

Expo 2020 Dubai Mega-Event Ensures Security With Splunk

Key Challenges

Building a mega-event demands comprehensive, flexible security monitoring, and Expo 2020 Dubai needed a solution that could meet the dynamic needs of its diverse environment and enable vigilance against potential cybersecurity threats.

Key Results

The Splunk platform ingested multiple data sources, providing Expo with resilient cybersecurity capabilities and the ability to closely monitor a high volume of network events to take rapid preventive action.

Industry: Media and Entertainment

Solutions/Use Cases: IT Operations, Cyber Security, Platform

Data Sources: Web Servers, ERP system, Network Access Points

Protecting a unique mega-event is no easy feat.

Which is why cybersecurity has been a key priority for Expo 2020 Dubai since its inception.

The unique challenge for Expo 2020 Dubai is protecting an event of this magnitude and duration. The first of its kind in the region, this six-month event will host over 190 participants and their respective pavilions across 4.38 square kilometers, in addition to Expo thematic pavilions dedicated to sustainability, mobility and opportunity. The Expo team is responsible for securing the diverse, dynamic and fast-evolving technology ecosystem capable of supporting hundreds of participants and millions of visitors, including VIPs from around the globe.

To tackle these challenges, Expo 2020 required a security platform that could scale quickly, manage operational security for hundreds of different data sources and technology solutions, and be flexible enough to adapt to the evolving cybersecurity needs of the event. The Splunk platform proved to be the best solution to meet these requirements.

Flexible Data Ingestion, Quick Scaling

Expo 2020 Dubai is expected to generate approximately one terabyte of data every day across a vast environment that includes over 8,000 access points, more than 100 security devices and multiple clouds.

With such a diverse environment and high volume of data, Expo needed a data platform that was up to the task. “Splunk proved to be a SIEM technology that is flexible, efficient and effective enough to handle the evolving demands of Expo’s cybersecurity environment,” says Eman Al Awadhi, Expo’s vice president of cybersecurity and resilience.

Data-Driven Outcomes

100+

security devices and technology solutions secured with Splunk

One

terabyte of data ingested per day

8,000+

access points and 1,400+ servers secured with Splunk

As Splunk seamlessly ingested data from a wide variety of sources, including bespoke technology solutions dedicated to Expo operations, the platform demonstrated its ability to handle both a high volume and demanding, constantly evolving environment. In addition, Splunk enabled the team to rapidly expand the scope of monitoring within a challenging timeframe.

“Splunk’s flexibility meant that we could easily resize the deployment to accommodate Expo’s changing needs during the pandemic, especially in terms of adapting to the one-year postponement of the event.” says Al Awadhi.

Tackling the Possibility of Insider Threats

Mega-events and large-scale organizations deal with a number of security incidents on a regular basis — and insider threats have evolved into some of the most challenging risks these organizations face.

To protect its technology ecosystems from insider threats, Expo relies on real-time monitoring to identify any suspicious behavior. With the ability to flag and classify any unusual activity, the Splunk platform allows the Expo team to respond to potential threats immediately and take corrective action.



Splunk’s flexibility meant that we could easily resize the deployment to accommodate Expo’s changing needs during the pandemic, especially in terms of adapting to the one-year postponement of the event.”

— **Eman Al Awadhi**, Vice President of Cybersecurity and Resilience, Expo 2020 Dubai



Splunk proved to be a SIEM technology flexible, efficient and effective enough to handle the evolving demands of Expo’s cybersecurity environment.”

— **Eman Al Awadhi**, Vice President of Cybersecurity and Resilience, Expo 2020 Dubai

Real-Time Data for 360° Visibility

Expo’s cybersecurity posture depends on many different factors — from strategic initiatives to customized Splunk dashboards that aggregate and analyze events in real time.

With rapid, comprehensive insights into cybersecurity events, the CSOC team identifies potential disruptions and proactively applies counter-measures when possible. In addition, the ability to slice and dice data directly within the Splunk platform has empowered the cybersecurity operations team to make faster, data-driven decisions that strengthen Expo’s overall cyber resilience.

“Intelligent reporting, flexible scalability and comprehensive representation of the information that matters the most are vital when it comes to communicating with different executives, operations teams and, of course, leadership,” says Al Awadhi.

Download [Splunk for free](#) or get started with the [free cloud trial](#). Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs.



Learn more: www.splunk.com/asksales

www.splunk.com