White Paper

Information-Centric Security: Why Data Protection Is the Cornerstone of Modern Enterprise Security Programs

Sponsored by: Symantec

Robert Westervelt
March 2017

IDC OPINION

Now, more than ever, chief information security officers face the significant challenge of adapting their information security programs to the rapid pace that emerging technologies and services are transforming the corporate network. At the center of every enterprise security program is the ability of the security team to apply and manage the controls that reduce the risks to the business' critical data assets.

But data security strategies of the past can no longer keep up with the skyrocketing amount of data being created, captured, and used by business teams to gain a competitive advantage. IDC estimates that in 2016, the amount of digital information being created, captured, and replicated exceeded 9.3ZB (that's more than 1 million petabytes). By 2020, the amount of data is expected to reach 44ZB. While much of this data is never stored, petabyte-scale deployments of data systems are commonplace with many organizations, and much of this information is often copied, shared, and stored in multiple repositories.

Getting a handle on these critical data assets requires a modern, information-centric security approach. Such an approach transforms a security program into one that focuses on protecting data assets without hindering business owners. It binds what traditionally have been largely isolated security solutions for data protection into one that is comprehensive and functions cohesively while reducing IT complexity. A fully configured and maintained information-centric security approach provides data protection that follows your information and is transparent to end users. It ensures the integrity and confidentiality of key data assets but steps aside to enable business managers to take advantage of the massive amounts of data being collected and focus on growing the business. It is a key challenge that is being compounded by the incredibly rich and unstructured nature that business data has become.

Adopting an information-centric security strategy helps alleviate some of the complexity involved in addressing data protection. The strategy involves the integration and automation of three major controls: data loss prevention (DLP), encryption, and identity and access management (IAM).

Each of these security controls has strengths and limitations when applied and configured properly. But an information-centric approach to security integrates these controls and transforms them from the rigidness associated with their past. It creates the automation and transparency required of safeguarding data assets without disrupting the dynamic nature of today's corporate environments.

IN THIS WHITE PAPER

This white paper discusses the various trends in data protection and security and explores the merits to an information-centric approach to data protection. In addition, this white paper examines Symantec's role in the important data protection market.

SITUATION OVERVIEW

Data is the lifeblood of most organizations. Whether it is a record of innovation that describes key intellectual property (IP), embodied as a financial transaction for business activities, or a set of information that portrays characteristics of a customer or any of many other user cases, it drives value to the organization.

The ubiquitous nature of data requires modern enterprise data protection solutions to be agile enough to adapt to the growing use of cloud services, smartphones, tablets, wearables, and other technologies used to create, consume, and share information. The most compelling products must work in harmony to protect an organization's core data assets in the cloud, on-premise, or in motion and do so in a way that doesn't limit the ability of business teams to collaborate among themselves and with business partners.

To enable the business without creating additional IT complexity, enterprises must adopt modern components to tried and true security technologies, data loss prevention, encryption and tokenization, and authentication, regardless of where the information resides (in the cloud or on-premise). A cohesive solution must gather enough telemetry data to maintain visibility and control, enabling an administrator to support data owners with the ability to take action when a compromise takes place.

Despite new and disruptive technologies and approaches, basic security best practices require information security professionals to gain situational awareness of the business' core assets. That requires a solution that can give administrators data telemetry about the frequency of data access and an audit trail to clearly understand how a core data asset is being accessed, shared, and manipulated. This supports the information-centric security strategy by continually monitoring existing data governance policies and understanding changes to business workflow and the efficacy of the enforcement mechanisms already in place. Reviewing current data governance policies and updating them to address workflow changes, SaaS adoption, and any perceived gaps is a key part of this information-centric security strategy.

There are three major controls for data protection that can be very powerful if they function together to identify and classify critical data, monitor and enforce data governance policies, and encrypt and obfuscate sensitive data as it is created and shared. IT provides a brief overview of the controls and their strengths and limitations when functioning single handedly:

- **Data loss prevention:** DLP solutions are the nerve system of an information-centric security strategy. DLP includes a broad range of solutions that support the discovery and monitoring of confidential data and often provides the enforcement mechanism for data governance policies. It is deployed to address insider threats, protect intellectual property, and control regulated data. Modern DLP solutions should incorporate information access, data handling rules, encryption, recovery planning, and other controls or enforcement mechanisms. A recent survey conducted by IDC found interest in modern data loss prevention solutions rising considerably, driven partially by the significant rise in ransomware in 2016, an attack

technique that encrypts data and holds the decryption keys for a ransom. Compliance continues to be the key driver of adoption, and the EU General Data Protection Regulation (GDPR), which will take effect in May 2018, is believed to be the primary compliance concern prompting the latest investments in modern DLP technology.

  - **Strengths:** Strong DLP solutions can extend data policy enforcement and protection to popular cloud-based email and storage services, such as Office365, Box, or Dropbox, using an integrated cloud security gateway solution. A DLP solution should also mobile devices and must detect critical assets regardless of whether it resides in structured data sources or confidential unstructured data, such as complex intellectual property.
  - **Solitary limitations:** When data loss prevention is deployed solo, organizations fail to gain the true value from their DLP investment. DLP solutions rely on rules to protect data and generally can only block or alert when it detects a policy violation. This has caused many organizations to limit blocking functionality to avoid disrupting end users.

- **Encryption:** Endpoint, email, and file share encryption are fundamental data protection technologies. Under an information-centric security strategy, encryption acts as the ligaments that bind information access and DLP. To scale and manage a robust encryption environment, the keys to unlock the data need to be managed themselves. Routines for creation, assignment, revocation, and recovery can be best implemented with a robust solution that can apply broadly across many platforms and applications.
  - **Strengths:** Compelling endpoint encryption products must support the ability to extend policy-based encryption capabilities wherever it resides and wherever it travels. The most robust solutions are flexible enough to provide file-based encryption and encryption of an email body.
  - **Solitary limitations:** Encryption alone fundamentally doesn't know the criticality of structured and unstructured data. If deployed improperly, encryption can give organizations a false sense of security. It must be applied with the ability of an organization to control the encryption key.
- **Identity and information access:** A key tenet in information security revolves around the least privileged to allow access to the data for the minimum necessary number of individuals. Shared file servers commonly have access control rules set at the folder level for business units and workgroups to share data. Various other types of access control exist, blocking sensitive data being sent via email or other unauthorized file transfer solutions outside of the organization's IT boundaries, and even access control in conjunction with encryption provides policy-based access at the individual file level — a form of enterprise rights management. Once trust is established and there is a connection, identity gets out of the way when access has been granted. Identity and access management products are benefiting from a strong focus on internal policy enforcement, especially context-driven identity.
  - **Strengths:** Modern identity and information access solutions can transparently connect users to the data or other resources required to do their work. Combining identity to modern rights management controls can actually improve the user experience and reduce policy complexity. These solutions enable organizations to validate the authenticity of a person accessing data or other resources.
  - **Solitary limitations:** Identity must have the capability to understand who is granted access to specific data assets. Identity alone cannot enable the data creator from eliminating an administrator from accessing it. If identity were functioning alone, an organization could not encrypt intellectual property and only give access to the legal team.

A fundamental best practice is to protect data through encryption, access controls, and data loss prevention, but organizations often struggle to integrate these core functions seamlessly. When each of these data protection and security controls is applied separately, as they have been in the past, the limitations of their effectiveness are enhanced. Only when deployed cohesively can they enable IT security teams to pivot from a perimeter-based approach to a strategy that holds data protection at its core. Security must support secure collaboration and sharing and be done in a centrally managed way that doesn't introduce more complexity.

Each of the controls certainly complements the others, with encryption essentially serving as the glue. For comprehensive data protection in the cloud that also encompasses mobility, security requires control of the entire stack — networks, devices, and so on — to create a layered defense. With the cloud, organizations do not have control over things such as storage, thereby hindering defense in depth. For these scenarios, the only place organizations can establish a perimeter is around the data (i.e., take an information-centric approach).

CONSIDERING SYMANTEC

Mountain View, California-based Symantec has strong reputation globally, and today, the company has more than 11,000 employees, operating in 48 countries. Symantec is one of the few early market constituents that continues to lead the security software market in both the consumer and the enterprise sectors. The enterprise security product segment includes Secure Socket Layer (SSL) Certificates, authentication, mail and web security, datacenter security, data loss prevention, information security services, endpoint security and management, encryption, and mobile security offerings. In detail:

- **Symantec Data Loss Prevention:** Symantec has held a leadership position in data loss prevention since its acquisition of Vontu in 2007. New features and capabilities have been added regularly, making Symantec DLP one of the most, if not the most, robust DLP solutions on the market. It supports full data loss prevention capabilities, including the ability to discover sensitive data in structured and unstructured sources and support full DLP capabilities at the endpoint, on network file shares and in the cloud. It provides full DLP monitoring and protection capabilities for corporate email regardless of whether it's hosted in a conventional on-premise email or a SaaS email service. Symantec recently added discovery and monitoring capabilities for Box, Gmail for Work, and Microsoft Office 365 Exchange Online. In addition, DLP controls can now be extended to 60+ cloud applications using DLP's cloud connector and Elastica (CASB). It also provides full support for both iOS and Android devices.
- **Symantec Endpoint Encryption and key management:** Symantec Endpoint Encryption and Symantec Encryption Desktop provide file and folder encryption based on Symantec's acquisition of PGP in 2010 and have since been tightly integrated with the company's data loss prevention platform. Customers can benefit from full disk, removable media, and email encryption capabilities. The centralized key management solution has automated policy controls and provides individual and group key management. In addition, file share encryption enables business teams to securely share documents on internal and cloud-based file servers automatically and incorporates file server access controls for strong end-to-end encryption and access through iOS and Android mobile devices.
- **Symantec VIP Access Manager:** Symantec's VIP Access Manager integrates single sign-on (SSO) with authentication, access control, and user management. It provides context-based identity policies to enable administrators to provide granularity by group, device, or IP range. It integrates with the Symantec VIP agent to support mobile users with strong authentication.

- **Symantec Information Centric Encryption (ICE)**: ICE is an innovative technology from Symantec that provides the centralized management needed to enable administrators to get a visual indication of the location of sensitive data assets. Using ICE, administrators can click on the audit trail created by users on both desktops and mobiles (via the Symantec VIP agent), with support for strong authentication. The identity agent becomes the authentication broker and is the first policy enforcement mechanism, calling back to ICE every time someone attempts to access a sensitive file. It can act as the decryption broker to enable access to an encrypted file, and it establishes an audit trail for file access. Should the file get into unauthorized hands, ICE provides the ability to revoke the file. In addition, administrators have the option to use on-premise encryption key store, offering full control over keys that secure critical organization data.

CHALLENGES AND OPPORTUNITIES

Symantec has the core capabilities that, when properly deployed and configured, can synergistically support information-centric security without introducing additional complexity or end-user disruption. Symantec acquired market-leading data protection offerings and has maintained its market leadership by providing consistent updates to support mobile and cloud data protection as sensitive corporate applications continue to be moved off-premise to Salesforce, Box, Office365, and other applications. IT security buyers interested in leveraging Symantec's data protection portfolio should consider the following cautions:

- Symantec is in a position to be a data security powerhouse and should be an attractive option for organizations seeking support for an information-centric approach to security. With that said, Symantec's strategy appeals most to organizations that have adopted the company's robust data loss prevention platform. Organizations — especially those that may have customized their Symantec DLP deployment — should consider the added cost and potential disruption associated with combining DLP with encryption and access management capabilities. Automation, control, and visibility should be the outcome of fully embracing Symantec's approach, but the process to get there takes time, commitment, and leadership from IT, business data owners, and senior management.
- Symantec acquired Blue Coat in 2016, integrating the Blue Coat products into Symantec's current portfolio. Symantec DLP Cloud and Symantec Cloud Data Protection leverage the Blue Coat functionality to discover sensitive data in 60+ cloud applications, including Office 365, Box, and Dropbox; apply encryption or tokenization; and use the Blue Coat gateway to enforce encryption/tokenization actions from DLP policies. Enterprises that invested in other cloud security gateway solutions may not gain the full functionality achieved from the tightly integrated solution.
- Symantec's information-centric solution, while a file format-agnostic solution, is an alternative standard to Microsoft, which maintains a proprietary nature of its approach. Microsoft has greater resources to move the market in its direction. With that said, enterprises that adopt the Symantec ICE solution should keep their eyes on the product road map and commitment of Symantec executives to this strategy. Symantec plans to publish its APIs and SDKs to create a broader ecosystem of third-party developers that can consume the Symantec ICE service.

CONCLUSION

As the amount of data being created, shared, and consumed skyrockets, IT security professionals face a significant challenge in keeping pace with identifying and protecting critical assets to reduce the risk of data loss or exposure. The siloed security investments made in the past with respect to data loss prevention, identity management, and encryption compound the challenge by adding complexity to IT architectures. Information-centric security that binds the major controls for data protection creates enough cohesiveness to scale in increasingly distributed corporate environments.

A data discovery exercise needs to be comprehensive and supported with a solution that can crawl endpoint devices and networked data stores throughout the distributed corporate environment. IT security professionals should ensure that data classification and protection are integrated into the risk assessment process. Identify and assign classification levels to data types within the organization. Consider solutions that automate this process and enable business users to classify data as it is created. Determine the location and affiliation of sensitive data with users and applications, and identify acceptable use cases based on this information.

Choose solutions that automate data protection by tightly integrating data loss prevention, access controls, and encryption or data obfuscation technologies. Together these security technologies can assist security teams by supporting policies that are based on knowledge of a password, identity of the user, nature of the content, time intervals, deadlines, and so forth. Data protection should no longer be limited to a single, rigid corporate network. An information-centric solution set should support data governance policies wherever data resides and wherever it travels. The controls must "follow the data" wherever it goes.

The cohesive solution set should also reduce complexity and enable IT teams to understand the various use cases in which data could be transmitted over untrusted networks and should be detected and encrypted so that the legitimate action can continue with stronger security. Modern encryption solutions should have a key-sharing capability that can be linked to DLP solutions for this purpose.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com