Runecast

WHITEPAPER

# AUTOMATING BANKING, FINANCIAL SERVICES, AND INSURANCE (BFSI) SECURITY: PROTECTING CRITICAL WORKLOADS AND SENSITIVE DATA

## OVERVIEW

The banking, financial services, and insurance (BFSI) sector is a highly competitive industry requiring organisations to rapidly adapt and meet changing technological demands to provide a consistent experience across regions and channels. Sensitive data storage necessitates the highest standards for digital security compliance, to maintain control of customer and financial data.

Unstructured data has created the need for privacy regulations such as DORA, GDPR, ISO 27001, NIST and PCI DSS, and greater workload transparency is required before effective processes can be established and implemented. Data breaches, compliance violations, and business interruptions threaten BFSI organizational integrity, business continuity, customer retention and can also result in long term reputational and financial losses.

> "Security and risk management leaders continue to be asked to do more with less — facing more demand for service, fast-changing threat landscapes and insufficient technical talent."
>
> – Gartner, Predicts 2022: Consolidated Security Platforms Are the Future, 1 December 2021

Regulations and compliance are a colossal challenge, with technology solutions that tend to be scattered across legacy platforms and new applications, with too many systems that barely integrate. Systems are only as good as the technicians behind them, and skill gaps naturally evolve with new technological capabilities. Solutions with little or no learning curve are in high demand, as IT security and operations teams are frequently overwhelmed, reactive at best, and inefficient, unable to work proactively on business-growth drivers.

As in many other sectors, BFSI organizations are running their workloads in highly distributed environments with a combination of different tech stacks online and in air-gapped sites. This not only increases the risk of blind spots but also turns the effort of keeping environments up to date with the latest standards and best practices into a time-consuming and cost-prohibitive task without the aid of automated processes.

Over the course of the first two years of the pandemic, an opportunity presented itself to threat actors to take advantage of a lack of administrators in datacentres, and with a shift from office to remote work, organizations' attack surfaces grew and greater risks emerged from criminal cyber activity, including malware, fraud and phishing attacks.

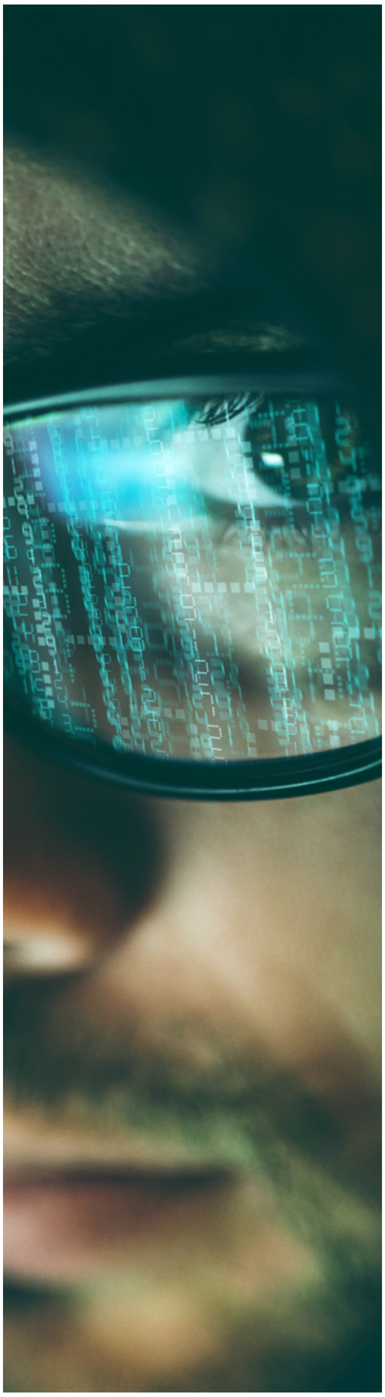
- “Three-quarters (74%) of banks and insurers experienced rise in cyber-crime since the pandemic began.
- IT security, cyber-crime, fraud, or risk department budgets had been cut by almost a third (26%) in the past 12 months.
- This mirrors the criminal activity detected by financial institutions that had risen by (29%) since the start of the pandemic.
- 42% of FIs said that the remote working model due to COVID-19 makes them less secure.”

Ref: businesswire.com

## ATTACK SCENARIOS AND RISKS

The BFSI sector faces a wide range of cybersecurity threats due to the sensitive nature of the information and assets they handle. Some typical attack scenarios and risks for the BFSI sector include:

- **Phishing attacks:** Attackers send fake emails or messages that appear to be from a trusted source, such as a bank or financial institution, to trick users into disclosing their login credentials or other sensitive information.
- **Malware attacks:** Attackers use malware, such as viruses, worms, and Trojans, to infiltrate and compromise banking systems, steal data, or disrupt operations.
- **DDoS attacks:** Distributed denial of service (DDoS) attacks overwhelm banking systems with traffic, causing them to crash or become unavailable, resulting in significant downtime and financial losses.
- **Insider threats:** Employees or insiders with access to confidential information may intentionally or unintentionally misuse or disclose sensitive data, resulting in loss or theft of critical information.
- **Ransomware attacks:** Attackers use ransomware to encrypt sensitive data or systems, demanding payment for their release, which can result in significant financial losses and loss of reputation.
- **Social engineering attacks:** Attackers use social engineering techniques, such as pretexting or baiting, to gain access to confidential information or systems.
- **Third-party risk:** Third-party vendors and service providers who have access to sensitive information or systems may become targets for cybercriminals or inadvertently cause a data breach. Financial organizations must ensure these vendors and contractors are adhering to security and compliance standards.



The BFSI sector must remain vigilant in protecting against cyber threats, employing robust security measures, conducting continuous risk assessments, and training employees to recognize and respond to potential attacks.

## CHALLENGES

IT administrators in the BFSI sector face a range of challenges due to the highly regulated and sensitive nature of the industry. Some of the main challenges include:

- **Security threats:** With the increasing prevalence of cyber threats, IT administrators in the BFSI sector need to implement robust security measures such as regular security assessment, patch management, and proactive remediation to protect sensitive data from unauthorized access, data breaches, and cyberattacks.

- **Compliance requirements:** The BFSI sector is highly regulated, and IT administrators need to ensure compliance with various regulations such as GDPR, PCI DSS, and ISO 27001. Failure to comply with these regulations can result in significant penalties and legal consequences, especially if customer data is not secured.

- **Legacy systems:** Many BFSI organizations still use legacy systems that are outdated and difficult to maintain. IT administrators need to find ways to modernize these systems while ensuring data integrity, security and business continuity.

- **Data management:** The BFSI sector generates a vast amount of data, and IT administrators need to manage this data efficiently to ensure data accuracy, availability, and confidentiality.

- **Cost management:** IT administrators in the BFSI sector need to balance the need for robust technology solutions with cost management. This requires careful planning and budgeting to ensure that technology investments align with business goals.

Reactive teams are ineffective at preventing issues and cost organizations in time, security audits and downtime. IT administrators in the BFSI sector need to be proactive in addressing these challenges and implementing solutions that support the organization's strategic objectives while maintaining compliance, data security, and cost-effectiveness.

# PROACTIVE PROTECTION OF BFSI MISSION-CRITICAL ASSETS WITH RUNECAST

To help BFSI institutions, the Runecast platform automates best practice, vulnerability and security compliance assessment across AWS, Azure, GCP, VMware, and Kubernetes domains. This ensures that no matter where your data is stored, or your environment is deployed, complete visibility is garnered throughout individual or dispersed environments. Runecast enables you to find, identify and propose solutions to known issues in your workloads before they can cause any outage in these mission-critical environments.

One of the major concerns for any organization is the lack of visibility of its endpoints, and consequently, the existence of blind spots and security gaps. The first step to protecting your environment is acknowledging the fact that it is not feasible to safeguard 100% from cyber-attacks. Pragmatically, what organizations can do is adopt a single-source solution that bridges the gap between IT Operations and Security to join the efforts to prevent these attacks from happening in the first place.

Runecast uses an AI-powered automation system to provide proactive, predictive, and prescriptive insights for organizations to holistically protect their infrastructure from cyber threats.

Automated compliance checks provide insights into exploitable vulnerabilities and regulatory security compliance, such as DORA, GDPR, ISO 27001, NIST and PCI DSS, ensuring BFSI organisations can not only gain complete visibility into their posture management, but also maintain audit readiness for regulatory compliance year-round, ensuring data breaches and possible fines are negated.

Whilst regulatory compliance is a must, corporate governance also plays a major role in everyday security requirements. By utilising the custom profiles in the Runecast platform, BFSI organizations can leverage Runecast to ensure regulatory and corporate compliance.

“We needed to ensure as a bank, being risk-averse, that our systems were compliant both from a regulatory point of view and by our own corporate governance. We were often managing this with multiple tools, which took time and effort that was in short supply, which led us to manage those demands only reactively.”

Ref: Mr. Avni. Near East Bank
https://www.runecast.com/case-studies/near-east-bank

## AUDIT READINESS, ALL THE TIME

Following the list of Runecast-detected issues and potential vulnerabilities as a Priority To-Do List will help to ensure security compliance. Runecast gives you the added ability to customize PCI-DSS criteria based on your enterprise-specific security requirements. Centered on the precise needs of your enterprise or industry you can:

- Set the maximum amount of time before automatically disabling local and remote shell access (in seconds). Default value: 900.
- Specify the password complexity policy.
- Specify NTP servers for time synchronization. Multiple servers are supported and must be separated with a comma. Default value: at least one NTP server.
- Set up the maximum vpxuser password age before automatic renewal (in days). Default value: 60
- Specify remote host to output logs. Multiple hosts are supported and must be separated with a comma. Default value: at least one Syslog server.

Editable PCI-DSS will help you to keep your data centre audit-ready all the time, to help you comply with industry standards as well as a company's unique internal security policies.

## RUNECAST ENABLES BFSI ORGANIZATIONS TO:

- **Obtain a real-time automated analysis** of VMware, AWS, Azure, Google Cloud, Operating Systems – Windows and Linux – and Kubernetes environments.

- **Choose** between **agentless or agent-based** analysis for on-prem and cloud environments.

- **Get unified visibility** and **consistent reporting** for vulnerability assessment, compliance checks, and IT Operations Management in a single platform.

- Conduct **continuous automated security auditing** and inspection of all environment assets for key frameworks in the BFSI sector such as DORA, GDPR, ISO 27001, NIST and PCI DSS.

- **Effectively assess vulnerabilities** based on severity and impact scoring from CISA's CVE and KEV identification. It also evaluates specific criteria related to the use case to accurately determine the validity of reported vulnerabilities, in addition to verifying the host version and build number.

- **Save time and budget** in employee training thanks to its intuitive user interface.

- **Ensure** that patient **data is secure and protected**, with all data processing done locally on the appliance.

- Analyze their systems **even in air-gapped environments** to minimize the risk of exposing infrastructure data to the public network.

- **Detect configuration drift** over time that can lead to security breaches.

- Speed time to resolution by providing detailed **remediation information** and **tailored scripts.**

Runecast combines vulnerability assessment with continuous analysis of the environment against security hardening guides and security compliance standards providing organizations with a solution that allows for the protection of mission-critical workloads while reducing operational overhead, potential attack surfaces, and speeding up the performance of security and operations teams

## OUR CUSTOMERS REPORT IMMEDIATE ROI

CISOs, CIOs, Security, and Ops Teams are benefiting from Runecast Intelligence

- 100% security audits passed successfully
- 75-90% time savings on vulnerability management and troubleshooting
- Up to 100% service uptime
- Increased operational efficiency and observability
- Ability to more efficiently utilize current staff
- Customizable reporting options demonstrate compliance
- Time freed up to deliver more value from IT ops

Most prominent customers in the BFSI industry:
**de Volksbank, Laboral Kutxa & The Near East Group.**

## USE CASE: TOP DUTCH BANK

### Overview

A top independent Dutch bank holding company offers four distinctive brands that are close to their customers and share a mission of banking with a human touch. Focused on the Dutch market, they offer transparent mortgage, savings and payment products to private individuals. The bank also offers insurance, investment and lending services through its brands and serves small and medium-sized businesses in a retail manner.

### Challenge

The IT team manages systems used by millions of customers across the Netherlands. Their virtualization platform is VMware-based with 2000+ virtual machines on 120+ hosts and 2 vCenters. As with any IT operations, unforeseen problems did happen, putting at risk the bank's ability to deliver its world class service to customers.

*"In the majority of cases, we would find the resolutions were already known to VMware which made them entirely preventable in the first place"*

Another challenge their team faced was related to security monitoring and reporting.

*"Adjusting monitoring and reporting on the status of security hardening was really hard in vRealize Operations Manager but Runecast made this simple!"*

**Solution**

The team deployed a trial version of Runecast Analyzer and immediately found their virtual environment prone to a number of critical issues. In addition, it identified security noncompliance issues on a number of virtual machines despite all VM's being fully compliant when initially deployed to production. None of these issues were easily identified by VMware vRealize Suite and the bank's commitment to privacy and security meant use of VMware Skyline was unacceptable.

As they stated, "Skyline is an online, cloud-based solution. As a bank, uploading and sharing environment information over a cloud-service is something we do not prefer."

## RESULTS

- Increasing uptime for their customers
- 75% time saved on troubleshooting and root cause analysis
- The ability to identify and monitor potential risks
- The ability to mitigate risks in a controlled and non-service affecting manner.
- Runecast Analyzer saves the bank's IT team 75% of time previously spent on troubleshooting and identifying root causes of issues. The tedious manual approach of crawling through VMware Knowledge Base articles has been replaced with proactive automated problem prevention.

## SUMMARY

IT administrators in the BFSI sector face multiple challenges, including cyber threats, regulatory compliance, outdated legacy systems, efficient data management, and cost management. It is crucial for them to implement robust security measures, ensure compliance with regulations, modernize outdated systems, manage data efficiently, and balance technology investments with cost management. Being proactive in addressing these challenges and implementing solutions that align with business goals is necessary to maintain compliance, data security, and cost-effectiveness while supporting the organization's strategic objectives.

Runecast is an enterprise platform for security compliance, operational efficiency, stability, and maximum uptime. In a single dashboard, it provides an out-of-the-box transparent view of your IT infrastructure, across your AWS, Azure, GCP, VMware, and Kubernetes estates, revealing not only configuration drift and vulnerabilities – including CVEs and VMSAs – but also vendor best practices alignment and security compliance audits and reporting.

Proving security compliance posture to customers is simple with Runecast's customizable reporting. Automated security standards for the BFSI sector include DORA, GDPR, ISO 27001, NIST and PCI DSS, vendor guidelines and more. Taking security a step further, Runecast works securely on-premises and in air-gapped environments –no data needs to leave your organization.

**Improved security and compliance posture**

- Risk-based vulnerability assessment
- Checks against over 13 security compliance standards
- Automatic update checks for security patches, bug fixes, and new feature releases

**Fast remediation**

- Detailed remediation steps based on recommendations from VMware, cloud providers, and industry best practices
- Custom-tailored scripts

**Increased staff productivity**

- Centralized dashboard for IT Operations and Security Management
- Intuitive user interface
- Easy reporting

**Enhanced system stability and performance**

- Configuration drift management
- Best practice analysis
- Real-time log analysis
- Upgrade simulation and hardware compatibility checks

**Learn more**

For more information please visit runecast.com or try Runecast on your environment by requesting an online demo at runecast.com/runecast-analyzer-online-demo.

Runecast

Gartner COOL VENDOR 2020

High Performer WINTER 2023

Best Support WINTER 2023

When your organization increases the complexity of its IT architecture and your workload spans across multiple systems and technologies, reducing complexity, lower operational overhead, and having full visibility of your environment becomes a critical burden to address.

To achieve unified issue visibility and reporting, organizations need to adopt a single platform that connects all disparate infrastructure technologies, from bare metal and hypervisor technologies to cloud service providers and containerized workloads.

Runecast brings organizations an integrated approach to security and compliance by tracking the exposure risk, compliance status, and environmental health via a single and automated platform.

For more information please visit runecast.com

## Runecast Solutions Ltd.

124 City Road,
London, EC1V 2NX
United Kingdom

## Runecast Solutions Inc.

300 Delaware Ave
Suite 210, Box #241
Wilmington, DE 19801
USA