TRUEFORT®

SOLUTION BRIEF

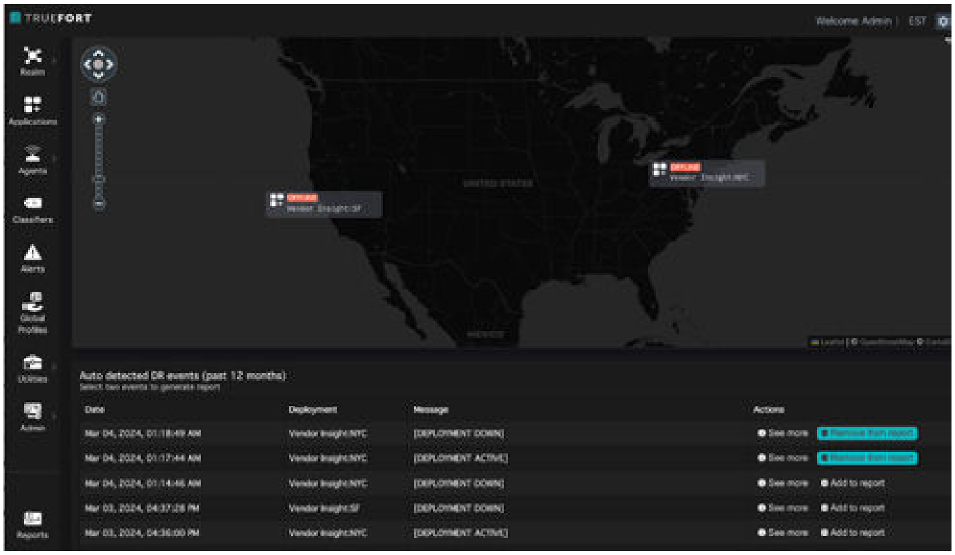
Business Continuity: Application Resilience

When organizations are essential to the economy, the resilience of their application portfolios is not just a requirement but a necessity.

Ensuring uninterrupted business operations amidst modern challenges is paramount. Financial institutions must ensure their applications' resiliency should unpreventable outages occur, through exceptional Disaster Recovery (DR) processes that satisfy regulatory requirements efficiently.

Challenges Faced by Financial Institutions:

- **Resilience of Application Portfolios:** Financial institutions must ensure their wide array of applications can withstand and thrive through failures. Regular DR simulations must be conducted to effectively demonstrate this resilience.
- **Coordinating DR Events:** Organizing DR events and gathering evidence is a labor-intensive process, plagued by non-uniform testing procedures and manual evidence collection.
- **Labor and Quality Concerns:** The manual and inconsistent nature of DR exercises leads to significant labor commitments and inconsistent evidence quality.
- **Regulatory Compliance:** There's an added challenge of maintaining auditable records of DR capabilities to meet regulatory standards.



Auto detected DR events (past 12 months)
Select two events to generate report

Date	Deployment	Message	Actions
Mar 04, 2024, 01:18:49 AM	Vendor Insight:NYC	[DEPLOYMENT DOWN]	See more · Remove from report
Mar 04, 2024, 01:17:44 AM	Vendor Insight:NYC	[DEPLOYMENT ACTIVE]	See more · Remove from report
Mar 04, 2024, 01:14:46 AM	Vendor Insight:NYC	[DEPLOYMENT DOWN]	See more · Add to report
Mar 03, 2024, 04:37:28 PM	Vendor Insight:SF	[DEPLOYMENT DOWN]	See more · Add to report
Mar 03, 2024, 04:36:00 PM	Vendor Insight:NYC	[DEPLOYMENT ACTIVE]	See more · Add to report

- **48%** of security breaches occurred at the application layer, making it the most commonly identified attack vector.
(Forrester)
- In the past year, **76%** of organizations experienced a security incident due to a lack of clear application visibility.
(Cisco)

Streamlining DR Processes:

- **Automating Evidence Collection:** By leveraging telemetry from existing tools (such as CrowdStrike and SentinelOne) combined with analytics, the process of collecting evidence from DR events can be significantly automated.
- **Efficiency and Reduction in Manual Effort:** This approach ensures minimal time to value with an estimated 80% reduction in manual efforts.
- **Uniform and Customizable Evidence:** Standardizing evidence collection processes for each application helps minimize errors and ensures uniformity.
- **Risk Identification and Auditability:** The system identifies dependency risks and ensures that the entire process is fully auditable and traceable with unlimited retention.
- **Enhanced Reporting:** Summary reporting and empirical evidence are provided for easy interpretation and decision-making, with auditor-friendly dashboards and clearly traceable recorded substantiation.

Benefits of an Advanced Application Resiliency Approach:

- **Comprehensive Application Visibility:** By identifying and cataloging all workloads, including legacy systems, the approach offers complete visibility over each application's behavior.
- **Application Behavioral Mapping:** Detailed profiling of normal application behavior aids in comparing failover operations to normal operations.
- **Dependency Mapping and Risk Identification:** Understanding interconnections among applications helps identify even the slightest risk to optimal operations in a disaster.

Partnership with Existing Security Systems:

- **EDR Integration:** Integration with existing Endpoint Detection and Response (EDR) systems like SentinelOne and CrowdStrike Falcon simplifies deployment and automation.
- **Insight into OT/IoT Devices:** TrueFort's collaboration with Armis ensures in-depth visibility into OT/IoT devices and their relationships to any enterprise applications.
- **Comprehensive Risk Posture:** This comprehensive approach ensures quick identification and mitigation of risks, fortifying the institution's continuity.

For financial institutions, application resilience is not just about business continuity; it's a strategic imperative in the face of evolving cybersecurity threats and regulatory pressures. By adopting a streamlined, automated, and application-focused approach, these institutions can ensure their operations are resilient, secure, and compliant, ready to face the challenges of tomorrow.

ABOUT TRUEFORT

TrueFort® Platform puts you in control of your applications and lateral movement across the data center and cloud, protecting service accounts and against zero-day threats. The TrueFort Cloud extends protection beyond network activity by shutting down the abuse of service accounts. Founded by former IT executives from Bank of America and Goldman Sachs, leading global enterprises trust TrueFort to deliver unmatched application environment discovery and microsegmentation for accounts and activity.

For more information on how TrueFort can enhance your manufacturing cybersecurity posture, please contact us for a detailed demonstration.

TRUEFORT®

3 West 18th Street
Weehawken, NJ, 07086
United States of America

+1 201 766 2023
sales@truefort.com