

SOLUTION BRIEF

# Fortinet and Symantec Security Solution

## A Comprehensive Solution for Cloud App Visibility, Data Security, and Threat Protection and Response

### Executive Summary

Fortinet and Symantec have partnered to deliver an industry-leading security solution by integrating FortiSOAR and the Symantec CloudSOC platform to provide enterprises with full visibility into cloud applications, enable threat information sharing and timely detection of threats for enforcement, and contain and thwart them in their path.

### Challenge

Many security teams struggle to keep up with the pace of alerts and enforcements. Their challenges include having too many consoles to monitor, alert overload, reliance on manual processes, and a shortage of cybersecurity personnel. Adding to their challenges is an effort to extend traditional security to the cloud. Cloud accounts are often accessible directly from the internet, introducing a new threat vector. Bad actors target user accounts to gain direct access to sensitive content and infiltrate an organization. Users connecting to accounts with malware-infected devices can inadvertently infect the broader organization or cause a data breach.

### Joint Solution

Symantec and Fortinet have partnered to deliver an industry-leading solution to address these challenges. The integration of the Symantec CloudSOC and Fortinet FortiSOAR solutions enabled through the Fabric-Ready Program in the Fortinet Open Fabric Ecosystem facilitates efficient investigation of alerts, allowing security analysts to better understand, review, and manage data in the cloud and on-premises, as well as to detect and generate alerts independently via its other integrations (e.g., with security information and event management [SIEM] platforms) and use that information to enforce administrative actions within CloudSOC.

### Joint Solution Components

#### FortiSOAR

FortiSOAR is a holistic and enterprise-built security orchestration and security automation workbench that empowers security operations teams. FortiSOAR increases a team's effectiveness by increasing efficiency, allowing for response in near real time.

### Joint Solution Components

- Fortinet FortiSOAR
- Symantec CloudSOC CASB

### Joint Solution Benefits

- Monitor, govern, protect, and place policy controls on sanctioned and unsanctioned cloud accounts
- Data loss prevention (DLP) with automated data classification to prevent accidental or malicious loss of confidential data
- Harness user and entity behavior analytics (UEBA) and unparalleled threat protection for automated detection of malicious insiders, attacks, and advanced threats
- Streamlined operational efficiency through custom automated framework that pulls together all of the organization's tools
- Multimode oversight using native cloud application programming interfaces (APIs), real-time traffic processing, and input from numerous data feeds



## Symantec CloudSOC CASB

Symantec provides visibility, data security, and threat protection for today’s cloud generation of users across a wide range of sanctioned and unsanctioned apps. A range of capabilities on the CloudSOC platform delivers the full life cycle of cloud application security, including auditing of shadow IT, user behavior detection, real-time detection of intrusions and threats, protection against data loss, as well as examination and prevention of compliance violations and historical account activity for post-incident analysis.

## Joint Solution Integration

The Fortinet FortiSOAR and Symantec CloudSOC joint solution operates to mitigate threat levels and high-risk activity of a user.

### Use Case 1

FortiSOAR consumes threat information from CloudSOC via API and enforces policies within the Fortinet Security Fabric. FortiSOAR generates an alert once it detects that a user has accessed privileged files (Figure 1). FortiSOAR will consult with CloudSOC and retrieve information on this user’s threat risk.

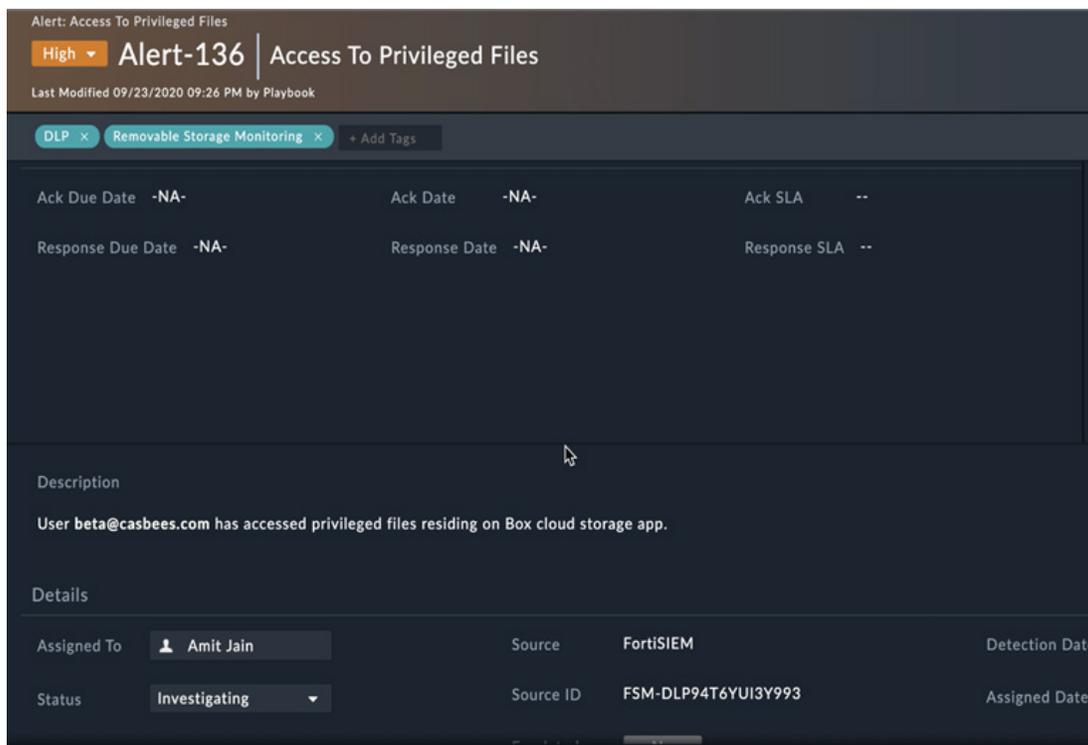


Figure 1: Alert within FortiSOAR upon a breach.

The Symantec CloudSOC UEBA solution component analyzes alerts and telemetry from diverse security sources to connect the dots between violations, users, accounts, and assets. A core data science engine uses machine learning (ML) to create individualized user behavior profiles, and in combination with threshold and sequence detectors, can identify a risk level for each user and each incident. The user risk levels and incident risk levels are aggregated into a numerical ThreatScore for easy identification of problem incidents and high-risk users. This comparative risk scoring helps to detect and identify malicious insiders and outsiders and deliver rapid prioritization of user and entity-based alerts that represent emerging risks across multiple platforms, along with categorizing those incidents tied to misaligned policies or user mistakes.



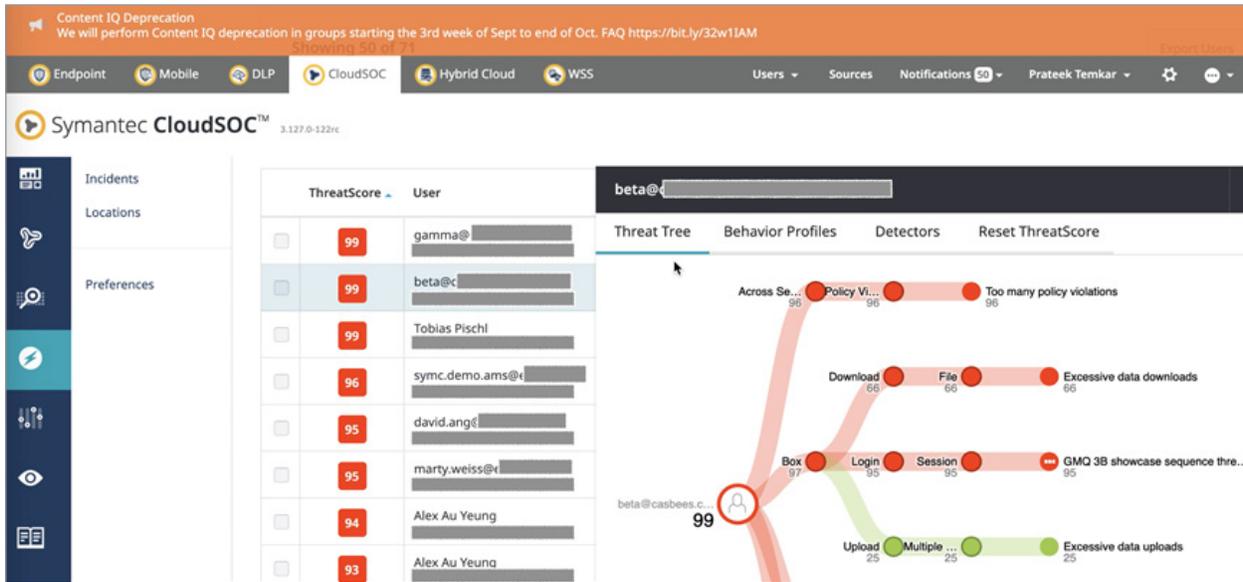
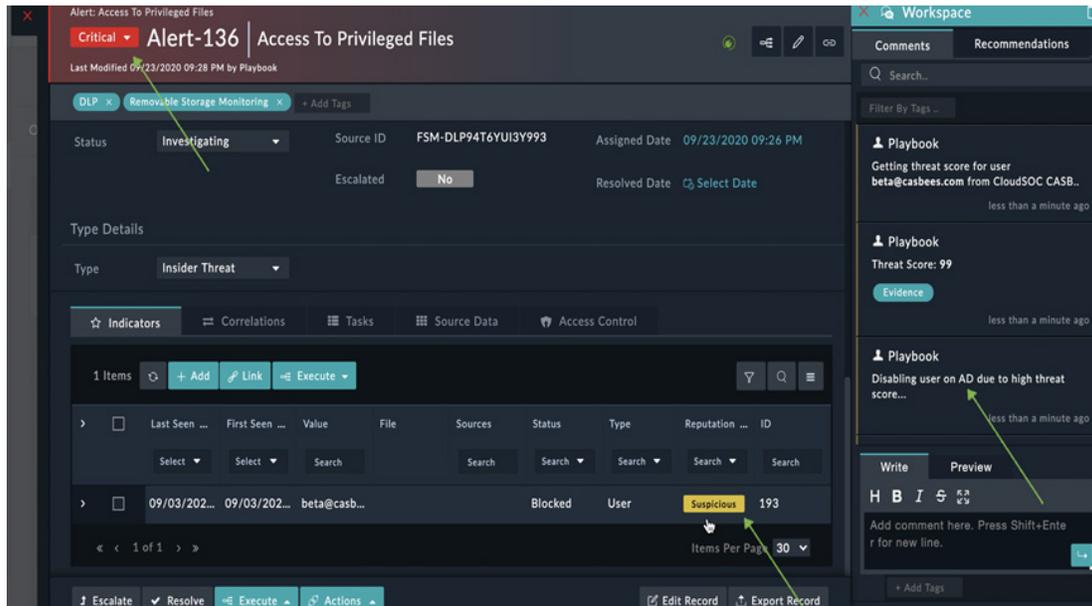


Figure 2: In this case, CloudSOC's UEBA engine has determined that this user is risky and has assigned a high "threat score" of 99 to this user.

FortiSOAR obtains this information from Symantec via its API and can enforce three actions within its platform:

1. FortiSOAR can mark the user as suspicious.
2. It can disable the risky user in AD.
3. It can raise the level of the alert to "critical."



## Use Case 2

The FortiSOAR-CloudSOC API integration can also be leveraged to enforce administrative action within CloudSOC. In a data leakage incident, FortiSOAR generates an alert (Figure 3) and notifies the admin to approve the deactivation of the user in CloudSOC (Figure 4).

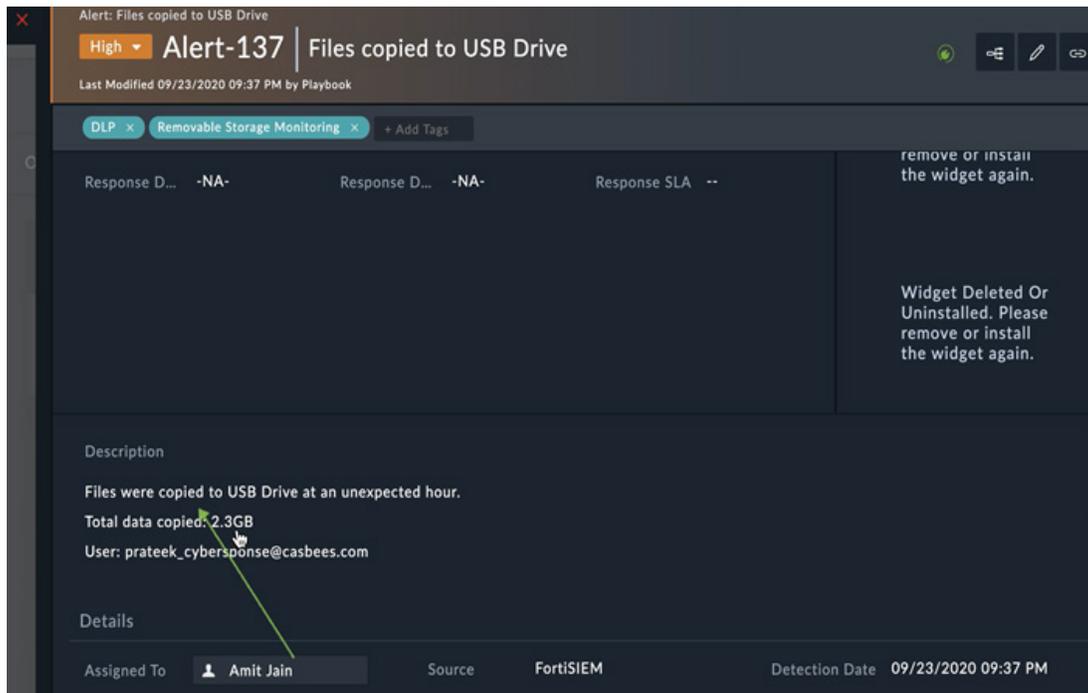


Figure 3: Alert generated by FortiSOAR upon detection of data breach and leakage.

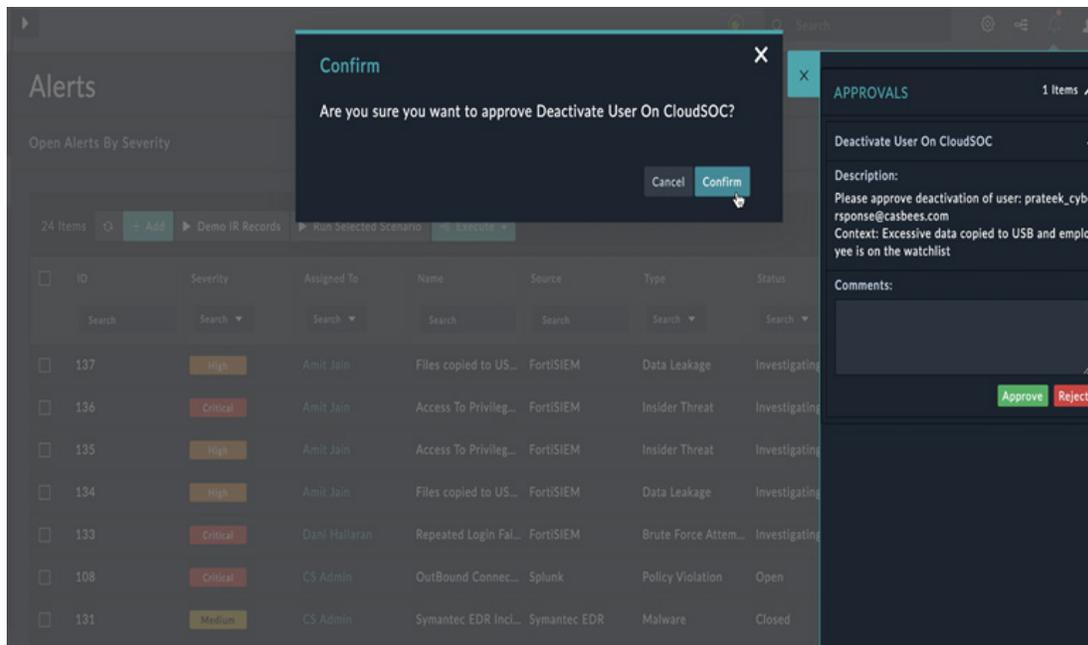


Figure 4: FortiSOAR will notify the admin to approve the deactivation of the user in CloudSOC.



Once approved, the user will be deactivated in CloudSOC (Figure 5).

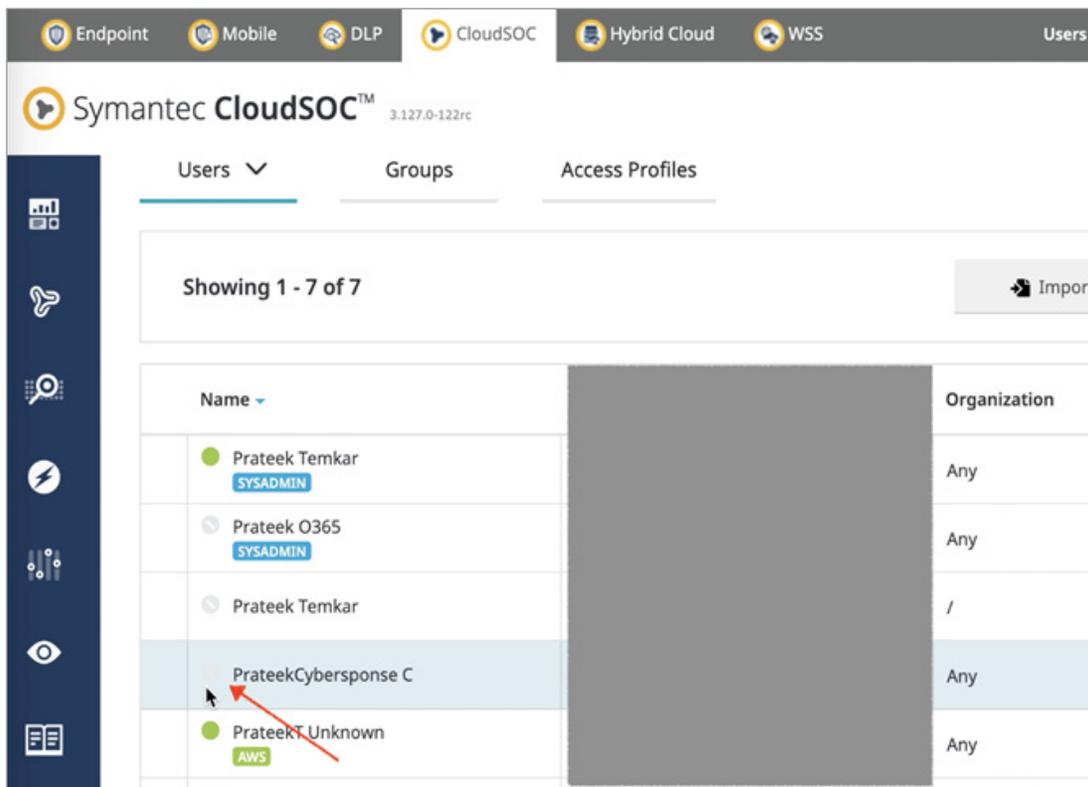


Figure 5: Deactivation of user through the CloudSOC console.

## Summary

While the expansion into the cloud has many benefits, security and data privacy professionals are being challenged to provide security and governance for cloud applications. The Symantec and Fortinet partnership extends the traditional security functions to protect sensitive data that is prevalent in the cloud environment. The combination of the Symantec CloudSOC with Fortinet FortiSOAR accomplishes this through visibility, data security, and threat protection for cloud users across a wide range of sanctioned and unsanctioned apps, resulting in faster responses and streamlined containment for reduced mitigation times.

## About Broadcom

Broadcom Inc. (NASDAQ: AVGO) is a global technology leader that designs, develops, and supplies a broad range of semiconductors and infrastructure software solutions. Broadcom’s category-leading product portfolio serves critical markets including data center, networking, enterprise software, broadband, wireless, storage, and industrial. Our solutions include data center networking and storage, enterprise, mainframe, and cybersecurity software focused on automation, monitoring and security, smartphone components, telecoms, and factory automation. For more information, go to [www.broadcom.com](http://www.broadcom.com).

