FORCEPOINT
POWERED BY Raytheon

Whitepaper

Data Theft Prevention

THE KEY TO SECURITY, GROWTH AND INNOVATION

EXECUTIVE SUMMARY

Data security tools and best practices continue to evolve, yet the losses attributed to data breaches continue to outpace data defenses. In 2014, data breaches compromised over 700 million records, with financial losses estimated to be at least $400 million. Even harder to put a price tag on is the damage caused to the company's brand and reputation after their data was stolen. Despite heavy investments in data security, many organizations found out the hard way that the point and current signature-based solutions do very little to stop advanced cyberattacks.

Industry and world leaders are calling upon the C-suite and governing boards to drive the much-needed change toward making cybersecurity a top priority. At the same time, security leaders need to keep their teams focused on the overall objectives of their cybersecurity investment. Fixating on the latest "cool technology" or getting distracted by the latest media-hyped threat does not help IT teams raise their organizations' level of data security.

Instead, IT teams need to adopt a more holistic approach to protecting their critical data. Cybersecurity from a Data Theft Prevention perspective is broader in scope, more intelligent in application and more effective in defending your critical data. Such a data-centric posture is an enhancement to data defenses, as it ensures that data is secured from inbound as well as outbound threats. Thus, Data Theft Prevention encompasses the entire security posture, not simply data loss prevention (DLP).

Additionally, organizations' IT teams must accomplish these data security objectives while also realizing the other two goals of IT, which are to help the organization both grow and innovate. Too often, these last two objectives become lost in the efforts to protect against data theft. But the fact is that IT, and the critical data that it manages and protects, exist to serve the organization by enabling it to adopt new technologies, evolve processes and maintain its competitive advantages in the marketplace.

In 2014…data breaches compromised over 700M records, with financial losses estimated to be at least $400M

THE YEAR OF DATA BREACHES AND BEYOND

The massive, high-profile data breaches last year that resulted in costly data theft incidents for major financial institutions, healthcare providers, government agencies, retailers and other organizations are just the beginning of a long-term trend. The lure of easy and substantial financial gain as well as the explosion in the number of threat actors all but guarantees that this costly data theft trend will continue. And though they occurred in a variety of different industries, the major data theft incidents of 2014 were traced to one or more of the three following main causes:

- Malicious attacks and data theft by external actors
- Accidental leaks of critical information through user error and broken business processes
- Insider data theft for financial, political, vengeance or other motivations

These three main data threat sources have allowed threat actors to become wildly successful in breaching the defenses of even the most heavily security-invested organizations. IT teams clinging to old ways of thinking about data defense and static security tools are simply making their critical data an even more vulnerable target for theft. This reality jibes with the Price Waterhouse survey that reports data security incidents grew 66% in 2014.

Security incidents grew 66% in 2014

For example, hackers found ways to exploit new technologies and gain access through trusted third parties as well as via sophisticated, socially-engineered lures. All of these methods of breaching data security were successful either singularly or as a combination. This new challenge of rising threats and highly successful attack methods puts even more pressure on IT defenses to incorporate real-time analytics on inbound and outbound traffic to detect potential threat activity.

DATA THEFT PREVENTION AND INSIDER THREAT

However, as risky as the external threat landscape has become, insider threats pose even greater risks to your critical data. Compared to intentionally stolen data, twice as much critical data is lost accidentally. Often, it's simply a case of employees and/or trusted partners inadvertently opening up new risks to your critical data as they find workarounds and pursue other "shadow IT" methods to fulfill their responsibilities.

Insider threats vary significantly and have different causes and sources. Some are without question motivated by financial reasons or personal or political conflicts with the organization. Often, however, a data breach is due to an employee inadvertently engaging in risky behavior out of habit, ignorance or both. Whatever the motivation or cause, insider threats will continue to cause devastating data losses to many organizations.

But data theft from insider threats is not just the end-user's fault. Unfortunately, data loss from internal causes and partners is often a result of IT's reputation as the "department of 'no'." This cause-and-effect dynamic must change. Data defenses need to be able to adapt to changing technology as much as the changing threat landscape to empower IT teams to be able to say "yes" to innovation and to opportunities for growth.

Compared to intentionally stolen data, twice as much critical data is lost accidentally

Data Theft Prevention defends against the insider threat by leveraging digital defenses to monitor webmail, social media, printing functions and other channels of data sharing for potential abuse. Additionally, it also puts physical defenses in place to secure USBs and other removable media. Furthermore, Data Theft Prevention allows IT teams to leverage anomalous behavior analytics to identify high risk users before any data theft occurs.

DON'T ALLOW FEAR TO STIFLE GROWTH AND INNOVATION

In this era of sophisticated attacks, rapid technological advancements and insider threats, organizations without a holistic approach to data security will struggle to find the balance between securing data and providing appropriate access. Quite understandably, fear of data loss plays a role in organizations' hesitance to adopt new technology as quickly as it otherwise would. The specter and cost of a public data breach on the level of a Sony, Home Depot, Target, Anthem and other high profile data theft cases over the last few years has had a chilling effect on leveraging cloud services like Office 365 and Box Enterprise, for example.

Yet, business needs demand that organizations regularly adopt new technologies if they are to continue to innovate and thrive. If they fail to do so, they risk falling behind their competitors, losing growth opportunities and market share, or even the ability to survive. This fear of data breach has, ironically, also been a factor in the emergence of "shadow IT" in some organizations, where employees unofficially adopt tools to perform their jobs, where and when IT departments remain unresponsive.

As noted, business demands are driving these risky responses. Roaming users have a need to access critical data from multiple locations, such as from their home office, a coffee shop or an airport. Personnel need to collaborate and share sensitive information internally and with trusted partners. Mobile devices and the emerging Internet of Things (IoT) will require data security to be adaptive. The truth is that new technology does in fact bring with it new risks, but it also brings new opportunities.

EMBRACE NEW TECHNOLOGIES WITH CONFIDENCE

Data Theft Prevention allows you to successfully embrace technological change and new opportunities while reducing risk by adding three elements to your security posture:

- Security that is adaptive and contextually aware
- Data protection that goes everywhere
- Raising the security IQ of IT teams and employees

Deploying adaptive security is an obvious and necessary response to the rapidly changing threat landscape. But it must also adapt to the changing technologies being adopted. Cloud services like Office 365, Mac endpoints and other technologies have been around for some time, yet even today, few solutions provide full support for securing data while using them.

Also, remote workers have a need to work with critical data wherever they are. But the adoption of cloud services and other collaborative tools can place your data beyond your defensive perimeter. Your critical data must be protected wherever it lives or is accessed. Your data security solutions must be able to identify, control and defend your data against theft anywhere and everywhere.

Finally, meeting the challenges of threat actors goes well beyond technological solutions alone. Organizations must invest in the ongoing training of their skilled security professionals to counter the growing skills gap. Fortunately, the current generation of users has grown up with technology such as smartphones and social media, which provides the foundation for understanding basic security principles. However, they still must be trained and regularly updated on best practices for using commonly exploited attack vehicles such as Wi-Fi, social media and email.

A HOLISTIC APPROACH TO DATA SECURITY

Data Theft Prevention forces us to think well beyond the latest threat or exciting new security technology. While there are lessons to be learned from the hype around a new, innovative threat technique, defenses must always be maintained to handle any threat, known or unknown. Becoming distracted by a shiny-new, cutting-edge defense technology has never provided long-term ROI. Cybercriminals will always find ways to go around or through them.

Too many email security solutions are not up to the task

Data Theft Prevention also addresses the need to coordinate defenses across outbound and inbound activity. Outbound defense must not only keep sensitive data from going places it should not, but should also monitor for botnet and other malicious outbound traffic. Inbound defenses are the proactive side of Data Theft Prevention, identifying threat activity indicative of an attack in progress, or even pre-attack probes and tests by an attacker. At a more granular level, IT should apply the Kill Chain as a tool to assess current Data Theft Prevention capabilities, with the added dimension of how defenses share information across the Kill Chain to identify highly evasive attacks.

This requires a change in the way we approach security in three main areas:

- Web security
- Email security
- Data Loss Prevention (DLP)

From compromised websites to malicious social media links, the web has become a primary factor in modern threats. But given the dismal track record of a malware detection focus, defending against web threats requires a coordinated defense that can analyze code and other web content in real-time, while checking for lures, redirects, exploit kits and the numerous other components of advanced threats.

For most of the major breaches mentioned earlier, investigators reported that they likely began with an email. Consequently, phishing attacks of this nature are on the rise simply because they work — the Verizon 2015 data Breach Investigations report states that 23% of the recipients opened phishing messages and 11% went as far as clicking on the link within the message. For those concerned with Data Theft Prevention, stopping a threat at the earliest stage is a priority, yet too many email security solutions are not up to the task.

Even the selection and deployment of Data Loss Prevention (DLP) plays a very significant role as part of a complete Data Theft Prevention strategy. Advanced capabilities such as OCR and Drip DLP become basic requirements. Securing Mac endpoints becomes just as important as a Windows endpoint, demanding the same capabilities when on the network as well as off–premise. And true Data Theft Prevention also demands capabilities to retain control of data stored in cloud services like Office 365, Box Enterprise, Salesforce.com, etc.

However, the full effectiveness of a unified Data Theft Prevention strategy can only be realized when the threat activity identified at various stages of an attack is correlated. Shared intelligence provides the big picture view so that multiple “suspicious” events can be correlated to identify a truly malicious threat. The validity of this holistic approach to Advanced Persistent Threats (APTs) and other advanced threats has been demonstrated by both analysts and third-party security testing organizations.

FORCEPOINT™ TRITON® APX AND DATA THEFT PREVENTION

Data Theft Prevention is a data-centric security approach that takes strategic decision-making above the noise of the latest threat or promising technology. It empowers employees as much as it secures the data at the heart of the organization. Data Theft Prevention encompasses the products, people and processes that touch data in ways that can move the organization forward. Without it, organizations remain at higher risk for a data breach.

As a unified defense, Forcepoint TRITON APX is a security platform that delivers a coordinated Data Theft Prevention solution. It monitors multiple channels for threat activity across the entire Kill Chain in order to identify malicious or suspicious inbound or outbound activity. It also provides industry-unique defensive capabilities along with support for increasingly popular technologies like Office 365 and Mac endpoints and elevates the security IQ of your IT team and employees.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

[WHITEPAPER_DTP_KEY_TO_SECURITY_EN] 200003.011416