# Retail Cyber Crime

Several high-profile data breaches have hit retail organizations over the past few years, exposing millions of customers' credit card details and personal information. Some of these breaches involved malware, while others involved malicious insider activity or the use of stolen credentials. In the event of any breach, however, all of these attack vectors leave indicators and forensic evidence of the compromise in their wake. When these indicators and evidence are analyzed in real-time via machine-based analytics, initial compromises can be detected so that data breaches can be avoided.

Identifying malicious behavior indicative of an initial compromise or attempted data breach requires that the entire infrastructure involved in card processing be properly instrumented and monitored for anomalous activity. This includes everything from Point-of-sale (POS) system endpoints to the payment processor, as well as all back-office and network infrastructure. This is a critical component of detecting specific behavior indicative of an attack.

For example, when a piece of malware is installed on a POS system, it might reach out to a Command & Control server – an abnormal communication from the POS. Or the malware might initiate suspicious process activity and/or make changes to the POS's file system. Another indicator might be a user attempting to abnormally access a back-office server hosting sensitive customer data. In all of these scenarios, various log trails will contain artifacts of anomalous activity that when properly monitored and analyzed, will alert organizations that a breach is being attempted.

LogRhythm's Security Intelligence Platform not only collects log data already generated by operating systems and network devices across the credit card processing infrastructure, but can also directly monitor endpoints and networks to generate an independent, detailed forensic audit trail. All available data can then be analyzed for anomalies and malicious activity by the AI Engine, LogRhythm's patented machine analytics technology.

This Threat Insight paper describes how to properly instrument a retail organization's IT environment to achieve a complete forensic view into anomalous and malicious activity. Techniques include configuring data to be analyzed by the AI Engine in real time to detect and identify threats and compromises and avoid costly data breaches.

## POS Endpoints

### Implement Instrumentation

For the AI Engine to monitor POS endpoints for malicious activity, the proper data must be collected by LogRhythm. Specifically, we are interested in understanding details about processes that run on a POS endpoint, file system activity, and user behavior.

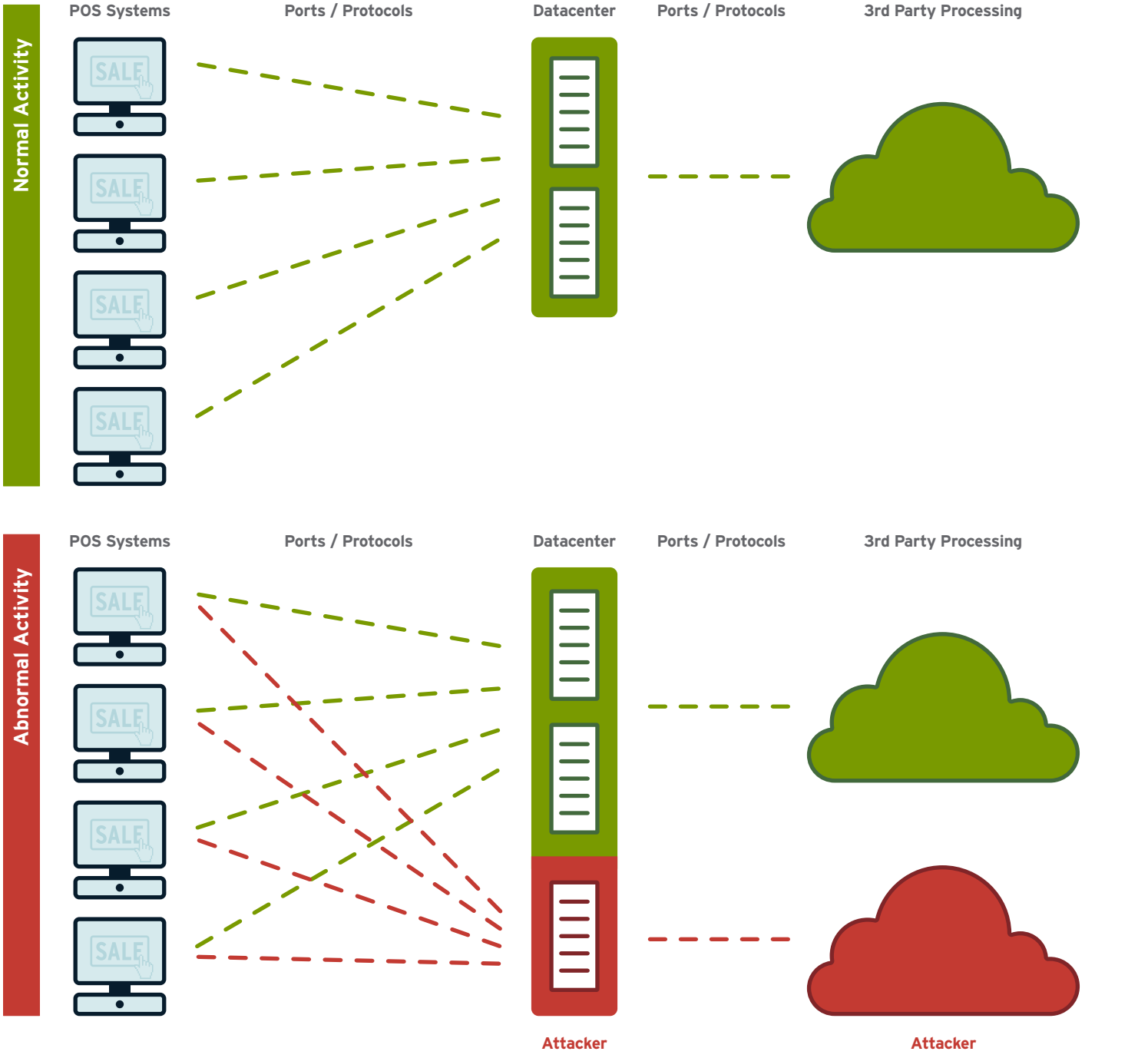
If the POS system is running an operating system that supports LogRhythm's System Monitor Agents, we recommend that one be installed to utilize its advanced endpoint monitoring features. These advanced features, including Process Monitor, Network Connection Monitor, User Activity Monitor, Data Loss Defender, and File Integrity Monitoring, deliver an independent and deeper view of system activity. Independent monitoring is critical since malware will first try to disable the native auditing system. Real-time forensic data generated by the System Monitor will be fed to AI Engine for continuous, machine-based analytics.

### Implement Security Analytics

POS endpoints are purpose-specific devices, making them excellent candidates for behavioral baselining/whitelisting, and for certain behavioral dimensions, peer trending. These activities make it easier to identify anomalous behavior that is indicative of malware or other unauthorized activity on the POS endpoint.

To accurately identify when malicious behavior is happening, certain attributes should be monitored on the endpoints. Each POS should be running the same set of processes. Their file systems should look identical to one another, and should only change during scheduled updates. Ideally, a single POS should be deployed in a known clean state and designated as the

## LOGRHYTHM ON CYBER CRIME IN A RETAIL ENVIRONMENT




**System Monitor**

- Process Monitor
- File Integrity Monitor
- User Activity Monitor

**Network Monitor**

- Ports/Protocols
- Layer 7 Applications
- Host Communications

**Analytics**

- Behavioral Whitelisting
- Anomaly Detection
- Peer Trending

"Gold Standard" system. Peer trending can then be utilized to compare all the remaining POS endpoints' processes and file systems to the Gold Standard POS. If they are not all completely identical, which is generally the case when malware is present on a system, LogRhythm will generate an alert.

In some situations attributes might vary between POS endpoints, such as the accounts used to log into each terminal, or the back-end systems with which POS terminals at different locations communicate. In scenarios like these, peer trending based on a "Gold Standard" will not be effective. However, for each individual POS, whitelisting normal behavior is an ideal approach. For example, standard AI Engine Whitelist rules can identify when a new user attempts to log in to any POS endpoint. This approach can be effective in cases where the type of POS in use across an organization is not homogenous by creating individual POS profiles of processes and file systems per endpoint, rather than the peer trending approach outlined in the previous paragraph.

In addition to monitoring process and file system activity, recognizing changes in the composition of the type of log data coming from each device can indicate malicious activity. For instance, when malware is delivered to a POS endpoint, it might generate a new type of event in the system logs that is not typically generated during normal operations. Or the malware might completely disable system or audit logging. In either scenario, an AI Engine Trend rule can profile the types of events and log data volume normally generated on a per-endpoint basis. AI Engine can then trigger an alarm when it observes a new event type.

## Back-Office Systems

### Implement Instrumentation

In many cases, an organization's POS endpoints communicate directly with third-party payment processors. However, in many situations those endpoints will also communicate with "back-office" systems that might serve a variety of purposes, particularly within larger organizations. They might aggregate transactions from multiple POS endpoints for processing, keep track of a customer's purchases for tracking by loyalty programs, allow a customer to enroll in a membership or sign up for e-mail alerts, or simply update information in an inventory tracking system. Although these back-office systems don't always process credit card data, they are generally authorized to communicate with POS endpoints, making them viable attack vectors. Other personal data may also be residing on these systems and needs to be protected along with credit card details.

LogRhythm's System Monitor, which includes Process Monitor, Network Connection Monitor, User Activity Monitor, Data Loss Defender, and File Integrity Monitoring, should be deployed to generate an independent forensics audit trail of activity on the hosts. All system and application log data should also be properly collected and analyzed.

### Implement Security Analytics

Similar to POS endpoints, back-office systems are generally purpose-built to perform very specific tasks. To help identify potentially malicious behavior on these systems, whitelisting various attributes is also a great approach.

The AI Engine Whitelist rules should be configured to monitor for changes in process, file system, and user activity. In addition, the log data should be monitored for a change in composition of log type, in a similar method that is described in the POS endpoint section of this paper.

## Network

### Implement Instrumentation

Network communications between components in the card processing chain should be tightly controlled and monitored, a process that is specifically mandated by PCI-DSS. There are a few options when it comes to monitoring network activity. The best solution for providing the most forensic detail through layer 7 is LogRhythm Network Monitor.

Although some powerful behavioral analytics can be applied to basic IP/port/protocol data provided by traditional flow sources, Network Monitor is the preferred solution due to its application identification capabilities and large set of metadata fields. The systems involved in processing credit card transactions should only be running a very small set of network protocols and Network Monitor can quickly identify unusual behavior. For example, Network Monitor can identity FTP sessions stemming from these systems, as well as data uploads to cloud-

sharing applications. Typically this type of network traffic will indicate unauthorized or malicious activity. Network Monitor can quickly identify these types of network traffic, regardless of the port used, and immediately provide the additional forensic detail required to halt the attacker.

If Network Monitor isn't an option, collecting flow data from all relevant network devices can suffice for basic end-to-end network traffic behavioral analysis. At a minimum, the goal is to generate an audit trail of all end-to-end communications happening on the network segments containing POS and back-office systems, and to identify when those communications change.

### Implement Security Analytics

Because POS and back-office systems are so specific in what they do, using LogRhythm to identify unauthorized network communications is also crucial. POS endpoints should only be engaged in specific communication, such as with back-office systems or third-party processors. Also, back-office systems should only communicate with other authorized systems. AI Engine's whitelisting functionality allows for appropriate end-to-end communications to be automatically identified and recorded. When a new type of network communication is observed, such as malware attempting to phone home or a malicious actor attempting to exfiltrate data, security personnel can be immediately notified.

LogRhythm provides an out-of-the-box Network Behavior Anomaly Detection (NBAD) module that can enhance the required whitelisting approach. This module contains a collection of AI Engine rules specifically created to analyze forensic data generated by Network Monitor. No matter how stealthy an attacker's activity might be on a host, eventually network communication will be required for data to be successfully exfiltrated. For example, additional tools are often downloaded and installed when a host is initially compromised. These tools may be used to establish remote access for the attacker or start beaconing out to a C&C server for additional instructions. Using built-in NBAD capabilities, LogRhythm can immediately identify these types of activities as abnormal and notify security administrators for rapid response.

## Conclusion

By properly instrumenting and monitoring the entire IT infrastructure involved in processing credit card transactions, administrators can identify malicious activity in the payment processing chain. The systems involved in these transactions have very specific purposes, and should be behaving in very limited and predictable ways. Whether an insider is accessing data they shouldn't be, malware is running and exfiltrating data, or a simple firewall misconfiguration is exposing a back-office server to the internet, the endpoints and/or the network's behavior will change. LogRhythm can recognize these changes of behavior as they happen, allowing retail organizations to identify and stop attacks against their payment processing chain before customer data is compromised.