SOLUTION BRIEF

# Fortinet and Rubrik Security Solution

## Unified event correlation and risk management for cloud data management solutions

### Challenges/Business Drivers

**Organizations are moving away from legacy data protection applications that are complex, difficult to manage, and costly to maintain and scale. Companies need solutions that provide simplicity, instant recovery and immutability from ransomware, enabling users to recover quickly and to integrate the advantages of public and private clouds into IT architectures.**

While significant change is occurring in data protection solutions, preventing potential security breaches – detecting incidents that would otherwise remain undetected and streamlining compliance reporting – remains critical for every organization. To solve this challenge, Fortinet and Rubrik have worked together to integrate Fortinet FortiSIEM with Rubrik Cloud Data Management.

### Joint Solution

The integration of Fortinet FortiSIEM with Rubrik enables customers to benefit from the simplicity and cost savings from Rubrik's data management solution, while providing system-level information into FortiSIEM for logging, analysis and compliance reporting. The integration provides distributed real-time event correlation, user and entity behavior analysis, out-of-the-box compliance reporting, and cross correlation of SOC and NOC analytics to provide fast mitigation and recovery from issues.

Rubrik forwards system level information about anomalies and events to FortiSIEM for centralized logging, analysis and retention. Once FortiSIEM discovers an incident, it will alert the operator and a deeper inspection can be undertaken. Should a file or virtual machine need to be recovered, Rubrik can list the recovery points and times available and quickly restore to that point in time, greatly reducing the impact to the organization.

The Fortinet-Rubrik integration provides unified event correlation and risk management for cloud data management solutions, delivering unparalleled security, performance and compliance management.

### Rubrik Cloud Data Management

Rubrik's Cloud Data Management platform consolidates legacy backup and recovery infrastructure into a single software layer that scales linearly. Users can simplify and automate cloud migration through an SLA policy engine that can be configured with only a few clicks. By reducing daily management time from hours to minutes, Rubrik frees resources for key value-adding activities.

### Joint Solution Benefits

- Leverage powerful unified event correlation and risk management capabilities of FortiSIEM for rapid detection and remediation of security events, and to implement comprehensive security, performance and compliance management
- Rubrik sends anomalous events and logging information to FortiSIEM, allowing admins to manage incidents in a central location
- Rubrik and FortiSIEM joint solution provides insights on metadata aggregated between snapshots and throughout operating periods
- Rubrik FortiSIEM integration allows admins to leverage FortiSIEM's outof- the-box reporting tools

FORTINET FABRIC-READY

By indexing file metadata during each backup, Rubrik also enables anomaly and ransomware detection through Radar: the latest application on the Polaris SaaS platform. Radar detects anomalous changes in file metadata and provides an added dimension of data intelligence, minimizing the impact of ransomware and enabling users to recover faster.

## Fortinet FortiSIEM

FortiSIEM is Fortinet's Multivendor Security Incident and Events Management solution that provides visibility, correlation, automated response and remediation in a single, scalable solution. Using a Business Services view, the complexity of managing network and security operations is reduced, freeing resources, improving breach detection. Worldwide 80% of breaches go undetected because of skills shortage and event information 'noise'. FortiSIEM provides the cross correlation, applies machine learning and UEBA to improve response, to stop breaches before they occur.

The architecture enables unified data collection and analytics from diverse information sources including logs, performance metrics, SNMP Traps, security alerts and configuration changes. FortiSIEM essentially takes the analytics traditionally monitored in separate silos from — SOC and NOC — and brings that data together for a more holistic view of the security and availability of the business. Every piece of information is converted into an event which is first parsed and then fed into an event-based analytics engine for monitoring realtime searches, rules, dashboards and ad-hoc queries.

## About Rubrik

Rubrik delivers a single platform to manage and protect data in the cloud, at the edge, and on-premises. Enterprises choose Rubrik's Cloud Data Management software to simplify backup and recovery, accelerate cloud adoption, and enable automation at scale. Rubrik's run-anywhere, scale-out architecture is built to empower IT departments today and in the future, reducing total cost of ownership while enabling infrastructure flexibility for a multi-cloud world.

For more information,
visit www.rubrik.com and follow @rubrikInc on Twitter.

Copyright © 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.