to an acceptable level. Stratejm performed an inventory of our entire infrastructure, implemented and documented the processes, and had all the alerts and integrations in place, in an amazingly short period of time. Using FortiSIEM, it took Stratejm just weeks to accomplish what would have taken our other vendor at least a year!"

## MANAGING CHANGE AND CONFIRMING COMPLIANCE

The CMDB also identifies changes within individual infrastructures that may warrant further investigation. "In addition to the value from a change management perspective, many of our clients need to comply with broad sets of industry and governmental regulations. They therefore need to be able to archive log files that demonstrate to auditors that they're meeting the requirements. FortiSIEM is the perfect answer for them," stated Menezes.

## OPEN APIS

A comprehensive set of APIs is made available by Fortinet to enable 2-way integration with other systems and sources. "The open API has been fantastic. We're able to seamlessly integrate other products to further enhance our capabilities and it makes us highly compatible with whatever we come across in clients' environments," observed Menezes.

## MINIMIZING RISK AND DELIVERING VALUE

With real-time data collection, information is parsed and fed into an event-based analytics engine. The unified NOC and SOC data is what provides unprecedented context. Comprehensive dashboards and ad-hoc reports enable Stratejm analysts to rapidly identify root causes of threats. "FortiSIEM helps us practice good cyber hygiene. It shows us where gaps are across each environment and how to fix them; significantly reducing risk," explained Menezes.

He concluded, "FortiSIEM allows Stratejm to provide comprehensive end-to-end protection across highly complex environments. Coupling the unique capabilities of FortiSIEM with our expertise and experience has enabled us to create a compelling value proposition. FortiSIEM is phenomenal!"

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990



**June 6, 2018**