ManageEngine
Log360

Strengthening financial cyber resilience and fraud detection with Log360

Table of contents

The current threat landscape in BFSI

The BFSI sector is experiencing a sustained escalation in fraud and cyberthreats. This is evidenced by the 2025 State of Fraud Report Survey which revealed that 60% of financial institutions and FinTechs reported an increase in fraud across consumer and business accounts over the past year. Enterprise banks are particularly affected, with nearly 70% reporting a rise in fraud, emphasizing their value and attractiveness to threat actors.

This growth is closely linked to digital transformation, as 80% of fraud events now occur through online or mobile banking channels, the same survey found. The expansion of mobile banking, digital wallets, online payments, and app-based lending has significantly broadened the digital footprint of financial institutions, increasing exposure to fraud, phishing, identity theft, and data breaches.

The same report mentioned that the most common fraud types were found to be credit card fraud, account takeover, and identity theft. Behavior and identity inconsistencies have become the leading indicators of attempted fraud, illustrating the shift toward credential abuse, compromised identities, and sophisticated social engineering tactics. The financial impact is severe: 42% of enterprise banks experienced direct fraud losses exceeding $1 million, while nearly one in three financial organizations overall crossed the same threshold.

Breach prevalence further compounds the risk, with 48% of (UK) BFSI organizations experiencing a data breach. In India, 96% of organizations were targeted by ransomware, and 77% of dark web threats targeting Indian BFSI organizations focused on data and databases. Moreover, according to IBM, 53% of all breaches targeted customer personally identifiable information (PII). Such persistent data-centric attack strategies highlight the importance of protecting customer data as both a security and regulatory priority.

The same IBM report states that the average cost of a data breach in the financial industry is $5.56 million, while malicious insider attacks alone average $4.92 million per incident. Apart from the direct financial losses, such incidents also result in reputational damage, customer attrition, goodwill compensation, regulatory fines, penalties, and legal repercussions.

Financial organizations recognize the strategic need for cybersecurity in the face of such threats. A recent report highlights this trend, with 87% of financial industry leaders stating that the savings from fraud prevention investments outweigh their costs. Reflecting this outlook, the global cybersecurity market in BFSI is projected to reach $266.67 billion by 2030. This growth is fueled by rising digital banking and FinTech adoption, which continues to expand both opportunity and risk across the financial ecosystem.

To scale securely, BFSI organizations require an enterprise-grade SIEM solution that transcends basic log management. ManageEngine Log360 is a unified security analytics platform that's designed to tackle the risk of internal and external threats while simplifying the burden of global regulatory scrutiny. Log360's scalable, distributed architecture is designed to handle the massive volume of log data generated in BFSI environment without performance degradation. This distributed model ensures high-speed processing, zero-loss data integrity, and a tamper-proof audit trail.

How Log360 helps financial organizations

For financial institutions dealing with complex threat environments, Log360 provides real-time security monitoring, signature-based, rule-based, and behavior-based threat detection, dark web monitoring, and audit reporting capabilities. These capabilities enable security teams to detect fraudulent activity, monitor insider risks, identify early signs of ransomware or data exfiltration, detect external attacks, and maintain compliance visibility across regulated financial environments.

Key feature highlights

Here are the key features of Log360 that can help elevate the security posture of BFSI institutions:

Centralized log management and analysis:

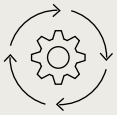
Log360 aggregates and indexes massive volumes of telemetry from more than 750 sources, including core banking systems, servers, databases, network devices, security devices, and from hybrid cloud environments, providing a single pane of glass for actionable security insights. This unified visibility eliminates data silos and helps security teams correlate events across the entire infrastructure to identify hidden attack vectors.

Advanced threat detection:

Accelerates threat detection with more than 2,000 out-of-the-box detection rules for a plethora of security use cases. Log360 utilizes an integrated threat intelligence platform and the MITRE ATT&CK® framework to identify known malicious IPs, URLs, and complex attack patterns like advanced persistent threats, lateral movement, and privilege escalation. It also identifies leaked PII, including compromised employee credentials.

User and entity behavior analytics (UEBA):

Leverages machine learning models to establish behavioral baselines for every user and entity, flagging anomalies such as impossible travel or unusual data access indicative of account takeover. Provides static and dynamic peer group analysis, seasonality, and user identity mapping features to enhance threat detection and risk scoring accuracy.



Automated incident response:

Log360 supports automated responses and executes predefined playbooks to instantly mitigate threats, such as killing a malicious process or isolating an infected workstation upon detecting ransomware activity. This helps BFSI security teams minimize the mean time to contain, ensuring that localized infections do not escalate into enterprise-wide outages.

Real-time alerts and incident investigation:

A high-speed search engine and an intuitive Incident Workbench centralizes high-fidelity alerts, enabling SOC analysts to visualize the entire attack timeline and perform root-cause analysis from a single console (without switching tools). This empowers security teams to prioritize high-risk incidents, ensuring that critical banking services remain available and secure.

Compliance management:

Log360 helps BFSI organizations monitor log activity, maintain audit trails, streamline their audit process, and avoid heavy non-compliance penalties through automated reporting and tamper-proof log archiving. It provides prebuilt, audit-ready templates for global mandates, including the PCI DSS, the GDPR, SOX, GLBA, and DPDP.

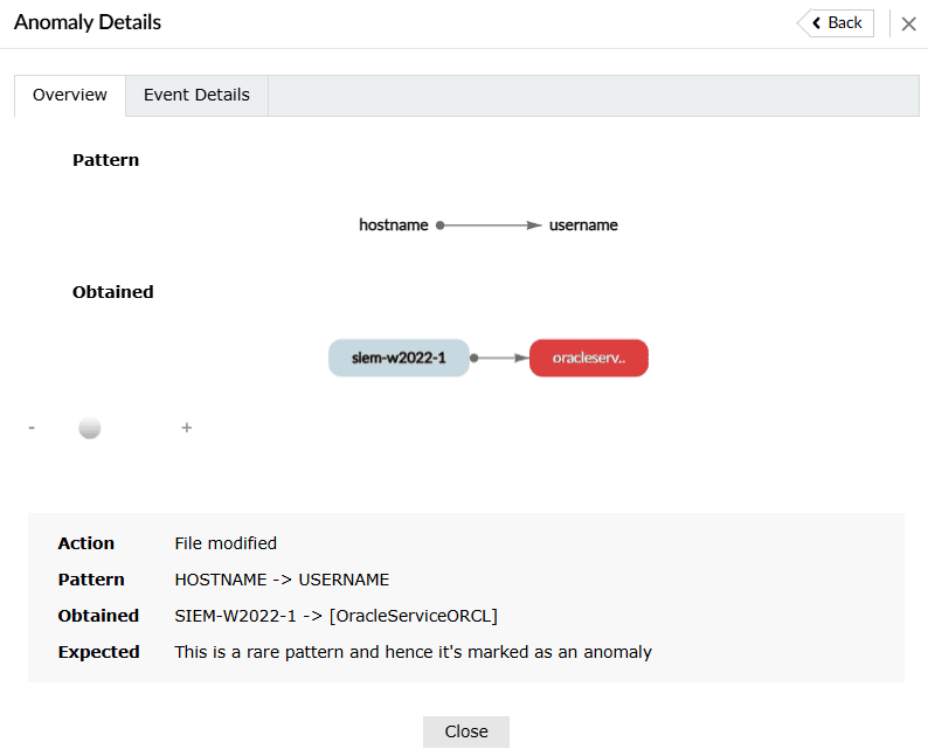
BFSI use cases

ManageEngine Log360 supports certain critical use cases for BFSI, such as:

1. Fraud monitoring

Digital banking platforms and payment systems are increasingly targeted by fraud schemes such as account takeover, and credential abuse, which traditional detection systems fail to detect.

How Log360 helps:
ManageEngine Log360 leverages UEBA to detect fraud indicators by establishing behavioral baselines for users, and identifying anomalies such as unusual login times, abnormal user activity, or access from new or multiple locations. The platform generates real-time alerts when suspicious activities, such as unauthorized data modifications or abnormal data access, are detected. Timely detection and containment of threats helps protect institutional assets and maintain customer trust.



Business outcomes

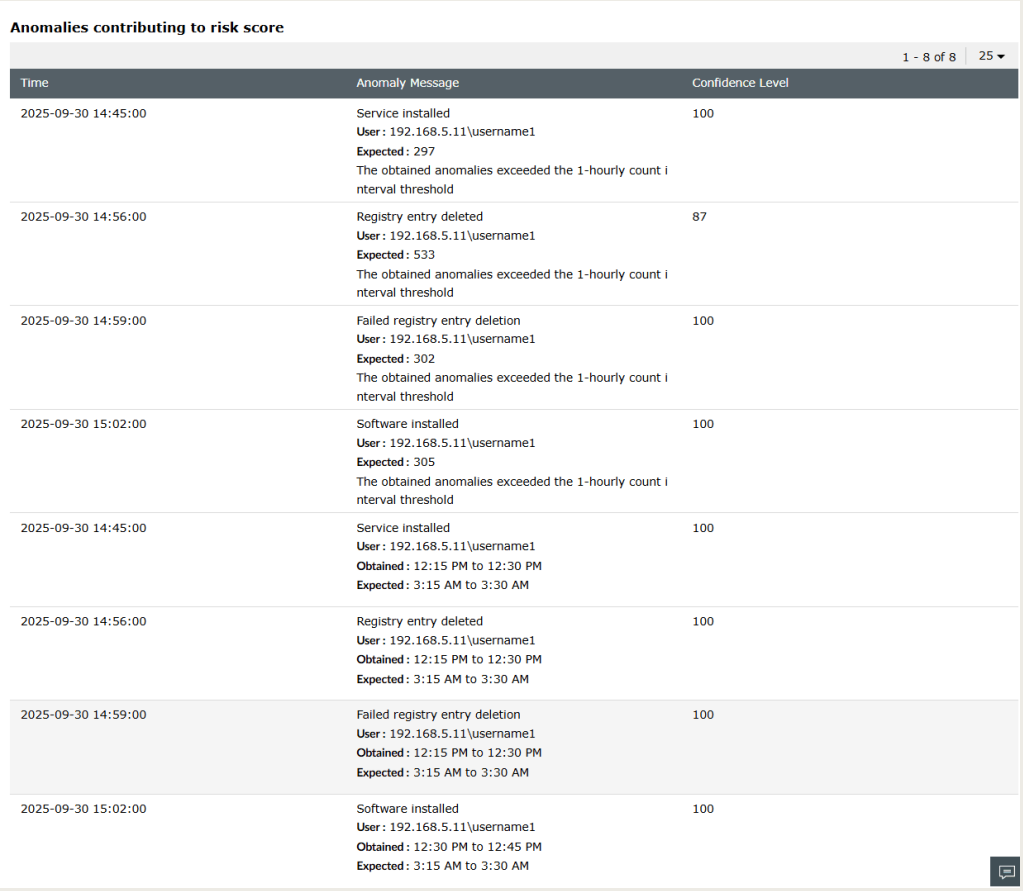
- Faster identification of fraud indicators
- Reduced financial losses from fraudulent activity
- Improved monitoring of digital banking systems

2. Insider threats

Malicious or negligent insiders can misuse privileged access to manipulate financial data, steal sensitive information, or disrupt systems.

How Log360 helps:

The solution continuously monitors privileged accounts for anomalous behavior, tracks administrative commands, and audits data access for privilege escalation attempts and unusual bulk exports. It then provides contextual intelligence using capabilities such as peer grouping and seasonality, and assigns dynamic risk scores to users to help SOC teams prioritize and neutralize critical internal threats.



Anomalies contributing to risk score

1 - 8 of 8 | 25

Time	Anomaly Message	Confidence Level
2025-09-30 14:45:00	Service installed **User :** 192.168.5.11\username1 **Expected :** 297 The obtained anomalies exceeded the 1-hourly count interval threshold	100
2025-09-30 14:56:00	Registry entry deleted **User :** 192.168.5.11\username1 **Expected :** 533 The obtained anomalies exceeded the 1-hourly count interval threshold	87
2025-09-30 14:59:00	Failed registry entry deletion **User :** 192.168.5.11\username1 **Expected :** 302 The obtained anomalies exceeded the 1-hourly count interval threshold	100
2025-09-30 15:02:00	Software installed **User :** 192.168.5.11\username1 **Expected :** 305 The obtained anomalies exceeded the 1-hourly count interval threshold	100
2025-09-30 14:45:00	Service installed **User :** 192.168.5.11\username1 **Obtained :** 12:15 PM to 12:30 PM **Expected :** 3:15 AM to 3:30 AM	100
2025-09-30 14:56:00	Registry entry deleted **User :** 192.168.5.11\username1 **Obtained :** 12:15 PM to 12:30 PM **Expected :** 3:15 AM to 3:30 AM	100
2025-09-30 14:59:00	Failed registry entry deletion **User :** 192.168.5.11\username1 **Obtained :** 12:15 PM to 12:30 PM **Expected :** 3:15 AM to 3:30 AM	100
2025-09-30 15:02:00	Software installed **User :** 192.168.5.11\username1 **Obtained :** 12:30 PM to 12:45 PM **Expected :** 3:15 AM to 3:30 AM	100

Business outcomes

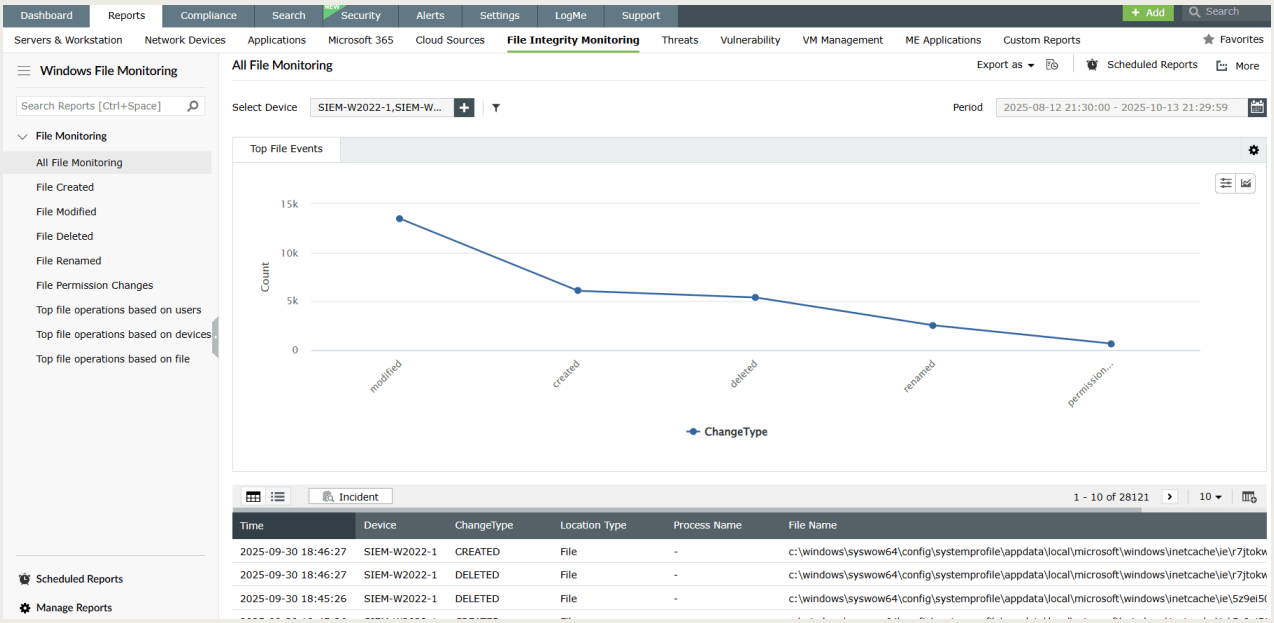
- Early detection of insider misuse or compromised accounts
- Improved monitoring of privileged access activities
- Reduced risk of internal data compromise

3. Data theft

Financial institutions manage large volumes of sensitive customer and transaction data, making them prime targets for data exfiltration and breaches.

How Log360 helps:

Log360 utilizes its integrated DLP and CASB capabilities to monitor file activity, database queries, and cloud access logs and identify suspicious data access or exfiltration attempts. It leverages its file integrity monitoring capabilities to track who accessed, modified, or moved sensitive customer PII in real time. It also provides visibility into data movements within hybrid environments like Microsoft 365, AWS, and Salesforce.



Business outcomes

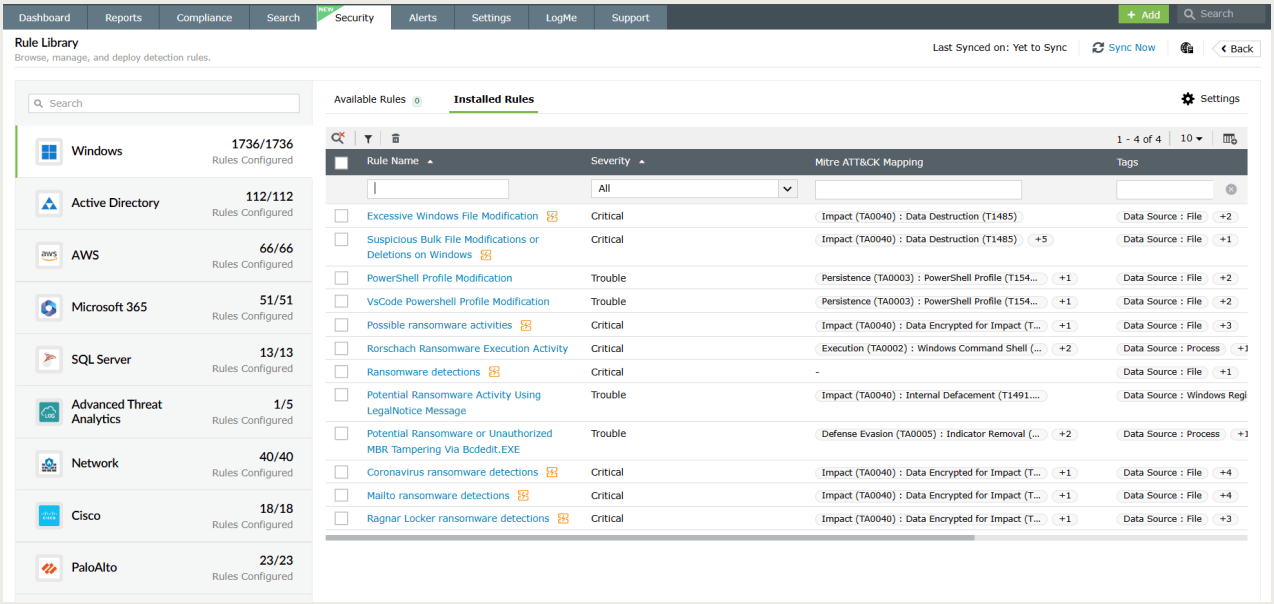
- Early detection of data exfiltration attempts
- Improved visibility into data access across hybrid environments
- Stronger protection of customer financial and personal data

4. Ransomware

Ransomware attacks can disrupt financial services operations by encrypting critical systems and data, and once encryption begins, the window for containment is extremely low.

How Log360 helps:

The solution monitors for mass file renaming, modifications, or deletions that exceed the expected thresholds, and flags sustained high CPU usage, which are the primary indicators of active encryption. It can trigger automated SOAR workflows to isolate infected machines and shut down malicious processes instantly. Even after encryption, it can help with forensic investigations.



Business outcomes

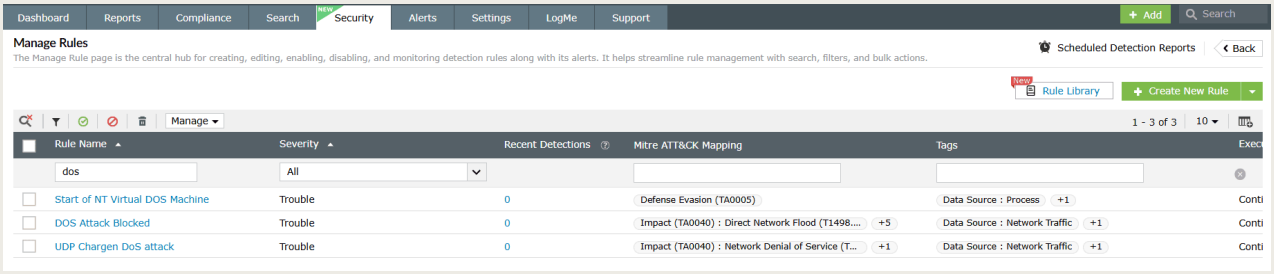
- Faster detection of ransomware activity
- Reduced operational disruption and improved resilience
- Improved incident response and containment capabilities

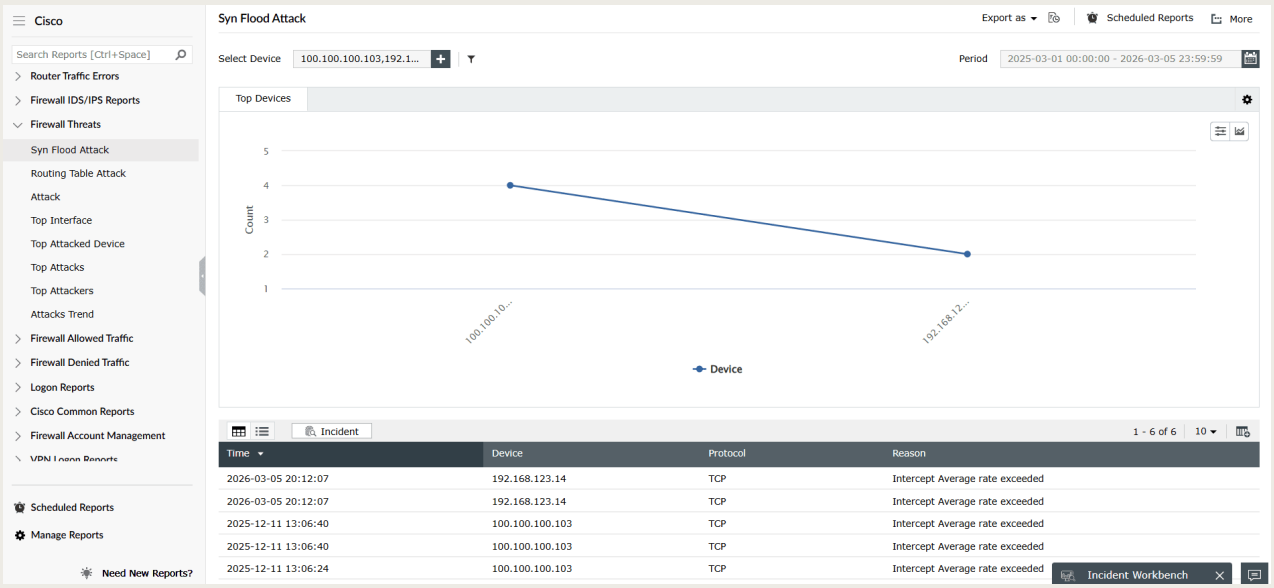
5. Distributed denial of service

The Financial Services - Information Sharing and Analysis Center reported that the financial industry is a prime target for distributed denial-of-service (DDoS) attacks. Sudden traffic surges can paralyze digital banking portals, leading to massive service disruptions.

How Log360 helps:

Log360 analyzes network, firewall, and server logs to detect abnormal traffic patterns and surges in connection requests that might indicate a potential DDoS attack. With the help of Incident Workbench, security teams can identify malicious IPs and block them by configuring inbound and outbound firewall rules directly within the platform.





Business outcomes

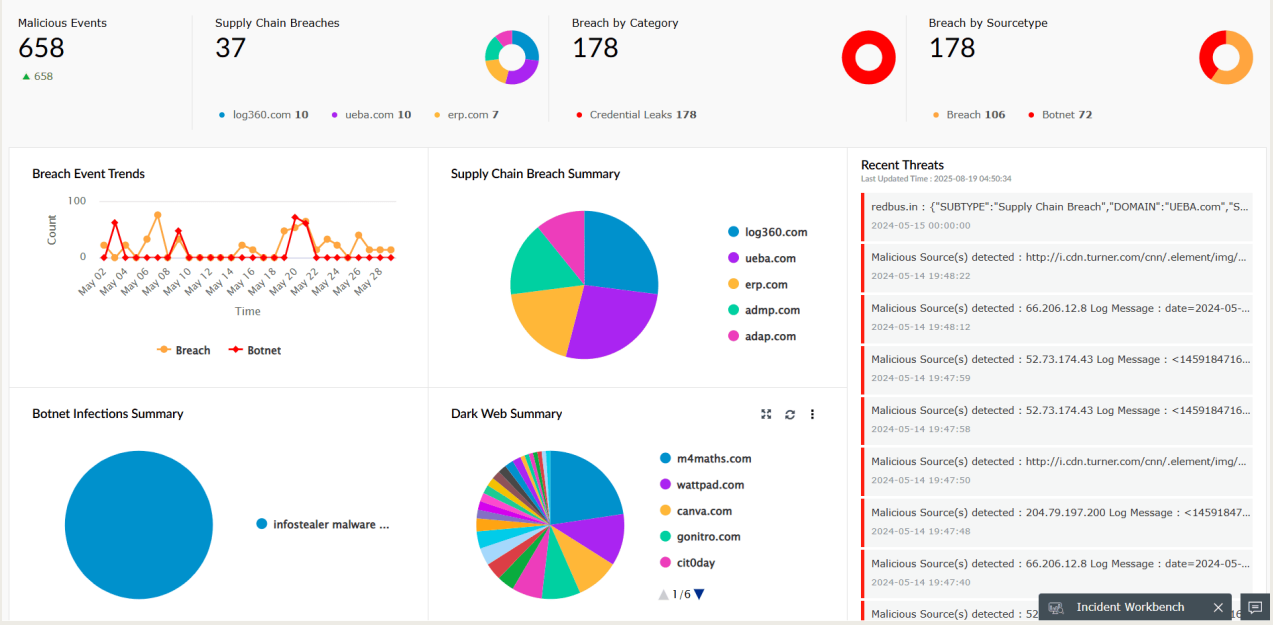
- Prevents enterprise-wide downtime
- Ensures uninterrupted access of financial services for customers
- Preserves the organization's competitive reliability

6. Dark web threats

Leaked credentials and sensitive financial data often appear on dark web forums before organizations become aware of a breach. Compromised credentials often serve as the attacker's entry point into the financial institution's network.

How Log360 helps:

Through integrations with threat intelligence providers such as Constella Intelligence, Log360 identifies leaked credentials, domain mentions, or exposed organizational data on underground forums. This enables security teams to take preventive actions such as resetting credentials or tightening access controls. It also identifies if credit card numbers or Social Security numbers associated with your organization have been exposed on the dark web.



Business outcomes

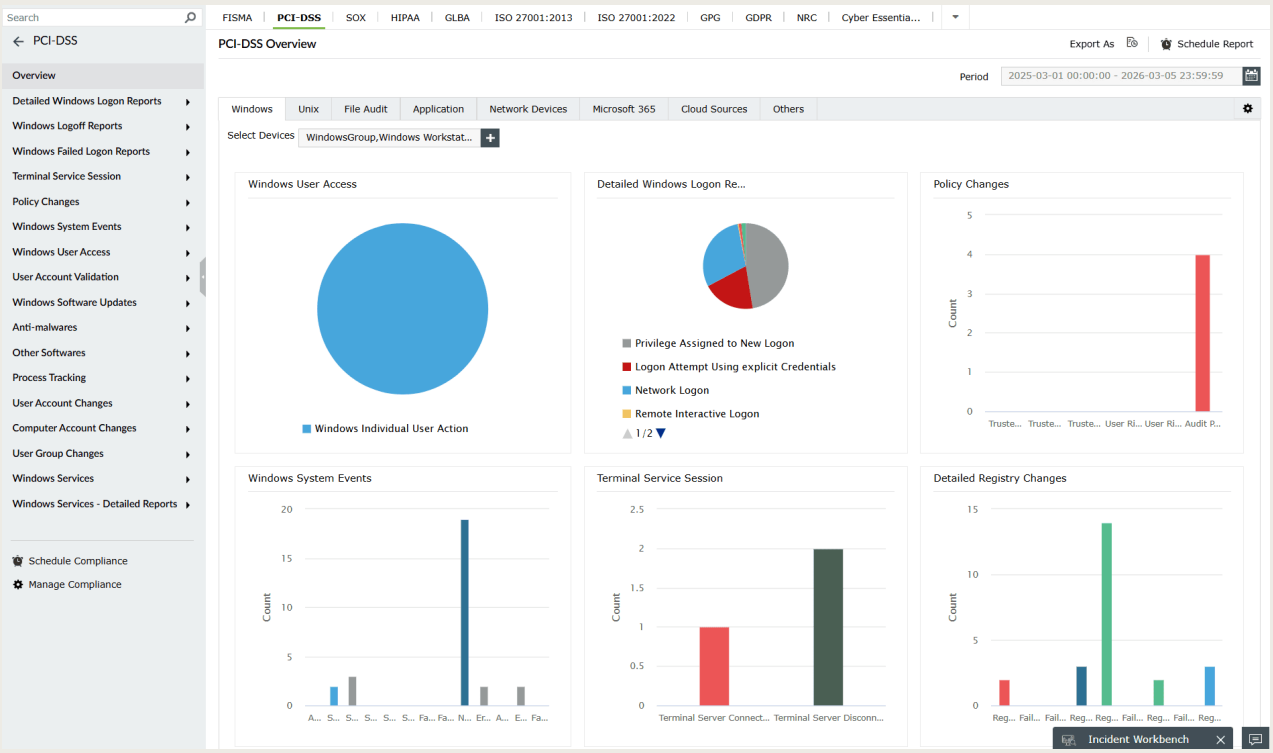
- Early detection of credential leaks and exposed data
- Reduced risk of account compromise
- Improved protection against external threats

7. Compliance complexities

BFSI organizations face some of the strictest regulatory requirements globally, and managing overlapping compliance mandates like the the PCI DSS, the GDPR, and SOX becomes challenging.

How Log360 helps:

This solution provides audit-ready templates for major regulations and automatically archives logs in an encrypted, tamper-proof format to meet long-term data retention mandates. It accomplishes that with the help of a tiered storage model: Hot storage (for real-time analytics and search functionalities), Warm storage (for historical data analysis), and Cold storage (archived for long-term retention). Log360 simplifies the audit process, and reduces reporting effort by empowering admins to automatically schedule the reports for periodic delivery.



Business outcomes

- Improved regulatory agility
- Simplified compliance monitoring and reporting
- Improved visibility into policy violations and security events

Conclusion

Cyber resilience is the fundamental pillar of business continuity and brand reputation today, and in a highly regulated environment like the BFSI industry, its importance is even greater. ManageEngine Log360 is a unified security platform that helps financial organizations move from reactive monitoring to proactive threat detection and resilience by centralizing security visibility, identifying anomalous activity, and enabling faster threat investigation and response.

About Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, an analytical Incident Workbench, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

$ Get Quote Download

Our Products

Log360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus

Exchange Reporter Plus | M365 Manager Plus