|  |  |  |
| --- | --- | --- |
|  | | |
| Info Lifecycle Protection | | |
|  | POV Whiteboard Storyboard |  |
|  | | |

|  |
| --- |
| 1. Data is everywhere |
|  |

As the executive responsible for <DRAW Person, WRITE “CISO”> security in your organization, you want to ensure trust in your brand by protecting corporate and consumer data from breaches and attacks. But it’s a constant challenge due to the endless flow of data in and out of your company. Today, data is everywhere. And it’s getting harder to know where it came from, where it’s going, and how to secure it throughout its entire life cycle.

Imagine <DRAW dashed circle> this represents all of the information you need to protect. In the past, this world consisted of data and documents that lived safely within the four walls of your building.

But today, users <DRAW person, WRITE “USERS”> are churning out information faster than ever before. And it’s not just coming from your own employees. There are also contractors, partners, suppliers and consumers. <DRAW circles with E, C, P, S inside> We’re talking massive amounts of data.

|  |
| --- |
| 1. Data flow is more complex than ever before |
|  |

And this data is extremely sensitive. You’ve got PII, <DRAW rectangle, WRITE “PII”> as well as your company’s IP, <DRAW rectangle, WRITE “IP”> which is increasingly determining the valuation of your organization. In fact, in the U.S., IP-intensive industries account for 38% of GDP.[[1]](#footnote-1) You also have government, <DRAW rectangle, WRITE “Gov”> and other types of regulated data <DRAW rectangle with binaries> that are very critical.

Not only that, but as channels increase, so does the complexity of the data. Think about all the ways users communicate today—email, <DRAW envelope> mobile devices, <DRAW smartphone> and laptops. <DRAW laptop> From an IT perspective, data is generated on endpoints, servers, <DRAW server>, and any number of web and cloud applications <DRAW rectangle, WRITE “Apps”> users can access inside and outside of your perimeter.

This data will ultimately be stored in your data center <DRAW tall rectangle, WRITE “DC”> or in a cloud environment <DRAW clouds> such as Office365, AWS, or Salesforce.com. <WRITE “MS, AWS, SFDC” in each cloud>

|  |
| --- |
| 1. Partial, siloed solutions don’t protect all your data |
|  |

Every stage of this complex journey is fraught with potential leaks and attacks. For example, as the data flows through each of these different vectors, do you know who’s creating the data? <DRAW ?> What type of data you have? <DRAW ?> Where the data is coming from and going <DRAW ?> or where it’s residing? <DRAW ?>

You might have partial solutions for different parts of this information flow. For example, you might turn on Microsoft’s cloud security features in Office365. However, this only covers a fraction of where <DRAW dashed square> and how this data moves. What if the data is flowing into your data center or into another cloud service?

And the same problem lies with each of the siloed point solutions. Authentication tools can tell you whether someone is actually who they say they are and keep out bad guys even if they’ve stolen a user’s password. DLP tools can tell you whether you can trust someone with the company’s secrets and keep them from being leaked. But neither can tell you whether a trusted insider should have privileged access and use of sensitive data.

As a result of having limited visibility and control of this information lifecycle, you may implement disjointed policies that are too restrictive—causing your users to go around your controls <DRAW arrow> to create their own access to what they need. These kinds of experiences leave users disappointed, which inevitably leads to shadow IT problems in your environment.

|  |
| --- |
| 1. New Approach: Information Lifecycle Security |
|  |

In today’s world of highly valued IP and increasing collaboration—and worsening cyber threats—you need to eliminate the <DRAW slashes through ?s> the vulnerabilities in the flow of your information.

The only way to do this is with a single point of control <DRAW circle> that protects your information throughout its entire lifecycle. <WRITE “Info Lifecycle Security”> With a single policy for all channels, you can monitor and control who’s creating and accessing all the data <DRAW line> that’s generated in your enterprise.

This allows you to better understand the data—how it’s created <DRAW line> and <DRAW line> how it moves throughout the various vectors—all while controlling <DRAW line/arrow> exactly where it flows throughout the information lifecycle.

With information protection everywhere, you can get complete visibility, control, and protection <WRITE “Visibility”, “Control”, and “Protection”> over *all* the information in your environment, allowing for improved collaboration, better user experiences, and enhanced protection of the data flowing in and out of your enterprise.

Only Symantec can provide the solution to make this happen, and that’s what I would like to talk with you about today.

1. *Global Intellectual Property Center: “IP Creates Jobs for America,”* NDP Consulting, May 2012 [↑](#footnote-ref-1)