

Stratecast

A Division of FROST & SULLIVAN

CHECK POINT CLAMPS DOWN ON DATA LOSS



A Frost & Sullivan White Paper

www.frost.com

"We Accelerate Growth"

Technology cannot comprehend the contextual subtleties of each worker's job duties to make reliably informed, on-the-spot decisions on when and why sensitive data should flow, be quarantined for further consideration, or be blocked. Information worker engagement must be part of a data loss prevention solution.

CHECK POINT CLAMPS DOWN ON DATA LOSS

INTRODUCTION

Businesses are faced with an assortment of security risks. Among the most prevalent risks are network attacks and infected computing systems (servers and end-user endpoints). The consequences of loss of use—that is, network failures and out-of-commission computing systems—are just too great for any business to ignore. In practice, most businesses have taken appropriate steps to avoid loss of use incidents by utilizing a variety of purpose-built security technologies such as firewalls, Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS), and anti-virus/malware software.

But what about the data that is flowing within and out of these networks and computing systems? Isn't that where the true value of most businesses exists—the building blocks of competitiveness and the lifeblood of effective communication and collaboration? Shouldn't the data itself be protected from loss too? The answer, of course, is yes.

Preventing data loss, however, can be very difficult especially when one considers the many ways information workers can place data at risk of being lost. For example:

- Mistyping an email address or clicking on the wrong email recipient from an automatically generated drop-down list.
- Uploading sensitive data to a file sharing website.
- Selecting the wrong file (e.g., highly sensitive) as an email attachment.

Furthermore, technology alone is not the answer. Technology cannot comprehend the contextual subtleties of each worker's job duties to make reliably informed, on-the-spot decisions on when and why sensitive data should flow, be quarantined for further consideration, or be blocked. Information worker engagement must be part of a data loss prevention solution.

In this document, we have chosen to review Check Point DLP (Data Loss Prevention) as it effectively combines the contextual understanding that only humans can bring with the power of technology. Moreover, our view is that Check Point DLP delivers the following business benefits:

- Directly support businesses’ objectives such as reaching and staying compliant with information protection regulations and protecting digital assets.
- Shorten the time to prevent data losses without breaking the budget or unduly impeding business operations.
- Systematically educate all employees on being responsible stewards of sensitive data, further demonstrating that technology without the human element is an incomplete approach.

EVERY BUSINESS HAS DATA TO PROTECT

All businesses have data they **have to** or **need to** protect. In the **have to** protect category are businesses that store or process information that is subject to one or more industry or governmental information privacy regulations. Notable examples in the U.S. include:

| <i>Regulation</i> | <i>Objective</i> | <i>Regulated Entities</i> |
|--|---|---|
| Health Insurance Portability and Accountability Act (HIPAA) | Protect patient personal health information (PHI) and personal identifiable information (PII) from misuse and improper disclosure | Any organization in the health-care field including but not limited to: clinics, hospitals, doctor offices, health care facilities in schools, pharmacies, insurers, and pharmaceutical companies |
| Payment Card Industry Data Security Standards (PCI-DSS) | Protect the private information of credit card account holders (account number, name, service code, and expiration date) from unauthorized disclosure | Physical and online retailers, merchants, and payment card processors and clearinghouses |
| Sarbanes-Oxley Act (SOX) | Protect non-public financial data and intellectual property (IP) from improper disclosure | All companies publicly traded in the U.S. |
| Gramm-Leach-Bliley Financial Modernization Act (GLBA) | Protect the security and confidentiality of client non-public personal information | Financial services firms including banks, financial institutions, insurers, and security brokers |
| State data notification and privacy laws. Notable examples: California SB 1386 and Massachusetts Data Protection Law 201 CMR 17.00 | Protect personal identifiable information (PII) as defined by the state | Organizations conducting business with customers in a covered state |

The U.S. is not alone in instituting regulations aimed at protecting sensitive and private information. European Data Protection Directive is among the most prevalent privacy legislation outside the U.S. Further, with growth in the number of regulations instituted at various levels of government (continental, federal, and state) and from within industries, an increasing number of businesses are subject to one or more regulations (e.g., doctor offices subject to HIPAA and PCI-DSS regulations).

Moreover, the consequences of compliance violations and data breaches can be costly. Depending on the incident, there are the **direct costs of fines and breach notifications**. There can also be substantial **indirect costs**, namely:

- Crisis management
- Escalation in compliance auditing depth and frequency
- Future investments in solutions and processes to avoid incident recurrences
- Litigation
- Short-term and potential long-term loss of public trust and its implications—lost business.

Regulatory compliance is one reason to protect sensitive data; preventing the loss of data that has value to the business is also critical. Consider customer account data. If received by one of your competitors, say through a disgruntled employee, wouldn't this data loss place your customer engagements at risk? This same exposure is present with marketing plans, financial statements, and product development roadmaps. For many companies, intellectual property (IP) is vital to their competitive advantages. Software code, manufacturing specs, and product designs are just a few examples of IP. The loss of intellectual property, whether through a malicious act or employee carelessness, can quickly diminish a company's competitive advantage.

Whether you have to protect what's important to others, need to protect what's important to your business, or a combination of both, businesses like yours are facing a daunting task in preventing data losses; a task that is growing in complexity in the digital age.

THE DIGITAL AGE INCREASES THE POTENTIAL OF DATA LOSS

Less than a generation ago, the risk of data loss was significantly lower. One of the reasons for this is that data was more centralized and controlled. Pre-Internet, data in digital form was accessible only by workers through closed, proprietary networks. Moreover, with the cost of computing and data communication networks being significantly higher than today, the number of workers granted network access was more restricted and their scope of access privileges limited. Closed networks, restricted access, and limited access privileges narrowed the exposure of data loss incidents. It is also worth remembering that electronic messaging, today's ubiquitous means to communicate with anyone with an email address, in the early 1990's was confined to intra-company communications—an example of a closed network.

Regulatory compliance is one reason to protect sensitive data; preventing the loss of data that has value to the business is also critical.

Now, high-speed computing and data communication networks are standard fare. Nearly every worker is networked in some fashion. The Internet has paved the way for closed networks to be open networks. Personal computers have reached the point where they are as commonplace as desktop phones and in every home (frequently in multiples). Gigabits of storage are available on finger-sized removable media. More recently, social networks (e.g., Facebook, Twitter, and LinkedIn) are proving that networks do not require IT approval, oversight, or technical expertise. Anyone can instantly create a network that literally spans tens to hundreds to thousands of connections. Our conclusion: the avenues to communicate are numerous, simple, and at nearly everyone's fingertips. Consequently, data that was once protected by being centralized in closed networks can quickly and easily be propagated to unaccountable destinations and people with just a few clicks and keystrokes.

Also, consider that workers conducting personal Web activities through business networks and connecting their personal devices into these same networks further add to data loss exposure. According to a 2009 survey conducted by Frost & Sullivan of IT decision makers, these are common and uncontrolled occurrences in small (less than 100 employees) and mid-sized (100 – 500 employees) businesses. The implications, unfortunately, can be profound. For example, a worker sends a sensitive document through a file sharing website to his/her home PC. Once on the home PC, all members of the household potentially have access to that same sensitive document and can share it, intentionally or in error, with anyone on the household's network of connected "friends". **While the worker's intent was benign, the data is lost and there is no formal record of its exposure.**

Our conclusion: the avenues to communicate are numerous, simple, and at nearly everyone's fingertips. Consequently, data that was once protected by being centralized in closed networks can quickly and easily be propagated to unaccountable destinations and people with just a few clicks and keystrokes.

| | Percent of Small-sized Businesses | Percent of Mid-sized Businesses |
|--|-----------------------------------|---------------------------------|
| Have employees accessing the Web for personal use through the business network | 70% | 86% |
| Have employees connecting personal laptops to the business network | 76% | 77% |
| Have employees inserting personal storage media | 69% | 82% |

Source: 2009 Frost & Sullivan Survey

Another important aspect in the escalating exposure to data loss is the extent that data losses occur from non-malicious acts. In a 2008 survey conducted by the TheInfoPro of 1000 Information Security Professionals, the respondents indicated that over 90% of the time data losses were the result of non-malicious acts. The point is that as workers

gained access to higher volumes of regulated, sensitive, and proprietary data as part of their work roles, so too has the risk of data loss grown.

Further evidence from Verizon Business Risk Team in its investigations of 2008 data breaches¹ highlights that “everyday” end-users are prominently involved in internally originated data breaches.

| Perpetrator | All | Financial | Food | Retail | Tech |
|-------------------------|------------|------------|---|------------|------------|
| Anonymous | 5% | 8% | Insufficient number of cases for statistical analysis | 11% | 0% |
| End-user | 41% | 53% | | 33% | 23% |
| IT Administrator | 50% | 31% | | 45% | 77% |
| Executive | 2% | 0% | | 11% | 0% |
| Agent/Spy | 2% | 8% | | 0% | 0% |

Source: Verizon Business

As Verizon Business noted, “Only in Financial Services are end-users responsible for more breaches than IT administrators. Based on our investigative experience, we associate this with the greater access non-IT employees have to sensitive resources. One doesn’t require highly privileged access to systems in order to compromise data.”

Additionally, security breaches are a high priority concern for a majority of information security professionals.

| Rated as a High or Top Priority Concern by Information Security Professionals | |
|---|-----|
| Customer privacy violations | 70% |
| Customer identity theft or fraud | 67% |
| Theft of intellectual property | 64% |
| Breach of laws and regulations | 61% |

Source: 2008 Frost & Sullivan Global Survey

“One doesn’t require highly privileged access to systems in order to compromise data.”

Source: Verizon Business

¹ 2008 Data Breach Investigation Supplemental Report authored by Verizon Business in 2009

Faced with points such as these, it would seem logical that businesses would be actively deploying solutions specifically designed to prevent data loss, much as they have done to protect their networks and computing systems. The current reality is quite different. Based on our research and surveys, most enterprises and SMBs do not have a data loss prevention solution deployed despite the overriding need and concern about data loss.

THREE DATA LOSS PREVENTION METHODS

There are three methods to reduce the risk of data loss today and it is important to understand each before making a decision on how to most effectively and efficiently reduce this risk and meet information privacy regulations. The three methods are: Data-in-Motion, Data-in-Use, and Data-at-Rest.

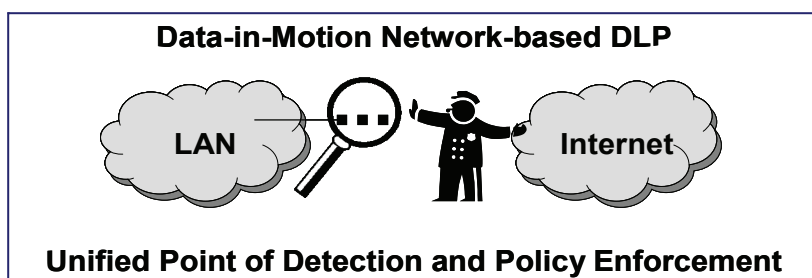
While each data loss prevention method (Data-in-Motion, Data-in-Use, and Data-at-Rest) has beneficial attributes in preventing data loss, we view the network-based Data-in-Motion method as having the greatest impact in the shortest timeframe.

As explained below, Data-in-Motion offers a unique combination of:

- Extensive range of detection (all outbound communication),
- Strategic location (between private and public network environments), and
- Deployment simplicity (no modification to end-user systems).

With a network-based DLP solution based on the Data-in-Motion method, businesses gain deep and wide visibility from which to take immediate action to prevent data losses that occur in a communication conduit used by virtually all of its employees.

Data-in-Motion – Detects and controls the movement of sensitive data² through outbound communication channels. Data-in-Motion DLP is also referred to as a network-based DLP solution.



- **Detection Range** – Potentially *all outbound communication flows* originating from all endpoint systems (business-owned and employee-owned) connected on the business' LAN.

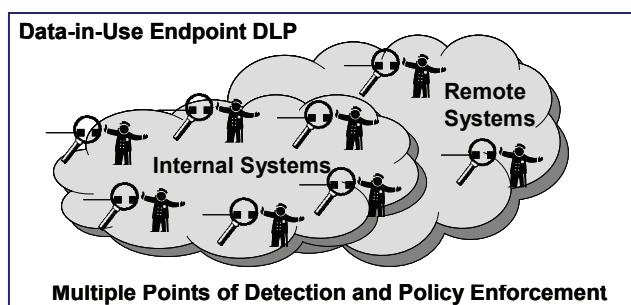
Based on our research and surveys, most enterprises and SMBs do not have a data loss prevention solution deployed despite the overriding need and concern about data loss.

While each data loss prevention method (Data-in-Motion, Data-in-Use, and Data-at-Rest) has beneficial attributes in preventing data loss, we view the network-based Data-in-Motion method as having the greatest impact in the shortest timeframe.

² For brevity, "sensitive data" includes all types of data in digital form that require data loss prevention.

- **Location** – **Unified DLP policy enforcement** at the perimeter between a business' private network and the public Internet.
- **Deployment** – Similar to traditional security gateways (e.g., network firewalls, IDS/IPS), connect inline or off a switch port. **No agent deployments on endpoint systems** (e.g., PCs, servers, file shares) or reconfiguration of endpoint systems are required.

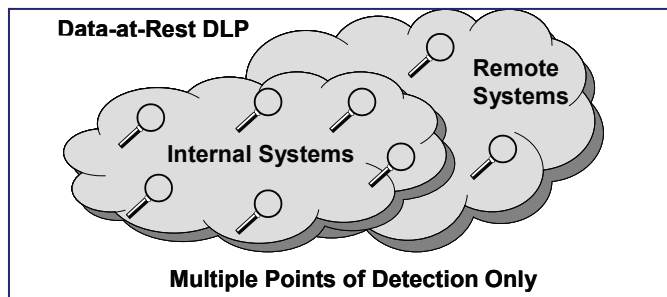
Data-in-Use – Detects and controls sensitive data movement within and from endpoint systems. Data-in-Use DLP solutions are also referred to as endpoint DLP.



- **Detection Range** – Potentially all user actions (e.g., outbound communications, printing, and file copying to external media) but **only on endpoint systems on which a software agent can be installed** (e.g., business-owned endpoint systems).
- **Location** – Distributed policy enforcement at endpoint systems. **Policy enforcement will only occur on endpoint systems that the company owns that can accept the agent.** Plus, businesses may choose not to install the agent on a subset of endpoint systems to minimize licensing and maintenance expenditures.
- **Deployment** – **Requires installation of a software agent** on each agent-compatible and chosen endpoint system. The software agent will utilize a portion of the endpoint system's computing and storage resources.

Data-at-Rest – Dissimilar to Data-in-Motion and Data-in-Use solutions whose objectives are to detect and control the movement of sensitive data through outbound communication channels and/or among the subsystems in endpoint systems, the objective of Data-at-Rest solutions is to detect the existence of sensitive data as it rests in data repositories—servers, endpoint hard drives, tape drives, etc. Enforcement of data loss policies is not an immediate outcome of a Data-at-Rest DLP. The information gathered through Data-at-Rest scans can be used to devise a course of action to reduce the risk of data loss.

With a network-based DLP solution based on the Data-in-Motion method, businesses gain deep and wide visibility from which to take immediate action to prevent data losses that occur in a communication conduit used by virtually all of its employees.



- **Detection Range** – Only detects the existence of sensitive data when a scan is conducted on addressable (i.e., known) data repositories chosen by the business.
- **Location** – Distributed detection with no immediate prevention/DLP policy enforcement.
- **Deployment** – Requires scans of data repositories through permanent or temporary software agents. Scans will utilize a portion of the system’s computing resources.

CHECK POINT DELIVERS IMMEDIATE DATA LOSS PREVENTION

Check Point’s recently launched DLP solution follows the Data-in-Motion/network-based approach, which we view as a proactive step for businesses in preventing data loss with effectiveness and consistency. Data-in-Motion, as previously stated, has the beneficial characteristic of being inline with the flow of outbound communications. From this strategic location, Data-in-Motion solutions can intercede on a wide swath of data loss avenues without having to “touch” endpoint systems or pre-identify and classify sensitive data stored in data repositories. In that respect, Check Point’s DLP is a self-contained, real-time sensitive data detection and policy enforcement solution—taking action on “active” sensitive data.

Furthermore, communication channels for many businesses are the most prevalent means to share data, and likely the most vulnerable to workers’ non-malicious but nevertheless careless acts that contribute to data loss. For example, the use of Web mail or file sharing websites to send work documents to home PCs, which are outside the control of a business’ security and IT personnel. **Once work documents land in a home system, the only control is the overly optimistic hope that employees can, not just will, apply the same level of information security as is possible within the business environment.** With the existence of home networks and sharing of PCs by multiple household members, this hope of control is further dashed. Once a piece of data is on an employee’s home computer, it should be considered exposed.

Similarly, the rush of the business day and the auto-complete capabilities of many email software applications contribute to the unfortunate ease for workers to select an incorrect email address or attach the wrong file (a file containing

sensitive data instead of one that does not). Again, not intentional policy violations by workers but once the communication with sensitive data is sent, the data is out the door and control is lost, plus there may be no record of the loss.

Check Point also supports many Data-in-Use DLP capabilities through its endpoint security software suite and recently introduced Abra platform. Check Point's endpoint security software suite includes port control and protection of the endpoint system from virus and malware contamination. Abra is a highly secure portable data container. With Abra, workers can carry sensitive files with them and onto uncontrolled endpoint systems, like home PCs, without losing control of the sensitive data or subjecting the sensitive data to a compromised system.

We will now turn our attention to the specifics of Check Point DLP.

REVIEW OF CHECK POINT DLP

In this review, we will focus on the challenges that have plagued DLP solutions, how Check Point addresses these challenges with its solution, and how the Check Point DLP delivers on the business benefits of:

- **Supporting businesses' compliance and protection of digital assets objectives**
- **Shortening the time to prevent data losses**
- **Systematically educating all employees on being responsible stewards of sensitive data**

Challenge #1: Accurate and Comprehensive Detection of Sensitive Data

Accuracy and comprehensiveness go hand-in-hand in effectively detecting sensitive data and judging policy violations. The converse, inaccuracy and incompleteness, has numerous business implications, such as: creating a false sense of data security, raising the risk of information breaches and regulatory compliance violations, and/or compelling businesses to rein in the scope of their DLP deployments. The reasons for these implications are simple:

- **The risk of data loss increases** as sensitive data is not detected and policy violations not flagged.³ Additionally, if information workers are not aware of legitimate policy violations, a reinforcing means to change unacceptable sensitive data handling behaviors is diluted.
- **Disruptions in business flows and excessive alert management costs rise** as inaccurate or aggressive detection schemes contribute to the volume of policy violation alerts. This adversely affects the routine cadence of business processes

³ Incidents of sensitive data not being detected and, consequently, violations of DLP policies not being flagged are also referred to as false negatives.

Check Point's DLP is a self-contained, real-time sensitive data detection and policy enforcement solution—taking action on “active” sensitive data.

as a higher number of communications are logged, quarantined until investigations can be completed, or blocked versus a DLP solution with more accurate or refined detection capabilities. Furthermore, a higher number of policy violation alerts add to the human cost of examining them and hampers efforts to modify worker behaviors as clear and consistent assessments of policy violations are absent.

Check Point's answer to accuracy and comprehensiveness is **MultiSpect™**, the company's data inspection engine. MultiSpect consists of three components:

1. **Multi-parameter data classification and correlation** - Inspects the most widely used TCP protocols including SMTP, FTP, HTTP and webmail to identify sensitive content types based on pattern matching and file classification independent of file extension and file compression.⁴
2. **File form and data type detection** – Detects sensitive data in a broad range of file formats and data types (over 600) and supports an open scripting language for creating customized file formats and data types.
3. **Built-in policies and custom template support** – Includes pre-defined policies and support for custom forms and templates to automatically detect and protect sensitive information defined in information privacy regulations (e.g., PCI-DSS, HIPAA, GLBA, and SOX). In total, Check Point DLP includes over 250 pre-defined policies that take into account the sender's identity and role, the communication channel, and whether the recipient has been preauthorized to receive sensitive data.

Challenge #2: Reining in DLP Incident Handling

Incidents are recorded when end-users violate DLP policies (e.g., upload sensitive data to a file sharing website). Depending on how the DLP solution functions, end-user communications that trigger policy violations can be quarantined until the incident can be reviewed and approved by a DLP administrator. While potential data losses were averted, there are several consequences that follow with this approach to incident handling:

- **The volume of incidents exceeds the time available by the existing pool of DLP administrators** resulting in demand to hire and train more DLP administrators; an added cost to the business.
- **Delays in the routine flow of business operations and processes** as policy violating communications are quarantined and DLP administrators struggle to stay current with a growing backlog of incidents to review.
- **DLP administrators may lack sufficient contextual understanding** to make wise decisions, and **inconsistency in decision making** may occur when there is more than one DLP administrator.

⁴ SSL and HTTPs will be added in the future.

- **Sensitive information is revealed to someone outside the “need to know” circle**, for example, confidential intellectual property or human resource materials (e.g., payroll details and performance reviews) being reviewed by people lacking “need to know” status.

The key to reining in incident handling—delayed business processes, the cost of DLP administration, incident handling inconsistencies, and exposure of sensitive data to non-circle members—is by reducing the volume of incidents.

Check Point reduces the volume of incidents by giving its customers the means to drive resolution of policy violations to the information workers, the people most familiar with the sensitive data and the business objectives in using the data. **UserCheck™** is the name Check Point applies to this capability.

Through this empowerment, information workers are presented with gentle reminders in real-time to “pause and reconsider” what they are doing. Is the action prudent, necessary, and accurate (e.g., correct file attachment and correct recipient)? As previously stated, only humans can fully comprehend the contextual subtleties of their job duties. With this comprehension, informed decisions can be made on when and why sensitive data should flow, be approved by another before releasing, or rescinded. UserCheck systematically and effectively inserts information workers into the data loss prevention process.

By inserting information workers into the data loss prevention process, beneficial extensions of UserCheck materialize:

- **Responsible data stewards quickly emerge** – As information workers are presented with alerts of policy violation, they become more informed and conscientious in their handling of sensitive data. This leads to improved handling of sensitive information, resulting in fewer alerts that workers receive. In early customer trials, Check Point reports that the number of alerts their customers’ workers received was dramatically reduced in a matter of weeks.
- **Fewer incidents reviewed by DLP administrators** – With fewer alerts generated because workers are more aware of sensitive data policies and more conscientious in how they handle sensitive data, the number of incidents that require review by DLP administrators naturally declines.

Of the lower number of alerts that are generated, Check Point’s logging and alert analysis capabilities built into its DLP solution provide DLP administrators the means to uncover lingering patterns of unsafe and questionable data use behaviors and they can then modify their worker education initiatives accordingly. Education can take several forms: formal classroom education, “did you know” type emails, and, within the Check Point DLP solution, the UserCheck alert screen is highly customizable to be an effective and targeted means for information workers to learn of their unacceptable behaviors.

Also contributing to the reduction in incidents is the accuracy in identifying sensitive data and policy violations. The more accurate the identification, the fewer nonsensical alerts

The key to reining in incident handling—delayed business processes, the cost of DLP administration, incident handling inconsistencies, and exposure of sensitive data to non-circle members—is by reducing the volume of incidents.

UserCheck systematically and effectively inserts information workers into the data loss prevention process.

are received by information workers and policy violation alerts by DLP administrators. Attention is then concentrated on the violations that reflect bona fide non-compliant behaviors.

Challenge #3: Cost

New security technologies, such as data loss prevention, raise legitimate concerns about cost—purchase price, on-going licensing fees, administrative burden, and training of administrators and information workers. It is therefore critical for any DLP solution to project a realistic sequence of benefits—reduction in the risk of data loss and in the avoidance of the compliance violations—relative to the anticipated costs associated with the solution.

Several of the points made earlier on how Check Point addresses the previous two challenges of DLP solutions also contribute to controlling costs.

- Accuracy and comprehensiveness in identifying sensitive data reduces the costs and consequences of identification inaccuracies and incompleteness.
- Check Point DLP addresses a significant avenue of data loss—outbound communications – without the expense and effort to touch endpoint systems and data repositories.
- UserCheck reduces alert management costs for both information workers and arbitrators and accelerates the transformation of workers into responsible data stewards, which in turn reduces the risk and business consequences of compliance violations and data breaches.

Other attributes of the Check Point DLP solution also contribute to controlling the cost of data loss prevention:

- Check Point DLP administrative interface was designed for intuitiveness and ease-of-use, a favorable attribute when administrators are not part of IT. Additionally, the DLP administrative interface is part of the centralized Check Point Security Management system, including the multi-domain Provider-I management system, saving the business the expense of purchasing and learning a separate management system.
- The Check Point DLP Software Blade offers savings and flexibility by co-existing on a gateway platform that is also hosting Check Point firewall and IDS/IPS security technologies.

It is therefore critical for any DLP solution to project a realistic sequence of benefits—reduction in the risk of data loss and in the avoidance of the compliance violations—relative to the anticipated costs associated with the solution.

Stratecast

The Last Word

At the onset of this document, we listed what we believe to be the top three characteristics businesses should require in a data loss prevention solution. They are:

1. Directly support business objectives.
2. Shorten the time to prevent data losses.
3. Systematically educate all employees on being responsible stewards of sensitive data.

After reviewing Check Point DLP and its key components (MultiSpect, UserCheck, and Event Management system), we believe the company is on the right track to deliver on each of these DLP solution requirements for its customers.

Michael Suby

Director

Stratecast (a Division of Frost & Sullivan)

msuby@stratecast.com

CONTACT US

Beijing
Bengaluru
Bogotá
Buenos Aires
Cape Town
Chennai
Delhi
Dubai
Frankfurt
Kolkata
Kuala Lumpur
London
Manhattan
Melbourne
Mexico City
Milan
Mumbai
Oxford
Palo Alto
Paris
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Singapore
Sydney
Tel Aviv
Tokyo
Toronto
Warsaw

Silicon Valley
331 E. Evelyn Ave.
Suite 100 Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SW1W 0DH, UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost
myfrost@frost.com
<http://www.frost.com>

ABOUT STRATECAST

Stratecast assists clients in achieving their strategic and growth objectives by providing critical, objective and accurate strategic insight on the global communications industry. As a division of Frost & Sullivan, Stratecast's strategic consulting and analysis services complement Frost & Sullivan's Market Engineering and Growth Partnership services. Stratecast's product line includes subscription-based recurring analysis programs focused on Business Communication Services (BCS), Consumer Communication Services (CCS), Communications Infrastructure and Convergence (CIC), OSS and BSS Global Competitive Strategies (OSSCS), and our weekly opinion editorial, Stratecast Perspectives and Insight for Executives (SPIE). Stratecast also produces research modules focused on a single research theme or technology area such as IMS and Service Delivery Platforms (IMS&SDP), Managed and Professional Services (M&PS), Mobility and Wireless (M&W), Multi-Channel Video Programming Distribution (MVPD), and Secure Networking (SN). Custom consulting engagements are available. Contact your Stratecast Account Executive for advice on the best collection of services for your growth needs.

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, partners with clients to accelerate their growth. The company's TEAM Research, Growth Consulting, and Growth Team Membership™ empower clients to create a growth-focused culture that generates, evaluates, and implements effective growth strategies. Frost & Sullivan employs over 45 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from more than 30 offices on six continents. For more information about Frost & Sullivan's Growth Partnership Services, visit <http://www.frost.com>.