WHITE PAPER: INFORMATION-CENTRIC SECURITY

PROTECTING YOUR DATA FROM THE INSIDE-OUT

Despite the growing number of high profile data breaches and the anxiety they’re causing organizations, too much information security spending still focuses on the prevention of attacks, while not enough has been done to improve (or simply create) information monitoring and response capabilities. The priority must shift from protecting information from the outside-in to securing it from the inside-out.

Greg Sullivan, CEO, Global Velocity
8/5/2014
WHITE PAPER: INFORMATION-CENTRIC SECURITY

PROTECTING YOUR DATA FROM THE INSIDE-OUT

When examining the effectiveness of your information security posture, consider the advice Jerry Seinfeld gave to George Costanza in the classic Seinfeld episode “The Opposite.” As George contemplates why he has no job, no wife and no prospects for either, Jerry says “if every instinct you have is wrong, then the opposite would have to be right.” George follows that advice and gets both the girl and his dream job with the New York Yankees. This same advice may well hold true for cyber security: instead of relying only on the traditional methods of securing data from the outside-in, organizations must also do the opposite and adopt an information-centric approach. This requires monitoring where files are kept, how they are moved and used, and by whom in order to prevent a breach.

In protecting data, the traditional approach is to harden the network and lock down PCs, laptops and mobile devices with antivirus software. That strategy is proving ineffective as cyber attackers grow more sophisticated and seek to steal data instead of only achieve notoriety. Consequently, it can take months, even years, to discover a breach, as evidenced by the 2013 Target breach that made headlines for the theft of millions customers’ personally identifiable information (PII). As these threats become more difficult to detect, information has never been more vulnerable. The adoption of cloud solutions like Dropbox and Salesforce, and allowing employees to use their personal devices to access information stores significantly increases the risk.

From Hacker to Thief

Years ago, the primary motivation for cyber hackers was bragging rights. They would break through an organization’s security defenses and openly boast about it to their fellow hackers. Today, cyber thieves typically share the same motivation of the businesses they’re attacking: to make money. Their tactics are more targeted and more difficult to detect for even the largest companies with sophisticated security systems and trained personnel in place, as the news headlines in 2013 demonstrate. The Target data
breach put the credit card numbers and other confidential information of millions of the retailer’s customers into the hands of cybercriminals. Attacks on companies including Adobe, Evernote and LivingSocial compromised millions of records containing PII. According to a February 2014 report from threat intelligence consultancy firm Risk Based Security (RBS), data breaches in 2013 exposed over 822 million records, nearly doubling 2011, the previous highest year on record.

Why are these attacks so effective? The answer is that they’re growing more and more difficult to detect with standard antivirus and endpoint security software solutions. Once attackers sneak past the network, they can sit unnoticed silently stealing data. The Verizon 2013 Data Breach Investigation Report finds that 66 percent of the breaches took months or even years to discover (64% months, 4 years). Compare that to Verizon’s 2012 report, which found just 56% of breaches took more than a month to be discovered.¹

One more statistic to throw at you: The Wall Street Journal on June 29, 2014 reported its own research found that 1,517 companies traded on the New York Stock Exchange or Nasdaq Stock Market listed some version of the words cybersecurity, hacking, hackers, cyber-attacks or data breach as a business risk in securities filings. That is up from 1,288 in all of 2013 and 879 in 2012.² With the headlines and turmoil these breaches caused in 2013, it’s not surprising that the topic is top of mind for businesses.

It’s important to note that not all data breaches are the result of outside hackers penetrating a network. Often information is leaked or lost by employees, either accidentally or

¹ Verizon 2013 Data Breach Investigation Report
intentionally. In these cases, antivirus and endpoint security software solutions can do little to prevent those losses.

Symantec’s recent admission that antivirus software is “dead” is an admission that the traditional approach of hardening the network and data center is growing obsolete, particularly as companies move their data to cloud-based services and enable employees to access that information remotely using their personal computers, laptops, smartphones and tablets. Encryption technology is a necessity, but is insufficient by itself. It’s still important to know where your data is stored and how it is shared and moved.

Think about how radically the business environment has evolved with the advent of cloud computing and the Bring Your Own Device (BYOD) trend. It wasn’t long ago that the majority of employees worked at the office and accessed information on servers and computers locked down by IT and behind firewalls, anti-spam and other traditional security solutions that hardened the network perimeter.

As workers became more mobile and able to work remotely, first with laptops and then on their smartphones and tablets, IT departments were forced to contend with more devices accessing information stores from outside the network. Information was still stored primarily on company servers and was accessed by logging into a virtual private network (VPN), typically a slow and frustrating experience. However, employees could also load data onto their personal devices and USB thumb drives, increasing the risk of theft or loss.

The advent of cloud computing services enabled remote workers to bypass the network and VPN entirely. Information now increasingly lives on the public servers of companies like Dropbox, Google, Salesforce and Evernote. A company can realize significant cost savings on infrastructure and IT systems management, and make collaboration among employees in remote offices and traveling all over the globe easier.

However, those benefits can carry a steep price. Network security measures can no longer prevent today’s advanced, targeted attacks. IT does not control the majority of user devices
(BYOD) or the cloud services employers use every day. When a large company endures an embarrassing and costly data breach, it will suffer financial losses and damage to its reputation. When a small company is attacked, it may never recover. An attack can set a small business back anywhere from $54,000 to $101,000 per incident. PCWorld in August 2013 reported that of the small businesses who suffered a breach, roughly 60 percent go out of business within six months after the attack.

Despite the growing number of high profile data breaches and the anxiety they’re causing organizations, too much information security spending still focuses on the prevention of attacks, while not enough has been done to improving (or simply creating) information monitoring and response capabilities. As I stated earlier, cyber attackers are in the business of information theft for profit and are driven primarily by the goal to make money. We need to drive up their cost of doing business without significantly increasing our costs. The priority must shift from protecting information from the outside-in to securing it from the inside-out, an approach I call “information-centric security.”

**Information-centric Security**

Imagine you have a security system for your house with sensors on all doors and windows and alarms that go off if anyone suspicious tries to break-in. However, you do not know exactly which filing cabinets, storage bins or closets your precious valuables and documents are stored in, or how family members use and share them. If someone is able to bypass the security system and not trip an alarm, you may not realize that a specific item the thief was targeting is gone for weeks or months, if at all. This scenario represents the traditional approach to information security.

Now imagine your alarm system can tell you exactly where every valuable is kept and provide you with a real-time view of who is handling and moving one item to a different room or even outside the house based on policies you set. The system can also alert you immediately if a single valuable is moved contrary to your policies and can prevent that from occurring, also in real-time. That’s the information-centric security model.
There is still value to hardening your network and using endpoint security software to try to keep the bad guys out, but those steps are now part of a larger strategy that must address the fact so much information is outside the company’s servers and is being accessed by so many different devices.

You must know exactly where sensitive data lives at rest, employing technologies like document fingerprinting, pattern matching, keyword dictionary comparisons that can all track digital file usage.

You should also be aware of how your sensitive data is being used in motion, and that requires pervasive monitoring to identify meaningful deviations from normal behavior that signal malicious intent. This can include examining file location, the time of day, what devices are being used, IP addresses and URL reputation.

This combination of content aware monitoring plus context aware monitoring equals information-centric security: knowing your digital assets are protected against unauthorized use, disclosure, modification, recording or destruction. It not only prevents thieves from stealing data, it also guards against the innocent employee who mistakenly tries to email confidential information to an unauthorized recipient.

Global Velocity Securio

Global Velocity’s Securio platform protects information from theft or loss whether it is stored inside the enterprise or the cloud, enabling the information-centric approach that is more effective than merely hardening points of entry to the data center and network.

Securio is available as a cloud-based software-as-a-service (SaaS), a prepackaged hardware appliance, or a combination of the two. There are four key components:
• **Discover**: inspects data storage areas at rest using document “fingerprints,” pattern matching and keyword dictionary comparisons. The digital fingerprints create a “virtual vault” that Discover uses to detect when the sensitive content, or portions of it, have been moved to unauthorized network storage locations, an indicator of possible malicious activity.

• **Protect**: defends against unauthorized data loss in motion over the Web and through email. Securio scans all outbound traffic for fingerprint, pattern, and keyword matches preventing sensitive data from being sent to unauthorized users or locations. The user defines policies that will determine if certain data is blocked, quarantined, or logged when it’s being sent.

• **Track**: constantly monitors data in use to track and record the genealogy and chain of custody of sensitive documents to identify meaningful deviations from normal behavior that point to possible malicious intent.

• **Manage**: easy-to-use and intuitive web interface showcases all of Securio’s results based on its single unified policy.

Securio provides real-time consolidated reporting and analysis across users and devices no matter their location. This enables companies to detect and prevent a breach or data loss without limiting employees from using their preferred devices and cloud-based services that sit outside the company network.

*Figure 1: Securio is available as a Software-as-a-Service*
Additionally, every business large or small should have a comprehensive security training program in place for employees. This involves not leaving files open or unattended, and making sure to lock or shut down unsecured devices like a smartphone or tablet. Also, classify your employees based on what they can and cannot access on the company system. Not everyone needs to have access to all cloud applications. Additionally, each employee should have a different and strong password for all accounts or services.

Traditional antivirus software may not be entirely “dead,” but the practice of solely relying on it to protect your data stores is. It simply cannot keep the bad guys out, and when those attackers do break through the network security system, they can sit quietly for months or even years stealing data before they’re discovered and the damage is done. The fact organizations are moving more information to cloud or SaaS-based services and permitting employees to access that information with their own personal devices makes an attacker’s job easier and increases the risk of accidental loss or deletion by a well-meaning employee. Instead of fighting to keep the attackers out and prohibiting the use of cloud computing applications or forcing employees to use costly IT-issued laptops and smartphones, adopt an information-centric approach that enables real-time monitoring of data at-rest or in motion to better protect against a breach.
About Global Velocity

Global Velocity provides affordable and easy-to-use information security solutions that allow companies to protect their most valuable digital assets and brands from loss or misuse, while assisting them in maintaining their compliance, audit and security obligations. This proven next generation cybersecurity software is scalable and extendable for deployment in both enterprise and cloud environments.

Global Velocity is made up of a world-class team with experience in designing cyber security solutions for U.S. government defense and intelligence operations. Learn more at www.globalvelocity.com and follow @GlobalVelocity on Twitter. Phone: (314) 588-8555

2013 Red Herring Top 100 Global Winner