TANIUM

The key to regulatory compliance and sensitive data asset security is integration

Regulatory compliance and data security are possible only if you know what your data is — and where it is — at any given time.

Most regulatory acts require that owners of sensitive data must always know where the data is currently stored, what state it's in, and how well protected it is. Two primary concerns surround the importance of having this knowledge — security and compliance, and they're not the same thing.

Security

When we speak of information security, we refer to practices that protect data from being accessed, copied, stolen, corrupted, or otherwise harmed by individuals not authorized to access it. This extends to networks the data travels across and storage it rests in when not being used. Tools and techniques that increase data and network security include firewalls, intrusion prevention systems, malware filters, encryption, and more. Tanium helps users achieve a high degree of cyber hygiene using a set of habitual practices for ensuring safe handling of critical, sensitive data and for securing networks.

Compliance

We are compliant when we observe and obey rules governing the use of information and information technologies. Such compliance exists at three basic levels. First is the level of compliance with the license from the software developer and provider that limits how their software may be used. Next is governance enforced by the organization the software users work for. Most sensitive are rules and regulations instituted by the government to control use of sensitive data. This includes personally identifiable information (PII), private health information (PHI), personal or business financial records, design and development information or similar. Applicable governmental regulatory acts include HIPAA for healthcare, PSI DSS for finance and credit cards, FERPA for education, or CCPA and GDPR, which are broader acts applicable to proper handling of data by all industries doing business in a specific geographic region.

Lapses or violations of compliance with various regulations often occur at a network endpoint where someone is accessing something they shouldn't be or in a way they shouldn't be. From a digital information management standpoint, compliance is best served by identifying the existence, location and status of all endpoints and all sensitive data entities.

Not the same, but both are critical

An organization may be fully compliant with all applicable regulations, but its data and networks may be nowhere near fully secure. Similarly, an organization's data and network may enjoy an admirably high level of security but not be fully compliant with all applicable regulations. Both situations are quite common and equally dangerous.

Value is key

Data is considered sensitive when exposure of it to unauthorized parties, or simply loss of access to it, could significantly and negatively impact the organization financially, strategically, reputationally, or otherwise.

More vividly stated, the average cost of an **organizational breach of sensitive data is $4.4 million.** That's purely lost value.

Even greater costs often accrue when sensitive data is used to compromise the individual or company the data belongs to. Compromised credit card information, for example, can be used to make unauthorized purchases worth thousands each time. Stolen Social Security numbers can be used to access all manner of resources belonging to an individual. Personal and business credit ratings have been severely damaged, as have brand reputations, proprietary product design and trade secrets and more.

We protect sensitive data to preserve its high intrinsic value.

“Sensitive” is in the eye of the beholder

But what is “sensitive” about sensitive data, and how does it accrue its value?

For a healthcare organization, diagnoses of patient conditions are “sensitive” data. For an aircraft manufacturer, the design of its latest fighter jet is sensitive information. For a financial institution, client accounts and holdings are sensitive.

For many companies, information and details about an upcoming merger may be sensitive if secrecy is a strategic imperative. Similarly, the formula for a new beverage about to be introduced may not be life-threatening, but that data is still highly sensitive to the maker that intends to take the market by storm.

Compounding the issue, for service organizations a wide variety of data and data types are all sensitive to one or more of their clients. They need a tool that can quickly adapt from one vertical market focus to another. As their clients, or any company, grow, the platform must be highly extensible and easily scalable to keep up with that growth.

It's all about knowing

Managing a network is one thing and managing sensitive data on that network is another.

Famed business consultant Peter Drucker taught us that you cannot manage what you do not measure. To manage a network, you must measure its performance, its capacities and its continued functionality.

To manage sensitive data, you must know much more.

Existence — You must know exactly which data assets currently reside anywhere on your network. If you're not aware that something exists, you cannot possibly manage or protect it.

Value — To properly protect each data asset residing on your network in storage or in transit, you must first know the intrinsic value of each data asset. You don't want to find yourself spending more to protect something than it is actually worth.

Location — In any network, there is a specific place where each data asset should be located at any given moment. Those boxes of documents were not where they were supposed to be, and nobody knew that for quite some time. Unacceptable.

All possible locations — To be sure you're aware of all data assets residing anywhere, you must know every possible place included in that anywhere — every storage site and transport path available on your network. People do all kinds of odd things with data. They copy it onto USB thumb drives. They send it to personal cloud storage. They delete files. Awareness of any of these actions is critical.

Changes and anomalies — For it to gain value, information must always be in motion and changing. But some changes don't always make sense. When a cybercriminal is moving data, that should instantly be detected and identified as an anomaly. Logging all changes provides a necessary audit trail if any of those changes cause problems later on. Identifying and alerting anomalistic changes helps protect data from unauthorized handling immediately, or at least detects it soon enough to take action.

Endpoints — Data most often egresses from networks inappropriately through unguarded, poorly guarded, or unauthorized endpoints, such as computers, tablets, smartphones, and others. You must maintain a complete and comprehensive knowledge of all endpoints on your network with alerts anytime an unauthorized device attempts to connect and access your resources. It's very much like accomplices blowing a hole in the back of a jail cell to break out their buddy. That's an unexpected endpoint, a way out that shouldn't be there.

It's not enough to look “at”... we must also be able to look “in”

Imagine you’re managing a shoe store, and you’re taking a cycle count of your inventory. One of your employees reports that you have 131 pairs of loafers on the shelf. Being an insightful, experienced manager, you ask them how they know that. When they report that they counted the boxes on the shelf, you instruct them to go back and look inside each box.

When they return, they sheepishly acknowledge that you have only 127 pairs of loafers. Four of the boxes were empty, the shoes stolen by a sneaky customer or perhaps another employee.

Apply this example to the management of data. Most data management tools will report the filename of every file in your system and count how many files there are. This is completely inadequate when managing sensitive data. You must be able to “look inside the boxes,” interrogate file contents to identify suspicious data patterns, strings, or other signatures that might suggest tampering or other misuse.

Managing sensitive data goes far beyond simple “data management.” It requires knowledgeable people armed with a powerful, extensible platform that enables all manner of data interrogation. Cybercriminals are clever thieves. You must be even more clever to catch them.

The advantages of a singular platform

In this eBook, we mentioned many different things — storage systems, data assets, networks, security devices, endpoints, and many more. Most information technology professionals identify specific tools they prefer to use when working with each of these. They tend to find a tool either provided by the manufacturer of the device they're working with, or a supplier that works extensively with that brand of device. Or they may find open-source software that does the trick. Or any dozens of sources for software tools.

The challenges come when those professionals work with other professionals who prefer other tools, or at least don't know theirs. You can end up with a mess of cross-training, inconsistent results, cracks that things can slip through, and plenty of confusion.

For this reason, many IT shops have recently transitioned from finding best-of-breed tools to identifying best-of-platform solutions. These platforms incorporate and integrate all the tools needed to monitor, measure, and manage all the components of an information technology system.

Without a singular platform, it becomes possible to search for sensitive data but miss some instances because you used the wrong tool. You need a tool that will find sensitive data wherever it may currently reside in whatever state it may currently exist. Often you may not be looking for a specific file type, but perhaps hard-to-find patterns such as malware signatures. Your search tools must conduct comprehensive discovery, or you may find yourself embarrassed when a missed instance brings down your network.

And when it comes to detecting and identifying anomalies or unusually high-risk activities, it's unimaginable to depend on an array of tools, each designed to detect a different kind of anomaly. You need one monitor to identify them all.

When you find something broken, what do you want to do next?

You want to fix it. That's just a natural reaction.

With point tools, that may not be possible. You may find yourself carefully copying large volumes for safety, then rushing to shore up defenses and maybe breaking some rules along the way. None of this is healthy for your network or your data.

Instead, you'd like to be able to immediately respond to the problem and fix it where it is occurring, usually on a particular endpoint. Your sensitive data solution must make this easy and immediate. By focusing all remediation on the endpoint, you avoid breaking too many rules, which can often happen when you hurriedly copy or move files around during your process.

When a user requests your assistance resolving a concern over possibly compromised sensitive data, time is of the essence, and you feel it. You either have to mitigate the risk or deal with the damage quickly. Time lost figuring out which tool to use is simply unacceptable. A comprehensive platform solution eliminates that delay.

Tanium has answers

With Tanium, you can gain complete visibility of all your data. Get a real-time picture of all the sensitive data in your environment and make sure it stays in the right hands.

Learn more about **Tanium's sensitive data monitoring solution** and **sign up for a free trial today.**

Tanium is the platform that organizations trust to gain visibility and control across all endpoints in on-premises, cloud and hybrid environments. Our approach addresses today's increasing IT challenges by delivering accurate, complete and up-to-date endpoint data — giving IT operations, security and risk teams confidence to quickly manage, secure and protect their networks at scale. Tanium's mission is to help see and control every endpoint, everywhere. That's the power of certainty.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.