FORTRA

WHITE PAPER (Titus)

Data Is The New Perimeter

The Technology World has Changed

From a technological standpoint, the world is a very different place than it was a decade ago. Remember when:

- Internet Explorer was the #1 web browser
- Facebook was just emerging
- The first video was watched on YouTube
- Google overtook Yahoo in search engine market share
- Millions of terabytes of data were created and shared
- 96% of data leaks were inadvertent

Let's take a look at those same areas in the world today:

- Internet Explorer is the #1 web browser for downloading other web browsers
- Facebook is just emerging as the 3rd largest country in the world
- A video is watched on YouTube every 43 microseconds
- Google overtakes Yahoo in search engine market share by a factor of 5
- Millions of terabytes of data has been created and shared today alone
- 96% of data leaks are inadvertent

The only thing that hasn't changed — the percentage of inadvertent data leaks. The number of those leaks and the amount of data involved has risen dramatically in the last decade. Since 2005, the Privacy Rights Clearinghouse has published information on data breaches that have exposed more than 540 million records. That's 1.6 records for every man, woman and child in the US and Canada. Why is it that so many other online and technological industry stats have advanced so significantly, but our data security is the same as it always was?

The Advent of the Perimeter

The history of data security starts with files. Not electronic files. Paper. For the better part of the 20th century, business was conducted on paper. This made the safeguarding of the information contained on that paper relatively easy. Sensitive information was marked to indicate that it should be protected, and was transported only by trusted individuals. The concept was simple: place the sensitive information in a secure environment (a strong box, locked desk or filing cabinet) and ensure only the appropriate people have the key.

However, this single "security perimeter" was not adequate enough for security-focused organizations. In the mid-19th century, classification systems were developed by governments and military organizations to identify different levels of information sensitivity in order to manage them appropriately. These classification systems were also adopted by many large commercial organizations around the world. It was the benchmark for physical information security. Data classification combined with a strong perimeter allowed for more fine-grained access to information. The information was organized well and therefore easy to keep secure.

When computers were first used for business functions in the mid to late 20th century, data management and information security became more difficult. Because most vital functions were still handled on paper, the situation was seen as manageable by most. At that time, not only were computers the size of a small gymnasium, they had no easy way to communicate with each other. Information contained on any one computer was relatively safe, and relied mainly on a physical perimeter, in this case, a locking door for security.

Entering the end of the 20th century and early into the 21st century, personal computing and networking became a reality, and organizations shifted to using computers primarily to do business. This enabled organizations to do business in new and exciting ways, primarily on computers. Organizations quickly adopted new advancements in computing and networking, and the Internet emerged. These realities lead to the realization that information, which was now so easy to access and share in its new electronic format, needed protection.

It was at this point (only 20 years ago) that the 'virtual perimeter', as we know it today, emerged. In order to prevent compliance problems, loss of reputation and loss of competitive advantage, organizations have spent the last decade carefully building a perimeter around their business information to prevent it from leaking. These perimeters typically consist of technology such DLP systems, security gateways, encryption, IRM solutions, or some combination of these.

Once again, this single perimeter for all data was not adequate enough for government and military organizations, the most secure organizations in the world. Physical information classification systems were carried over to the virtual world, to identify different levels of information sensitivity and to manage and protect them appropriately.

Today's Perimeter

At the outset, building a perimeter seems like a modest undertaking. You have servers and users' systems, both relying on some combination of security systems to make up a perimeter for your data.

User systems that reside inside the perimeter share data with each other, and the perimeter security ensures nothing gets in or out. Is this the reality? Chances are that you have some kind of roaming sales force, or perhaps remote employees, people outside of the physical limits of your controlled space, needing to access and share data inside the electronic perimeter. A VPN of some kind must be used in order to allow that group of users to create and share information with other users.

Chances are you also have some partners or customers that your organization needs to share information with. Again, the perimeter needs to be extended to this group via perhaps a reverse proxy, which allows them to share information back and forth also.

Further, it has become commonplace for today's organizations to move to the Cloud. Some organizations are moving some servers into the Cloud like their email, SharePoint, etc… Once again, new lines must be drawn so that information can be shared back and forth, to and from the Cloud.

All this extension, retraction and re-tracing of your security boundaries leaves out the expanding number of different devices and applications now living within every organization which also must be accounted for.

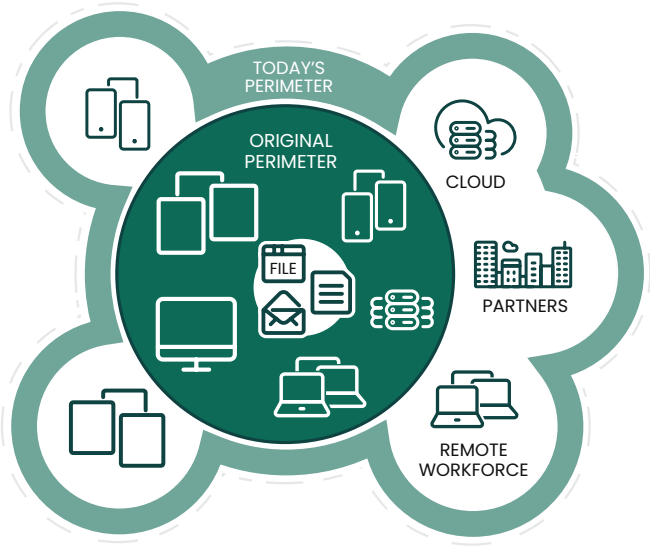

Figure 1: The original perimeter is constantly being extended.

The complexity of today's world in terms of information sharing is staggering, and becoming more complex every day. The original vision of the security perimeter has changed to something almost unrecognizable because of the constant expansion and change. Today's perimeters rely on technologies which were not originally built to deal with the current working reality. As a result, they have become very much a virtual concept, constantly changing, and information is able to ooze around these concepts which we so carefully constructed over the last decade.

The New Perimeter

At the core of the issue is unstructured information. Lack of structure allows your sensitive information to leak outside of your perimeter and is potentially causing your organization not to meet their compliance requirements.

Unstructured information is comprised of emails, documents and other file types, as well as information captured in a collaboration system such as SharePoint. It is no longer enough to put a fence around this information like a traditional perimeter because this information is not all the same.

Figure 2: The new perimeter is the data itself.

It is not all sensitive, nor is it all non-sensitive. This information also lives everywhere. It lives on different devices. It lives in different physical locations. And it exists in many different forms. The new perimeter is the information itself. By securing the information and making it inherently secure, instead of putting up a fence to try and contain it, you can enable your existing technologies to protect that information more effectively.

Enable Your Existing Perimeter with Metadata

Organizations have spent countless resources on building traditional perimeters around their information. Each piece of technology that makes up these strategies has a specific purpose, and executes that purpose well. There is a gap however when taking a more holistic view of the problem, especially when it comes to protecting unstructured data which makes up the bulk of information in today's organizations. All the effort that has gone into building existing perimeters is not without value, however, as these systems all need a common focal point upon which to make security decisions: classification metadata.

Each piece of unstructured data is unique. It needs to be identified as such or your security perimeter does not know what information to let in and out or where to let it travel within the perimeter. For example, an email thread about a company soccer team schedule may be public information and can be let in and out of the perimeter at will. Other types of information(an income statement spreadsheet, for example), may be very sensitive in nature and probably needs to stay within the perimeter or even be restricted to a certain group of people within the organization.

By classifying information, and embedding classification metadata within the information itself, existing perimeter security solutions in your organization, like DLP systems, gateways, even encryption and IRM solutions, can apply tailored security decisions to that data.

> ***"Structured data is stored in a format that you know about; that's predictable like inside of a database. Unstructured usually refers to things like Word documents or PDF's or spreadsheets, text files, anything that's free-form in nature... So classification is going to be the first thing that you'll want to look at. It'll be the main thing; it's in the driver's seat."***
>
> — **Wendy Nather**,
> *Research Director*
> *451 Research*

Titus can ensure that all of an organization's unstructured data is classified, and contains embedded metadata which can enable existing perimeter solutions to protect data wherever it goes. Entire enterprises can be assured that their intellectual property – such as confidential engineering drawings, or perhaps sensitive HR information or export controlled information – is effectively protected.

In order to do this all in "run time", you must first determine who is responsible for the unstructured data. Users are constantly creating and sharing this information, and they know the sensitivity of the information they deal with. Wouldn't the most effective way to ensure protection of every piece of information be to ensure that the users are involved as they are creating and sharing it?

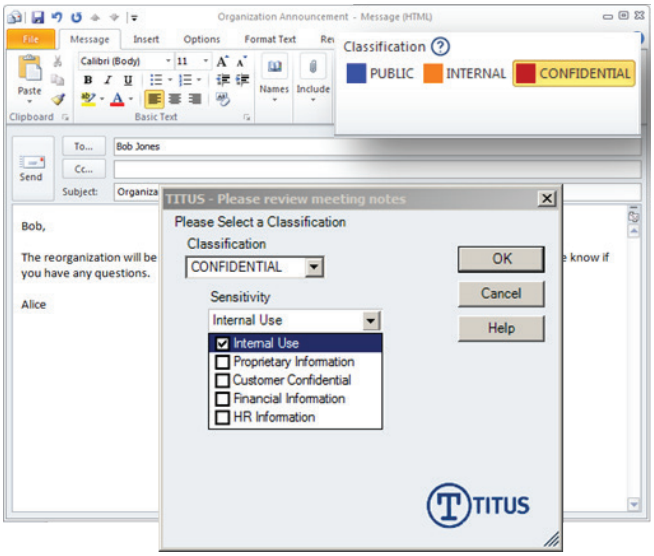

Figure 3: Users can opt to classify their information in a number of different ways including an easy to use ribbon bar or a prompt to classify their information.

The Titus Advantage

Titus Message Classification is an email security solution that ensures every email is classified or identified and protectively marked before it is sent. Classification metadata is embedded into every single email. With users classifying email at the time of creation, organizations can identify the value of that information and manage it appropriately Titus policies also help users classify emails properly by validating email content, attachment content, recipients, domains, and more. When emails are sent, protective markings are applied to raise awareness of the sensitivity of the email and comply with regulations. Titus Message Classification works on Outlook 2010, Outlook Web Access, Lotus Notes, as well as older versions of Outlook 2007 and 2003.

> ***"You need to classify unstructured data in a way that reflects the business logic and how you're already working with that data in your systems. You need metadata and attribute descriptions that everyone is going to be onboard with. And then you're going to have to do all of this in 'run time'."***
>
> — **Wendy Nather**,
> *Research Director*
> *451 Research*

Titus Classification for Microsoft Office is a document security solution that ensures every Office document is classified and protectively marked in the same way. Users can be prompted to classify when saving or printing documents. Headers, footers and watermarks can be automatically applied to raise security awareness of the sensitivity of documents and to comply with any regulations or standards your organization may need to comply with. This solution also embeds rich metadata in those documents.

Titus Classification for Desktop allows all other file types (like PDF, Jpeg, CAD etc…) to be classified by users. So users can classify their files within the Windows Explorer paradigm with a simple right click. Titus applies overlay icons to the files to denote their sensitivity. Titus classification metadata is also automatically inserted into the information.

Titus SharePoint security solutions can apply user permissions based on Titus classification metadata. As information is uploaded to SharePoint, you can ensure that the right people have access to the right information within SharePoint.

Conclusion

If you are wondering how to get started with information classification, Titus can help. Titus has helped some of the most secure organizations in the world implement classification as the cornerstone of their information security and governance initiatives. History seems to be repeating itself, as Titus solutions were spawned in response to the need from the military and government world. However, in the last few years, we are seeing a revival of information classification in many commercial organizations, large and small, using it as the foundation of their security and compliance initiatives, making their existing perimeters truly effective.

Titus has seen many different types of organizations succeed at eliminating information breaches by implementing classification. Experience tells us that the key is to start simple, and to start now, in order to get a handle on all of your unstructured. Existing perimeters are continually being extended, and the information within them keeps growing. While the amount of information continues to increase, and the risk increases in lock-step, every day.

Titus solutions are widely deployed and are in use by over 2 million users worldwide. Customers include NATO, Nokia, International Civil Aviation Organization (ICAO), Dow Corning, Pratt and Whitney, United States Air Force, US Department of Defense, U.S. Department of Veterans Affairs, Australian Department of Defence, and numerous other organizations.

To find out how Titus can help enhance your organization's security, please visit ***www.titus.com***