

LogicMonitor
PLATFORM SECURITY WHITE PAPER



Examining the security of a
“Software as a Service” monitoring system.

LogicMonitor Platform Security

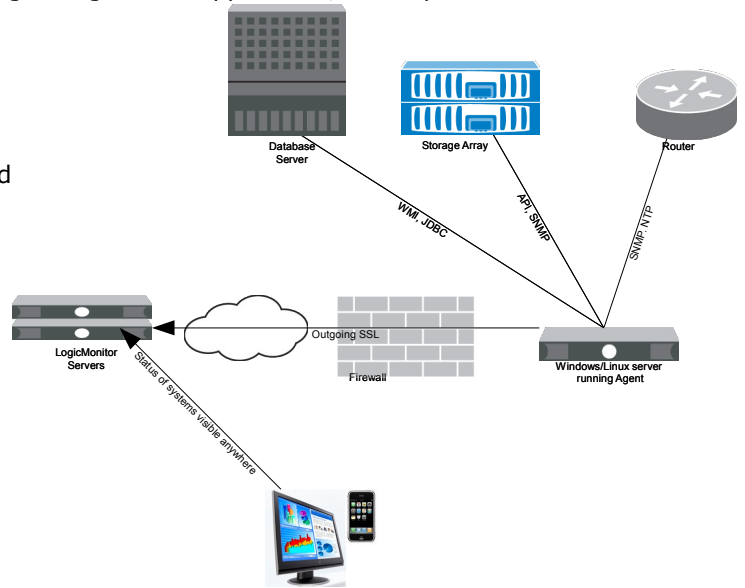
Any Software as a Service (SaaS) product raises a number of important security concerns. In this paper we show some of the measures LogicMonitor uses to protect your data.

LogicMonitor utilizes a hybrid service architecture: a small agent runs on one or more hosts on the internal enterprise network, behind the firewall. The agent is a lightweight Java application, which performs two functions:

- polling monitored devices using various data collection methods
- sending collected data via SSL to the centralized LogicMonitor servers for processing, storage, formatting, and alerting.

Is the agent secure?

The agent has been carefully developed with secure coding practices. Other than for local data collection, the agent makes only outgoing connections over SSL, and accepts no connections from the network. The agent stores no data locally, except for its own configuration sufficient for it to know with which LogicMonitor servers to authenticate. All collected data is buffered in local memory only long enough to transmit to the LogicMonitor servers.



What level of access does the agent have to the devices it monitors?

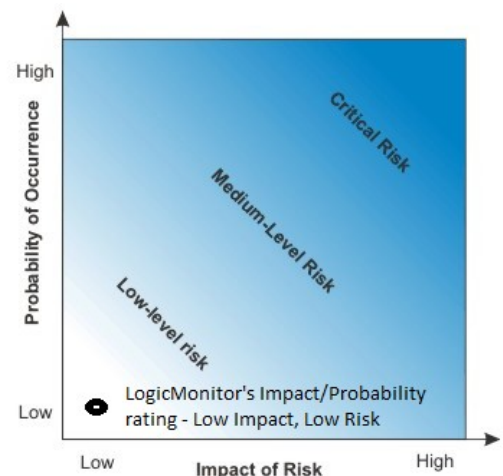
LogicMonitor's best practices dictate that the agent have no more than readonly access to any device. This is entirely within the customers control, by configuring appropriate read-only snmp community strings, creating a NetApp account with read only API access but no other rights, creating specific MySQL users that have no rights to any existing database, etc. LogicMonitor does not require write access for any of its standard monitoring, and all LogicMonitor documentation details how to create the minimum rights required.

How is data transmitted between the agent and LogicMonitor servers?

All communication between the agent and LogicMonitor servers is encrypted and protected with SSL. The agent uses certificate authentication to ensure it is talking to valid LogicMonitor servers and thwart any man-in-the-middle attacks. The agent initiates all communication to the LogicMonitor servers, as outgoing SSL connections are typically in accordance with existing customer security policy enforced by data center firewalls.

What kind of data is collected and stored?

There are two kinds of information collected and stored by the LogicMonitor servers: attributes of hosts (IP address, system type, snmp community string, etc) and performance information of hosts (CPU load, disk utilization, request latency, etc). All attribute information, even though typically not sensitive, is stored in encrypted form in LogicMonitor's systems. Performance information is even less sensitive. Compare the business significance of storing this metadata to the business critical information that is commonly stored externally with other SaaS products, such as Salesforce.com, and consider that LogicMonitor



has very similar security measures in place, and you'll see that LogicMonitor rates very well in risk Impact/Probability ratings.

Who can see the collected data?

Only your users can see your data. Administrative users can add, delete, suspend or change the access levels of other users in your account. User accounts can be defined with different privilege levels to control whether they can view or change data in the system. While there is a pre-configured account for LogicMonitor support staff, it is disabled by default. You may elect to temporarily enable that account so we can login to help you with a specific configuration issue.

How is the collected data protected while it is being stored on LogicMonitor servers?

Our servers are located in secure datacenters, with excellent security measures:

- 24 x 7 x 365 manned data centers
- 24 x 7 x 365 secured access to data centers
- Servers housed in locked cabinets
- Ingress and egress secured with electronic key cards and biometric hand scans
- 24x7x365 high resolution, motion-sensitive video surveillance
- Fully redundant power and HVAC
- VESDA Fire-threat detection and suppression

What operational procedures do you have to protect collected data?

Only LogicMonitor operations staff can log in to live servers - developers do not have access to production systems. Employees cannot access customer passwords, as they are stored only as hashes. The information of each customer is stored in a separate database, so even in the event of an application coding error, information cannot be leaked from one customer to another. There are regular external security scans of our servers. LogicMonitor regularly applies current security patches to our hardened servers, and, of course, our servers are very well monitored!

Can I trust you?

Of course, this is the fundamental question. We are interested in your success, and meeting your needs, because we wish to keep you as our customer. We have extensive experience running sophisticated datacenters, and ensuring that data is safe. Indeed, in many cases your monitoring data will be safer with LogicMonitor than with premise based systems. We hope that the above information will give you confidence that LogicMonitor Hosted Monitoring has been built with security in mind, and that it will meet your standards. After all, monitoring is all we do, and we have our entire organization built around doing it well, in a highly available manner, and securely.