Glassbeam White Paper

Machine Data Security

glassbeam™

Contents

The world is evolving in using Machine Data to better service clients, improve product quality, reduce costs in servicing clients and to drive increases in top line revenue. The increasing use of machine data generates a lot of questions. One recurring line of inquiry is around the overall security of log data, system data, and other forms of machine data.

This paper is meant primarily to provide the reader with a definition of machine data, a data classification scheme to use when considering the sensitivity of machine data, steps to help ensure data protection, and guidance pertaining to adherence to security or privacy compliance mandates. At Glassbeam, we classify all machine data as private data and we protect it in accordance with industry Best Practices, further described in our Data Security white paper.

Use of Machine Data

One of the fastest growing areas of growth in technology is leveraging machine data for trouble shooting IT issues, debugging network or programs. Today, ground breaking firms and traditional firms alike are creating new markets to build mining equipment to use Machine Data gain knowledge gleaned for the analysis of this data. Today your Electric Vehicle can be analyzed and modified to drive faster and safer. Massive earth movers extracting shale for oil production can be monitored to see part fall out and prevent down time.

Whether its medical devices or Storage arrays, machine data is being mined for intelligence and knowledge in powerful ways that were never leveraged before.
How should you approach your potential use of Machine Data as a competitive weapon? Your competitors may very well be doing it, and your clients may very well be experiencing benefits in the use of machine data. Analytics of this kind are being used by network routing companies, storage companies, medical device companies and more.

We see leadership firms packaging the knowledge derived from Machine Data into value added services that are increasing customer satisfaction, and top line revenue numbers.

Machine Data Security

As alluded to earlier, connected devices are being implemented everywhere - from factory floors to wrist wear – and the amount of data available from these devices

is growing exponentially. IDC believes that by 2020, 42% of all data being stored will be Machine Data.

Organizations are turning to data analysis of this machine data to help them understand their operations, improve their performance, and increase efficiencies. Once you understand the structure, content, and sensitivity of the data being collected, you can determine how to best protect this data and safely allow machine data, and Glassbeam, to start working for you.

Classifying Machine Data

Machine data is information created by a process or application for machine to machine use in tasks like relaying status or providing feedback. Strings or chunks of machine data are usually very small, providing one response or output per message. Examples of machine data include log data about an event that just occurred (example: a machine instruction to have an imagine devise turn on), a notification of status change, or a relay of data needed for directing another process.

These messages might come from a traditional computer, a smart device, or even a sensor directly or indirectly connected to your network. Machine data is rarely viewed by humans or used interactively.

It is important to understand the sensitivity of the information included in machine data. Using a data classification scheme allows your organization to detail the value and handling procedures of different types of data. Classification scales usually have at least three categories: public, internal, and confidential:

Public data is the least protected, because it is information that for the most part is publicly available or would not cause harm to you or your customers if it were to be displayed on someone's web site.

Private data (also commonly labeled as 'internal' data) is usually information that's important for the business to function but is not severely damaging if released. Day to day operational procedures or company directories would fall into this category.

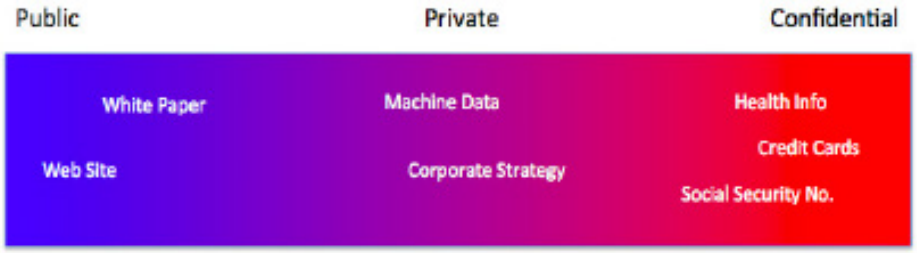
Confidential data will be the most protected data class and usually includes

corporate data such as strategy documentation, unreleased financial data, or customer's personally identifiable information such as credit card data.

Sensitive or compliance related data should not be included in machine data messages. The following examples by industry verticals are types of sensitive data that should be prohibited from inclusion:

- Storage
  - Content data
- Wireless & Networking
  - User names
  - Passwords
- Medical
  - Patient Information protected under HIPAA
- Energy Management
  - Customer information associated with device or location
  - Login data such as User name or passwords
- Retail & ATM
  - Uniquely identifiable customer data
  - Cardholder data including
    - Full track data
    - CVV Security Code
    - PIN & PIN block

Most machine data is considered benign and should be classified as private or internal data. Each piece of data carries a very limited amount of information. Data reconnaissance from individual messages will not yield a significant amount of intelligence in most cases.



Ensuring Safe Machine Data

Machine data could be raised to confidential classification if sensitive data were to be included with the message. This should not occur under normal circumstances. There are a few steps you can take to ensure that this does not happen.

Understand your data flows – At the core of information security is the assertion that you know what data you have and then make decisions on how to best protect it. You should be aware of business requirements for sensitive data; such as who must access this data, and how the data is acquired, transmitted, and stored. You should monitor how sensitive data is used or accessed internally and externally.

Baseline all devices – Under normal circumstances, machine data should not include any sensitive or confidential information. Proactively review your machine data files as part of your system implementation process to ensure that no sensitive data is being written to these files and understand the circumstances that could impact your environment where sensitive data would be written (i.e. if a system were to be put in 'debug mode').

Look for specific data – Never make the assumption that you know where all of your sensitive data resides. You can use automated or manual regular expression searches to look for unknown data. For example, you can run a REGX check for payment card data. Perform routine checks, periodic or real-time, to help validate that no sensitive data unknowingly resides on your systems.

Monitor system changes – Troubleshooting modes such as debugging may introduce sensitive data in the messages or logs. In the event that you must resort to troubleshooting modes, you should verify the resulting data from those sessions does not include sensitive data. If sensitive data is found, use a secure deletion program to remove the files securely. Glassbeam and its partners can assist you in this area. You should monitor your systems to trigger an alert whenever they are put into 'verbose' or 'debug' mode and initiate a message review process to ensure that there is no sensitive data present.

Practice good security hygiene – Data classified as Private or "Internal" shouldn't be under the same scrutiny as Confidential information, but it still requires some

handling care. Ensure that systems and networks are restricted appropriately and securely configured. Update systems with the latest security patches as often as possible.

The Importance of Machine Data

Every device is now creating some type of machine data and the volume of data being produced is increasing rapidly. This data can be any type of message created by the operating systems or applications. Messages about device status, diagnostic messages, server or application logs, location data, or network information.

Consider each small piece of machine data to be a piece of a jigsaw puzzle. Each piece tells a small part of the overall picture you are assembling. The information on each piece and its shape is incredibly important, without it you could not locate its correct location. However, any one puzzle piece will not allow you much headway to understanding what the entire puzzle looks like. Each piece of machine data does not carry the full context needed to understand its importance. Once assembled, however, they form a very important aggregation of data that can be used to create an invaluable context. Seeing the entire puzzle allows your organization to make informed decisions based on the analysis from Glassbeam.

The transmission and centralization of all of these small pieces of data is required for analysis of the information. This aggregation to assemble the machine data from random pieces into the full picture is the point where machine data (as a whole) becomes more valuable and correspondingly, more sensitive. Business decisions may be made based on the analysis of the machine data. This value is the reason for collecting the data, but also is the reason why it must now be secured.

Glassbeam uses strong encryption for both the data and the connection protocol to protect the data as it is transferred over public networks. The data also undergoes integrity checks for changes to the data patterns to ensure no tampering has occurred and to ensure that the format/structure of the received machine data matches the defined format/structure. In the event that there is a mismatch, Glassbeam rejects the incoming data and informs the customer of the issue. Once the data resides on Glassbeam's platform, a full lineup of industry standard best practices are implemented to secure your information.

Conclusion

Machine data, especially if it is generated through a common process, should not be considered sensitive. It does not inherently contain information that would be damaging or regulated. However, steps should be taken to ensure that no data is added to the machine data messages that could be considered sensitive or regulated. Once you've ascertained that your baseline machine data patterns do not contain sensitive data, you are in a position to securely transfer your data to Glassbeam and let us analyze your machine data on our secure platform to provide you valuable analyses to improve your business.

Contact us at sales@glassbeam.com

Glassbeam, Inc.
5201 Great America Parkway, Suite 360 • Santa Clara, CA 95054
Phone: 408-740-4600 • www.glassbeam.com