IDC ANALYZE THE FUTURE

IDC TECHNOLOGY SPOTLIGHT

Sponsored by: Seclore

Data-centric security technology has witnessed a decade's worth of progress in the last couple of years driven by Machine Learning and Artificial Intelligence, replacing manual tasks with automation.

Data-Centric Security Coming of Age, Enabled with Automation

April 2021

Written by: Frank Dickson, Program Vice President, Cybersecurity Products

Introduction

The age of digital transformation has resulted in sensitive data residing across on-premises and distributed environments as well as cloud applications, carrying different risk levels and approaches to mitigate the risk to critical data. Compounding the complexity of protecting these assets is employee demand for ubiquitous access to corporate resources, regardless of device, connectivity, or location.

Traditional security solutions, such as secure web gateways (SWGs) and data loss prevention (DLP) platforms, were designed decades ago to reduce the risk of traditional network perimeter architectures. This perimeter-based security was applied in silos for policy enforcement at ingress and egress points and to attempt to detect data theft and prevent accidental data loss and exposure. The security solutions were rarely integrated, poorly maintained, and often deployed passively rather than in line to prevent disrupting business workflows or simply address negative audit findings. The result is inconsistent data governance policies, increasingly limited visibility into encrypted traffic, and a lack of context of user activity. The floodgates have opened the floodgates for cybercriminals, who frequently seize upon these limitations to identify and target vulnerabilities and configuration issues or simply leverage stolen account credentials to bypass enforcement mechanisms to attack.

These issues have been validated in many survey findings. Although a quarter of sensitive data still resides in on-premises datacenters, the sensitive data making up the other three quarters is spread evenly across desktops and laptops, smartphones, and public and private cloud environments. Approximately 30–35% of this data is encrypted, according to a survey of 620 IT and IT security practitioners across North America and Europe. Tracking and controlling sensitive data are significant challenges because data owners are often remote and working with external customers, contractors, and business partners. The most sensitive data resides at the endpoint, with more than 64% of those surveyed indicating data to be very sensitive or extremely sensitive.

The data security market is evolving to address these issues. A converging security infrastructure shows promise in reducing the complexity of managing data governance policies across hybrid and multicloud environments.

Applying Digital Transformation to Data Security

Enterprises today are confronted with a constant "data chase" reality, tracking data as it moves with accelerating velocity. Data facilely flows from devices to on-premises applications, from the cloud to business partners, being presented with a myriad of technical, legal, and process controls to secure data based on its infrastructure or location. The approach has unpredictable and often undependable success rates. Data-centric security instead looks to change that application of security to one that focuses on the data itself rather than the infrastructure.

The problem, however, is we are jaded by the experiences of the past. Frankly, being jaded is warranted as legacy solutions were hard to use and awkward to implement, created friction with end users, and produced inconsistent results. We struggled with:

- Deciding what to protect
- Determining the correct rights & policies to apply
- Updating rights when roles change
- Making sense of audit and telemetry data

The result, if we are to be completely honest, was that we either placed many of our data-centric security initiatives in passive/monitor mode or, even worse, we turned them off completely, continuing to pay for protection as needed to provide evidence of the security measures to pass an audit.

Data-centric security technology, however, has made a decade's worth of progress in the last couple of years. Machine learning and artificial intelligence techniques have been the tools that enabled progress. In essence, automation has replaced the manual.

To address the concerns directly, we describe point by point how yesterday's reality is addressed by a modern, digital transformation approach.

Deciding What to Protect: Visibility Is Key

Yesterday's Reality

Perhaps the biggest challenge to all data protection solutions is "user friction." Solutions required end users to be an active participant in the data classification process, asking them to consistently identify critical data.

The Modern Approach — Automating Data Visibility

By leveraging the visibility created by data access–centric technologies, such as DLP, cloud security gateways (also referred to as cloud access security brokers or CASBs), and SWGs, we can ameliorate the role of the user. DLP and cloud security gateway solutions can be automated to work seamlessly with a digital rights management (DRM) solution. As the DLP solution "detects" sensitive information, the DRM solution automatically adds the appropriate granular usage controls and tracking. This interoperability requires bidirectional communications, a flexible policy engine that can ingest existing DLP, data classification, and content management system labels/rules as well as share threat indicators to support rapid detection and response operations. This security market convergence enables enterprise security teams to leverage a single unified policy engine, a single management console, centralized analytics, and a consolidated reporting framework. Whether data-centric security solutions are classifying, detecting, or protecting documents, the use of automation wherever possible can maximize the adoption of these solutions

over the long run. This will reduce training requirements and ensure security loops are closed as much as possible and facilitate adoption.

Determining the Correct Rights and Policies: Application Accuracy

Yesterday's Reality

Even if we were able to get 100% commitment from users to participate in sensitive data identification, we are also relying on users to accurately identify that data as the manual approaches of the past require end users to decide or choose from one of the predefined admin policies, which is problematic. The result is the incorrect application of data security policy. In IDC's *2021 Data Protection and Privacy Survey*, we found that organizations placed data security controls on data that did not need them and not protect intellectual property (IP) that needed it.

Additionally, manual privacy methods are not sustainable as privacy programs and the regulatory ecosystem grow more complex. Spreadsheets, questionnaires, or simple web portals are just not scalable and no match to the real-time data control and orchestration needs of modern privacy regulations, such as the California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR). Broad and complex laws are not overly prescriptive on how to achieve compliance, and their application is challenging for many organizations, particularly those lacking privacy resource and expertise.

The Modern Approach — The Accurate Automation of Security Policy

Automation determines the correct rights and policies to apply at scale by the system fetching security policies from the underlying application and applying them to the information, whether data lives in SAP, Box, Salesforce, SharePoint, or any other application or storage medium. Data-centric security platforms can ingest existing data classification tags to extend the detection and prevention of unauthorized use and transmission of confidential information beyond the traditional corporate perimeter. These platforms support a cloud-based global policy store to maintain a single policy language to ensure compliance and ease of policy updates when business processes and workflows change. They also make critical data searchable and trackable regardless of the location of the assets.

Automation is critical as modern and ever-evolving privacy requirements will crush data security measures that are manually powered. Automation can leverage content and data repositories to create portals that enable consumers to view the data associated with them with little to no uplift on behalf of the organization except the initial implementation. Privacy needs to be operationalized with the automated discovery of each individual's data across structured and unstructured systems and layers of automation and orchestration on top of it to comply with all the aspects of global privacy regulations. A PrivacyOps framework is required, which enables such individual-level data intelligence and layers of automation in a collaborative environment for various stakeholders. The key requirements of an effective PrivacyOps framework are:

- The most foundational element of a PrivacyOps framework is the ability to automatically find personal data about an individual and make it easy for data, privacy, and compliance teams to interact with that data.
- It should have an easy-to-use, secure platform to engage with individual consumers, enabling them to exercise data rights and update consent.
- It involves the automation of critical privacy compliance requirements, such as data subject access requests (DSARs), breach notifications, and assessments.
- It requires a comprehensive record of all privacy compliance activities.

» It involves a secure collaboration system among privacy stakeholders to avoid personal data sprawl.

Updating Rights When Roles Change: Just-In-time Agile Application

Yesterday's Reality

In the past, changing security policies was a manual process that relied on the end user and/or administrator intervention. At best, access rights changes lag the access protection requirements by days or weeks, leading to user friction. At worst, overly permissive access policies are implemented, providing users with unneeded or unwarranted permissions. The price of the resulting violations of the least privileged access is audit failure or excessive data loss in the event of a breach.

The Modern Approach

The modern approach extends the automation of the identity life cycle to data-centric security. As a new employee is entered into a human resources management platform, such as Workday, a corresponding digital identity is created in Active Directory, Google Identity, or any other identity platform (IdP). A data-centric security platform can then apply the data access rights to the identity roles based on policy.

The real power in the approach comes from the application of data access rights as the employee continues with an organization. As an employee transfers to another division or gets promoted, the changes in the human resources management platform automatically update IdP roles and cascade rights to the DRM platform almost instantly. When the employee leaves the organization, all digital rights are revoked at scale.

Rights automation is about adjusting not just to the changing roles of an employee but also to the changing environment. The organic growth of regional privacy requirements is simply at a scale that cannot be managed manually. By automating role-based data access controls in real time, companies can easily adjust to an increasing complex set of data sovereignty and control issues.

Making Sense of Audit and Telemetry Data: Data-Centric Intelligence

Yesterday's Reality

Making sense of audit and telemetry data policies is hard for corporate IP; today's compliance and privacy requirements make it even harder. Yesterday's approach of having specialists in security, privacy, and/or compliance do the work is expensive and not scalable; asking end users to attempt it is simply ludicrous.

The Modern Approach

By leveraging automation and artificial intelligence gained by working with leading data-centric security experts, platforms can automate the audit process with prebuilt analytics. These modern DRM solutions support data privacy initiatives by enabling the active tracking of data usage and residency. Tracking and auditing telemetry can enrich the data set used by security monitoring, analytics, and audit reporting downstream. Security teams gain situational awareness into sensitive data use and improved context behind potential malicious activities so they can make better-informed policy decisions regarding high-risk employee activities.

Integrations with tools that security professionals are accustomed to is important. The tool of choice is security information and event management (SIEM). Why make them use another platform? If there is an unauthorized

access attempt, existing response playbooks can generate alerts. Thus, data-centric security can adjust to the existing people and processes rather than the other way around.

The automation of the data security process enables technologies to be deployed as most security technologies are deployed without the involvement of end users within the enterprise. Automation and machine intelligence have created transparent data visibility and control. Time to value is reduced, and enterprises can get to security fast and easy.

Where to Start?

If your organization is just beginning the process of implementing data-centric security, where do you start? IDC recommends starting with the low-hanging fruit. By focusing on the use cases that provide the maximum value, data protection initiatives can get some early wins and enable a foundation for continued success. Three use cases commonly stand out for a big return on initial investments:

- **Collaboration and email**. The COVID-19 pandemic had two major impacts on data security. First, it made us quickly realize that email is a primary threat vector as cyber miscreants leverage it for phishing, ransomware, and business email compromise attacks. Second, the use of collaboration platforms accelerated as organizations rushed to regain work productivity from home migrations. A few asked how data would be secured over these platforms. By implementing data-centric security measures integrated into your email and collaboration platform, security professionals can have a massive impact on the threat to an organization's data.
- **External collaboration**. What happens when confidential data and IP need to be shared with external agencies, such as contactors and partners? Ensuring the security, privacy, and compliance of data usage in the supply chain has been a largely unsolved problem. By "inoculating" the data before it leaves the enterprise, the enterprise can regain control and visibility of the data when it "lives" outside of IT architectures.
- **Extending DLP and cloud security gateways beyond the enterprise and beyond the cloud**. Well-implemented on-premises DLP and cloud security gateway policies provide little protection when the workforce has migrated to home-based work. Even when COVID-19 vaccines become common and plentiful, workers are not necessarily returning to the workplace. Before the pandemic, 14% of the workforce was remote, whereas 22% of the workforce will remain working from home after vaccines are readily available. The new location-agnostic work reality is a concept that IDC refers to as hybrid work. Extending DLP and cloud security gateway policies to seamlessly accommodate a location-agnostic reality provides a tremendous reduction in organization risk through consistent data security implementation.

Data Security in the Modern Workplace Is All About Tools and How Quick and Easy You Can Get Them Running

As stated earlier, in 2020, integration and automation are integral to security but especially to data-centric security. While being continually presented with a rising tide of complexity by digital transformation, security professionals must appropriately discover, classify, monitor, contain, encrypt, and/or destroy data. The volume of enterprise data creation and acquisition typically increases at a compound annual growth rate of 40–50%. The scale of the data security task mandates tooling to the deployment of controls in ways that efficiently address the applicable risk. The long-standing control objectives of data confidentiality, integrity, and availability are important components to a data protection security strategy.

Now, it not enough for a tool to offer integration and automation; tools must also be easy to implement and use. In the COVID-19 era, time to value is the metric of the day.

In IDC's first assessment of the impact of COVID-19 on security (*Cybersecurity Impact of COVID-19: Work at Home Is a Mixed Bag*, IDC #US46171520, March 2020), we predicted that:

> Security products requiring on-premises management servers could suffer during this period. These implementations could be slowed as teams work to support the radical transformation of the manner work is being accomplished. Turnkey projects could suffer the most because transporting resources across the world is not possible in some regions. In addition, organizations planning to release new request for proposals in the next three to four months may delay these proposals until 2021. Planned security implementations in 2021 may be greatly inhibited as the required 2020 planning and approvals could be disrupted or delayed. The security market impact from the 2020 seeds sown of COVID-19 will likely be reaped in 2021 in many cases. Finally, software-as-a-service (SaaS) cloud security services will be the beneficiary as the demand for multifactor authentication, VPN, data protection, endpoint management software, and remote productivity tools increases. Available tools assist IT teams with servicing remote workers, enabling seamless access to corporate resources, and easing the deployment of new software and services.

We were essentially correct, but our verbosity was far from elegant and did not get to the salient issues. In our follow-on analysis (*Security and COVID-19: Better Optics Enabled by Data*, IDC #US46871820, October 2020), we noted that platforms that require complex implementations suffered. Whether the offering was on-premises-based or in the cloud was irrelevant. Time to value is the differentiating feature. Solutions that offered quick time to value were able to grab new logos at rates significantly higher than those that require complex implementation. Identity is a perfect example. SaaS-based single sign-on (SSO) and authentication offerings flourished but not so much for transformational identity migrations.

Finally, although the emphasis of this paper has been protection, data-centric security platform tools also facilitate response, enabling a faster reaction time to data breaches. Forensics is facilitated with robust data monitoring capabilities (i.e., who did what, when it was done, and from what location or device). The use of a data kill switch can limit the spread of ransom or data theft, allowing you to revoke access to data that has left your building.

MESSAGE FROM THE SPONSOR

Seclore (www.seclore.com) enables organizations to adopt a unified data-centric approach to security and compliance across hybrid environments. Seclore Data-Centric Security Platform combines data discovery, classification, protection, and tracking of data into a single, automated framework, regardless of how or where data goes. Seclore's platform:

1. Integrates with best-of-breed DLP, CASB, data classification, and rights management into an agile, automated platform
2. Provisions data-centric security as a service in the cloud within 24 hours with no IT administration
3. Eliminates chasing your sensitive data shared internally, externally, or from bad actors by automatically protecting it when discovered, downloaded, or emailed
4. Removes the need for user intervention by automatically attaching persistent, granular usage controls to sensitive emails and documents

5. Tracks user activities on documents and revokes access immediately to any file, anywhere it resides

Find out more at www.seclore.com how you can get more out of your data-centric security tools for a stronger, easier, and faster data security offense.

About the Analyst

***Frank Dickson**, Program Vice President, Cybersecurity Products*

Frank Dickson is a program VP within IDC's Cybersecurity Products research practice. In this role, he leads the team that delivers compelling research in the areas of network security; endpoint security; cybersecurity analytics, intelligence, response, and orchestration (AIRO); identity and digital trust; legal, risk and compliance; data security; IoT security; and cloud security.

Frank is a frequent speaker at security events domestically and internationally and is often sought out for his expertise and insights on the cybersecurity market.

IDC Custom Solutions

IDC Corporate USA

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

Twitter @IDC

idc-insights-community.com

www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.