Innovations

LEARNING SERIES

EXPRESS EDITION

Modern Blueprint to Information Protection

Lawrence Miller

INSIDE THE GUIDE:

- Understand Why It Is Harder Than Ever to Protect Your Data
- Recognize the Need to Modernize Traditional Protection Methods
- Find Out the Best Ways To Defend Your Precious Data

ActualTech Media
actualtechmedia.com

BROUGHT TO YOU BY
proofpoint.

Modern Blueprint to Information Protection

EXPRESS EDITION

By Lawrence Miller

ACTUALTECH MEDIA
6650 Rivers Ave Ste 105 #22489
North Charleston, SC 29406-4829
www.actualtechmedia.com

PUBLISHER'S ACKNOWLEDGEMENTS

EDITORIAL DIRECTOR

Keith Ward

DIRECTOR OF CONTENT DELIVERY

Wendy Hernandez

CREATIVE DIRECTOR

Olivia Thomson

SENIOR DIRECTOR OF CONTENT

Katie Mohr

PARTNER AND VP OF CONTENT

James Green

WITH SPECIAL CONTRIBUTIONS FROM PROOFPOINT

Itir Clarke
Joel Borgmeier
Brian Reed

ABOUT THE AUTHOR

Lawrence Miller, CISSP, has worked in information security and technology management for more than 25 years. He received his MBA in Supply Chain Management from Indiana University and has earned numerous technical and professional certifications throughout his career. He is currently working as an IT security solutions consultant. He has previously worked as the Vice President of IT for a major Verizon reseller, director of IT and e-commerce for a retail merchandising company, and IT operations manager for a top 100 U.S. law firm. He served as a Chief Petty Officer in the U.S. Navy and is the author of more than 200 books on various topics including information security, cloud, unified communications and collaboration, storage, 5G, and the Internet of Things.

ENTERING THE JUNGLE

CALLOUTS USED IN THIS BOOK

THE 101

This is where we turn when we want to provide foundational knowledge for the subject at hand.

OFF THE BEATEN PATH

This is a special place where you go to discover insight into topics that may be outside the main subject but that are still important and relevant.

BRIGHT IDEA

When we have incredible thoughts (at least in our heads!), we express them through eloquent phrasing in the Bright Idea section.

DEEP DIVE

Takes you into the deep, dark depths of a particular topic.

EXECUTIVE CORNER

It’s not all tech all the time! This is where we discuss items of strategic interest to business leaders.

ICONS USED IN THIS BOOK

DEFINITION

Defines a word, phrase, or concept.

KNOWLEDGE CHECK

Tests your knowledge of what you've read.

PAY ATTENTION

We want to make sure you see this!

GPS

We'll help you navigate your knowledge to the right place.

WATCH OUT!

Make sure you read this so you don't make a critical error!

TIP

A helpful piece of advice based on what you've read.

INTRODUCTION

Welcome to the Modern Blueprint to Information Protection Innovations Express Guide®. Whether you're a CISO, privacy officer, CTO, CIO, IT director, SOC manager, or network/infrastructure/cloud architect, this guide will help you understand why a people-centric, unified information protection platform is crucial to help your business protect its valuable data.

Data is one of your company's most valuable assets, so modern information protection is imperative. Legacy data loss prevention (DLP) tools do a poor job of protecting enterprise data in the face of a disappearing network perimeter and expanding attack surface. This is evidenced by the rapidly growing frequency, scope, cost, and impact of data breaches. Clearly, a new approach to DLP is needed. Let's get started by taking a look at the information protection imperative...

CHAPTER 1

Understanding the Information Protection Imperative

Data Breaches Continue to Rise

Data breaches are a constant threat for every organization—regardless of size or industry. Whether perpetrated by an external compromise or insider threat, a data breach can have a devastating impact on a company. According to the Ponemon Institute, the average total cost of a data breach is $3.86 million. This cost includes:

- **Detection and escalation** activities such as incident response, forensic investigation, and threat containment/eradication.
- **Notification**, including communications to customers, stakeholders, regulatory bodies, law enforcement, and third-party experts.
- **Post-breach response activities**, such as legal costs, regulatory fines, punitive damages, and remediation services for victims (for example, credit monitoring, identity protection, and re-issuing accounts or payment cards).
- **Lost business**, including lost productivity and revenue due to downtime, loss of customers (both existing and new), and brand reputation damage.

EXECUTIVE CORNER

Easy employee access to sensitive data and large-scale credential theft

Desjardins Group is a Canadian bank and the largest credit union federation in North America. In late June 2019, the Desjardins Group revealed that an employee had stolen bank customer information—including names, addresses, birth dates, social insurance numbers (SINs), email addresses, and information about individual transaction behaviors—to share with a malicious third party. The insider breach affected all 4.2 million credit union members, as well as 1.8 million credit card holders who were not members and 173,000 businesses. The estimated cost of the breach to the organization is $108 million.

The Expanding Attack Surface and Disappearing Perimeter

Even before the global pandemic, the traditional network perimeter was quickly disappearing as companies increasingly embraced cloud computing and remote/mobile working. Today, users routinely access cloud-based email and Software-as-a-Service (SaaS) applications such as Microsoft 365, Salesforce, and Workday from their laptops and mobile devices while working from home or a hotel lobby. As a result, the attack surface expanded greatly, and people became your new security perimeter (see **Figure 1**). In the wake of the pandemic, many companies have had to redefine the nature of work and rethink how work gets done. A hybrid workforce—including work from home (WFH) and work from anywhere (WFA) users—is the new normal. Workers are accessing sensitive data with fewer security controls

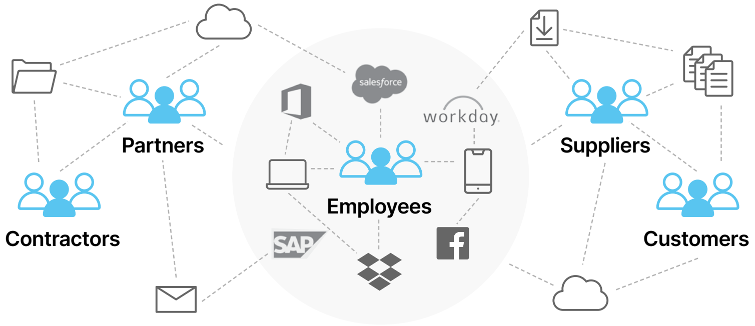


Figure 1: People are your new security perimeter

while security teams have incomplete visibility into data access and movement by users. Threat actors—both external and internal—have taken notice.

Remote work during the COVID-19 pandemic increased the time to identify and contain a potential data breach. It also increased the cost of a data breach by nearly $137,000 to an average total cost of $4 million according to the Ponemon Institute.

People are the Leading Cause of Data Breaches

Data doesn't just lose itself. People are always involved. Although external threat actors are responsible for the majority of data breaches (78 percent according to the Verizon *2021 Data Breach Investigations* Report), insiders are responsible for an average of 22 percent of all data breaches and 61 percent of breaches involve credentials. In some industries, such as healthcare, insiders are responsible for as much as 39 percent of data breaches. But before you start wondering if people are inherently bad or if it's time to revamp your recruiting and hiring practices, let's take a look at the nature of the insider threat.

Attackers—whether insiders or not—are clearly after credential and personal data. However, an insider threat can be more difficult to detect and therefore may cause more damage over a longer period of time than an external compromise.

Negligent – "USB always comes to the rescue on my flight"

Negligent users comprise most insider incidents—62 percent according to the Ponemon Institute. Negligent users are generally well-intentioned but may be unaware of risky behaviors (such as copying sensitive files to a USB drive), oblivious to data protection requirements ("I'm too busy to deal with all of this security stuff"), or otherwise distracted (perhaps multitasking and accidentally sending an email to the wrong recipient).

Compromised – "I may have clicked on a malicious link in a phishing email"

Compromised users (that is, credential theft) are responsible for 61 percent of incidents. Like negligent users, a compromised user is generally well-intentioned, but may have fallen victim to phishing, social engineering, or malware. A compromised user may also have unwittingly created a weak password, or perhaps used the same password across multiple personal and work accounts, essentially opening the door for an external threat actor to take over and misuse a compromised user's credentials (think of it as the technical equivalent of "name dropping").

Malicious – "I've given my two-week notice; I'm taking 'my work' with me"

Sadly, malicious users account for nearly a quarter, 23 percent, of insider incidents. Malicious users are motivated by greed, spite, or indifference. Perhaps they were passed over for a coveted promotion or believe they're unfairly compensated. They view any work product they created during their tenure as "theirs" and have no qualms about taking sensitive data (such as customer information or intellectual property) with them.

How you mitigate risk due to insider threats depends on user intent. Next, we'll take a look at the need for a modern information protection platform and the future of information protection.

CHAPTER 2

Recognizing the Need for a Unified Information Protection Platform

User security awareness training is an important first step in mitigating data breach risk associated with negligent and compromised users. However, you need to do more to protect your organization's sensitive and valuable data. Effective data loss prevention (DLP) requires a unified information protection platform that delivers seamless end-to-end protection for your digital estate across all data loss channels and against all attack vectors.

Data is Poorly Protected by Legacy Tools

DLP is a key component of any comprehensive security strategy. The goal of DLP is to ensure your users do not share sensitive or valuable data—personally identifiable information (PII) for employees and customers, trade secrets, intellectual property, customer lists, vendor information, and more—with unauthorized parties. DLP also helps organizations comply with industry and government data privacy regulations.

However, legacy DLP tools do a poor job of protecting data for the modern hybrid workforce. From your users' perspective, these tools increase friction and negatively impact productivity. From your security operations center (SOC) analyst's perspective, these tools provide only limited visibility and create too much noise. Let's take a closer look at these challenges.

While monitoring and protecting regulated data and intellectual property is important, credentials and personal data are the two most likely targets of data compromise according to the 2021 Verizon *Data Breach Investigations Report*.

User friction and loss of productivity

According to Forrester, in 73 percent of all organizations that deploy DLP tools, their employees complain about it. Why? It gets in the way of productivity, especially when it mistakenly blocks your employees from using or sharing data, accessing internet websites, or running software-as-a-service (SaaS) applications they need to get their work done. These legacy DLP tools may block workflows and business processes they shouldn't, thereby creating a poor user experience, increasing user frustration, and negatively impacting productivity. This problem is even more prevalent today because legacy DLP tools were designed to protect the traditional corporate perimeter rather than the remote hybrid workforce that has become the new normal in the wake of the pandemic. The unintended consequence of these overly restrictive tools and policies is that "shadow IT" (the use of unauthorized applications) runs rampant and increases organizational risk.

According to Forrester, 66 percent of companies say their DLP tools often prevent employees from accessing data, even when they follow policy.

Limited visibility and too much noise

SOC analysts spend too much time searching for the proverbial "needle in a haystack." They're inundated by daily security alerts—as much as 75 percent of those alerts are false positives, according to data provided by managed security services provider, Critical Start. Further exacerbating this problem, legacy DLP tools may not be giving your SOC analysts a complete view of your digital estate. In other words, they're being overwhelmed by false-positive alerts and are only seeing part of the haystack! This "noise" provides threat actors—both external and internal—all the cover they need to go undetected long enough to exfiltrate your sensitive and valuable data.

Data silos and long cyles of deployment, discovery, and classication

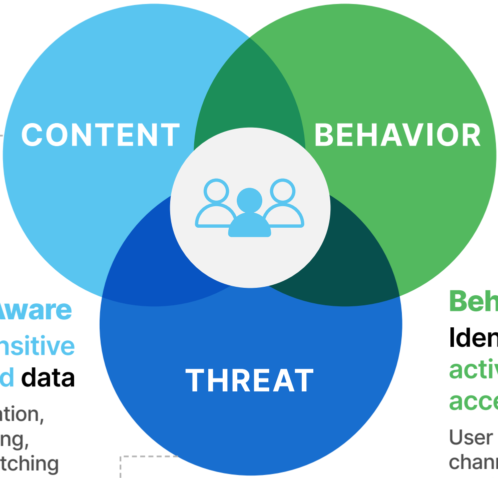
Pursuing a best-of-breed approach to DLP can result in data silos and unnecessary complexity. You end up with multiple DLP teams deploying and managing solutions on-premises and in the cloud. Disparate rule sets create frustration and inconsistent data protection. Instead of focusing on the risky ways users are handling data, traditional DLP solutions focus on discovering and classifying data, which can take months. Some 75 percent of IT leaders surveyed by Forrester said deploying their DLP solutions took at least a month. A full 24 percent said it took six months or longer. Another problem is that most DLP tools, including Microsoft Information Protection, cannot ingest prior data classification efforts without high-priced professional services. With each new program, organizations have to reclassify their data within the new tool.

Reimagining Information Protection

Clearly, it's time to reimagine information protection. A modern, people-centric approach to information protection offers a unified, easy-to-manage solution with scalable cloud-native architecture. People-centric information protection is more effective and requires less administrative overhead than legacy DLP, which is data-centric and spends an inordinate amount of time on data discovery and classification. Instead, a people-centric approach focuses on user risk and data handling, provides more comprehensive protection, and facilitates faster investigation, response, and remediation—thereby reducing the risk of a devastating data breach. The three keys to a modern information protection solution are:

- **Offers comprehensive visibility and control.** Modern information protection connects users to data movement and risky behavior—across email, files, applications, and endpoints—covering key vectors for data exfiltration and providing a unified view of activity and consistent controls across all channels.

- **Delivers contextualized and accurate alerts.** Modern information protection recognizes risky user actions, not just static data classifications. It uses content, behavior, and threat telemetry to build context (the "who, what, where, and when") and understand intent, to generate accurate and actionable near-real-time alerts (see **Figure 2**). For example, it uses real-time threat intelligence to identify compromised accounts, recently phished users, and other high-risk users. Prioritized alerts align security best practices and compliance requirements and mitigate real risk. It leverages modern classification techniques and provides an intuitive interface that facilitates investigation and action.



Content Aware

Identify sensitive or regulated data

Data classification, labelling/tagging, exact data matching and more

Behavior Aware

Identify user activity, intent and access context

User activity across channels, file source and destination, device, network, role, watchlist and more

Threat Aware

Identify compromised accounts, phished users

Advanced threat intel/insights across cloud and email telemetry

Figure 2: Understanding and mitigating user risk require a people-centric approach to information protection

- **Built on cloud-native architecture.** Modern information protection is cloud-native so that it's easy to implement and delivers fast time-to-value. Key capabilities include:
  - Email DLP via a highly scalable cloud-based email gateway with advanced workflows
  - Cloud access security broker (CASB) visibility and enforcement for cloud apps leveraging application programming interfaces (APIs), in-line methods, and isolation
  - Endpoint/insider threat management (ITM) in a lightweight endpoint sensor with context-based DLP

- Web security via a proxy that can inspect traffic for safe browsing and DLP and apply granular controls through integration with browser isolation
- A unified admin and response console that integrates policy management to incident workflows, reporting, and analytics across key data loss channels

In its report, *It's Time For Next-Generation Data Loss Prevention*, Forrester Research found that 81 percent of decision makers believe they need a better way to protect their sensitive data while keeping up with the pace of innovation, including cloud-first, work-from-anywhere, and mobile initiatives. It's time for a unified information protection platform for visibility, detection, prevention, and response with multiple layers of protection across all channels.

CHAPTER 3

Envisioning the Future of Information Protection

Armed with the knowledge of what isn't working today and why, it's time to envision the future of information protection for your organization. In this chapter, we'll help you get started with a risk treatment plan, gap analysis, and maturity model. We'll also explore managed information protection services as an option to augment your current capabilities, and the benefits and business outcomes that a modern information protection platform can deliver for your organization.

Getting Started with Enterprise-Wide Information Protection

Identifying your valuable assets—including your data—is the first step in protecting those assets. Of course, your data is constantly changing so identifying your valuable data is somewhat different from inventorying other assets, such as equipment, facilities, or furniture.

Start by building a risk treatment plan for the data in your organization. Building this plan requires some thought and collaboration with different stakeholders and information owners across your organization to help identify the diverse types of data within your organization, the value of each data type, and the potential risks to that data. Also consider any regulatory requirements associated with your different data types, for example:

- **Financial data** may be subject to the Payment Card Industry Data Security Standards (PCI DSS), Sarbanes-Oxley (SOX) Act, Gramm-Leach-Bliley Act (GLBA), and Securities and Exchange Commission (SEC) and Federal Trade Commission (FTC) regulations, among others.

- **Personally identifiable information (PII)** may be subject to the European Union (EU) General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), Canada Personal Information Protection and Electronic Documents Act (PIPEDA), and other laws.
- **Personal health information (PHI)** may be subject to the U.S. Health Insurance Portability and Accountability Act (HIPAA) and Health Information Trust Alliance (HiTrust), and so on.
- **Classified government information** may be subject to the U.S. National Industrial Security Program Operating Manual (NIPSOM) and others.

You also need to understand the characteristics of the different data types within your organization. These characteristics include:

- **Content**—What is it?
- **Community**—Who interacts with it and how do you know if they're compromised or malicious?
- **Channels**—How does data move within your environment and how do you monitor and protect the data throughout its life cycle?

Now it's time to build an information protection program that addresses five key areas including:

- **Application management**—How do you keep everything running, up to date, and communicating properly?
- **Scope and policy governance**—How do you build and tune your information protection policies?
- **Event triage**—Who manages the alerts and what is the service-level agreement (SLA) or service-level objective (SLO)?

- **Incident management**—How will you respond to security alerts and incidents (including identification, escalation, containment, eradication, and recovery)?
- **Reporting and analytics**—What key performance indicators (KPIs) and success criteria matter most to your business stakeholders?

Assessing Your Current Capabilities

Building a strategic roadmap to your envisioned future state requires you to recognize where you're starting from. You need to assess any DLP technology currently deployed in your environment and consider the following questions:

- What capabilities and limitations exist?
- Are there specific pain points or coverage gaps that need to be addressed?
- How can your existing investments be used as part of a more comprehensive information protection solution for your organization?
- What additional capabilities do you need to protect your hybrid workforce today and in the future?

Many organizations use a capability maturity model to help determine their current state and identify key areas where improvements are needed. In the case of modern information protection, there are four key capabilities that most organizations have already deployed, but with varying levels of success and functionality:

- **Level 1: Email.** Email remains the most common attack vector for data breaches today. Increasingly sophisticated phishing campaigns lure unsuspecting users into exposing sensitive information (such as account credentials) or to click on malicious links and attachments. At its most basic level, email security should provide some level of protection against spam, phishing, malware, and data loss for all your users. More advanced capabilities should include business email compromise (BEC) protection and seamless yet robust email encryption for partners and others you need to share sensitive data with.

- **Level 2:** Cloud. A cloud access security broker (CASB) service provides organizations with visibility and control of the software-as-a-service (SaaS) based applications and file-sharing services used by your workforce—no matter where they're accessing the cloud from. Advanced CASB capabilities include application programming interfaces (APIs) for cloud apps, traffic log auditing, application risk scoring, adaptive access controls, browser isolation, forward proxies, and cloud security posture management.

- **Level 3:** Endpoint. Modern endpoint protection should extend beyond basic malware protection to include data activity monitoring for all users and insider threat management (ITM) for specific business purposes. Some examples of users and business purposes include newcomers, leavers, and business activity groups like mergers and acquisitions, finance, research and development (R&D), and so on.

- **Level 4:** Web. In the age of work from anywhere and data everywhere, having a web gateway appliance in centralized data centers doesn't work. A global and highly-elastic cloud framework is critical to ensure users stay safe while browsing the web—and that attackers don't compromise an organization's critical data and assets. Modern web security capabilities include the ability to inspect all traffic (including encrypted traffic) for threat protection and DLP as well as the ability to apply granular controls through integration with browser isolation. While in isolation, the user can access the site in read-only mode without risking exposure to threats or data loss.

- **Level 5:** Integrations. A modern information protection platform should provide seamless integration to enable complete end-to-end coverage of third-party and custom systems, applications, and services across your entire digital estate. This includes on-premises, cloud, and remote/mobile. Advanced analytics should enable deep business and security insights into threats across email and cloud, user behavior, and data usage. Integration with interactive security awareness training modules ensures that the right users get the right training to maximize effectiveness while reducing user friction. A unified admin and response console simplifies day-to-day security operations and accelerates response by combining advanced tools including:
  - Policy management
  - Incident and investigative workflow
  - Threat hunting and explorations
  - Reporting and analytics
  - Attribute-based administration and data privacy controls

Looking at Managed Information Protection Services

Technology is just one aspect of modern information protection. You also need the right people and processes to use your technology effectively. Finding security experts to operate disparate technologies is both challenging and expensive. Effective security management requires high volumes of general work skills and low volumes of extremely rare and expensive skill sets. A recent study by the International Information System Security Certification Consortium (ISC)2 found that although there are 3.5 million individuals currently working in the security field worldwide, there is still a shortage of 3.12 million security professionals in the global workforce. To fill this talent gap, employment will need to grow by approximately 41 percent in the U.S. and 89 percent worldwide.

Faced with these challenges, many companies do one of the following with their internal security staff:

- Do not staff appropriately and fail to deliver effective information protection outcomes to the business.
- Hire a limited number of resources with high-end skill sets that they cannot retain because those resources do not want to spend most of their days doing the "mundane" work.
- Hire resources with the necessary general skill sets but lacking the high-end skill sets, which creates a low-value information protection program that has spiraling costs since the high-end skill set is what controls the volume of the low-end workload.

Because it's difficult to hire the right skills in the right amounts to build a comprehensive information protection operation, in-house staffing and professional services approaches deliver low efficacy, high costs, or both. A better option is to consider leveraging a managed services model with a trusted partner. Look for a partner to help you implement and operate your modern information protection platform with capabilities and services that include:

- Enterprise data loss prevention (DLP)
- Cloud access security broker (CASB)
- Web security
- Insider threat management
- Security awareness training

Realizing Key Benefits and Business Outcomes

A modern information protection solution helps your organization mitigate data loss risk from threat actors—both external and internal. Key benefits and business outcomes include:

- Protection from data loss starting with people-centric visibility
- Improved information protection efficacy and contextualized alerts for real-risk mitigation
- Accelerated incident response, remediation, and investigation
- Faster response gains and reduced investigation time to limit damage and impact
- Reduced costs with a consolidated approach to information protection
- Faster time to value delivery through a cloud-native platform and managed information protection services

Call to Action

As cloud adoption and the pace of innovation continue to accelerate, businesses of all sizes in all industries are challenged to support and protect today's hybrid remote workforce. Legacy DLP tools designed for perimeter-based security provide limited visibility and control while inhibiting user productivity and increasing user friction. Instead, a modern people-centric solution is needed to deliver effective information protection. Built on a cloud-based architecture, modern information protection helps reduce data loss from insider risks and external threats, accelerate incident detection and response, and increase team efficiency through faster time to value and consolidated capabilities managed in a single, intuitive console. As organizations embark on the modern information protection journey, they need to look for a solution that takes a holistic approach and includes these essential elements:

- Scalable information protection that extends to all data types and protects email and cloud applications
- Cloud-native, flexible architecture that enables seamless integrations with other security solutions
- Fast to deploy with a lightweight footprint that offers immediate visibility across the computing environment, with no need to set up rules for endpoints in order to see what's going on
- Security and privacy by design, with well-defined data exclusion policies and strong access controls so the right people have access to the right data at the right time
- Managed security services to close skills gaps, ease resource constraints, support regulatory compliance, and accelerate time to value

Learn more about modern information protection at https://proofpoint.com/us/products/information-protection.

ABOUT PROOFPOINT

proofpoint®

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

ABOUT ACTUALTECH MEDIA

ActualTech Media

ActualTech Media is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.

If you're an IT marketer and you'd like your own custom Gorilla Guide® or Innovations Learning Series title for your company, please visit https://www.gorilla.guide/custom-solutions/