WHITE PAPER

Are Users the Achilles' Heel of Security?

Presaging the Death of an Industry or a Path to User Activity Monitoring Enlightment?

By Mark Bloom
Product Marketing Director, Security & Compliance
Sumo Logic

John Chamber, ex-CEO of Cisco, once said that there are two types of companies, those who have been hacked and those who don't yet know they have been hacked? Consider for a moment, the following statistics:

- There were 783 **major** breaches in 2014 [1]
- This represents a 30% increase from 2013 [2]
- Median number of days before detection: 205 [3]
- Average number of systems accessed: 40
- Valid credentials used: 100%
- Percentage of victims notified by external entities: 69%

Large enterprises are finally coming to the conclusion that security vendors and their solutions are failing them. Despite the unbelievable growth in enterprise Security spend – see figure 1 - organizations are not any safer.

And security attestations like PCI and HIPAA, while helping with compliance, are not equated with a stronger security posture.

Don't believe it? Take a look at the recent announcement from Netflix where they indicated they are dumping their anti-virus solution. And because Netflix is a well-known innovator in the tech space, and the first major web firm to openly dump its anti-virus software, others are likely to follow.

Even the federal government is jumping into this security cesspool. In a recent U.S. appellate court decision, the Federal Trade Commission (FTC) was granted authority to regulate corporate cybersecurity. This was done because the market has failed and it was necessary for the government to intervene through public policy (i.e. regulation or legislation).

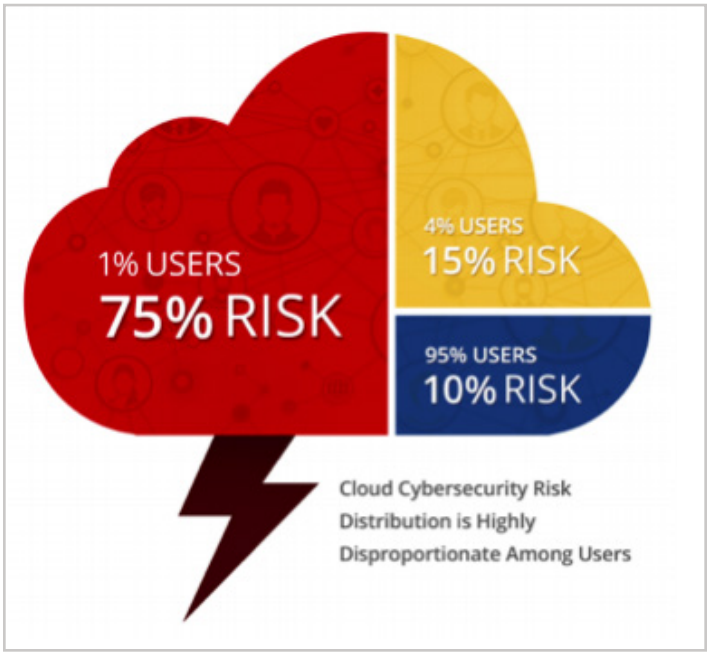
Figure 1: Growth in Security Solutions

Research has indicated that security solutions are rarely successful in detecting newer, more advanced forms of malware, and scans of corporate environments reveal that most enterprises are already infected.

"Enterprises are recognizing that adding more layers to their security infrastructure is not necessarily increasing their security posture," said George Gerchow, Product Management Director, Security and Compliance at Sumo Logic. "Instead of just bolting on more and more layers, companies are looking for better ways to tackle the problem."

While security has gotten better over the years, so too have the bad actors, whether cybercriminals, hacktivists or nation states. Malware-as-a-service has made this was too easy and pervasive. You know the bad guys are going to find ways to penetrate any barrier you put up, regardless if you are running physical, virtual or cloud (PVC) infrastructures. So is all hopeless, or is there a path to enlightenment by looking at this problem through a different lens?

According to a new report from CloudLock, Cybercriminals continue to focus their efforts on what is widely considered to be the weakest link in the security chain: the user. According to CloudLock CEO Gil Zimmerman, "Cyber attacks today target your users—not your infrastructure. As technology leaders wake up to this new reality, security programs are being reengineered to focus where true risk lies:



with the user. The best defense is to know what typical user behavior looks like – and more importantly, what is doesn't."

And the ROI of this approach is huge, because the report – which analyzed user behavior across 10M users, 1B files and 91K cloud applications – found that 75% of the security risk could be attributed to just 1% of the users. And almost 60% of the apps installed are conducted by highly privileged users.

Given these facts, and that cybercriminals always leverage these highly coveted, privileged user accounts during a data breach, understanding user behavior is critical to improving one's security posture.

"As more and more organizations deploy modern productivity tools like Microsoft Office 365, Google Apps and Salesforce.com, not understanding what users are doing injects unnecessary and oftentimes unacceptable business risk," said Mark Bloom, Product Marketing Director, Security & Compliance at Sumo Logic.

Leveraging activity-monitoring APIs across these applications, it becomes possible to monitor a number of activities that help in reducing overall risk. These include:

- Visibility into user actions and behaviors
- Understand who is logging into the service and from where
- Investigate changes made by administrators
- Failed/Valid login attempts
- Identify anomalous activity that might suggest compromised credentials or malicious insider activity
- Tokens: Information about 3rd party websites and applications that have been granted access to your systems

This new, emerging field of User Activity Monitoring (UAM) – applied to Cloud Productivity and Collaboration Applications - can really help to eliminate guesswork using big data and machine learning algorithms to assess the risk, in near-real time, of user activity. UAM (sometimes used interchangeably with user behavior analytics – UBA) employs modeling to establish what normal behavior looks like and can automatically identify anomalies, patterns and deviations that might require additional scrutiny. This helps security and compliance teams automatically identify areas of user risk, quickly respond and take actions.

"As more and more organizations deploy modern productivity tools like Microsoft Office 365, Google Apps, and Salesforce.com, not understanding what users are doing injects unnecessary and often times unacceptable business risk."

Mark Bloom, Product Marketing Director, Security & Compliance
Sumo Logic

Sumo Logic applications for Office 365, Salesforce, Google Apps and Box brings a new level of visibility and transparency to activity within these modern day, cloud-based services. And once ingested into Sumo Logic, customers are then able to combine their activity logs with logs from other cloud solutions and on-prem infrastructure, to create a single monitoring solution for operations, security and compliance across the entire enterprise.

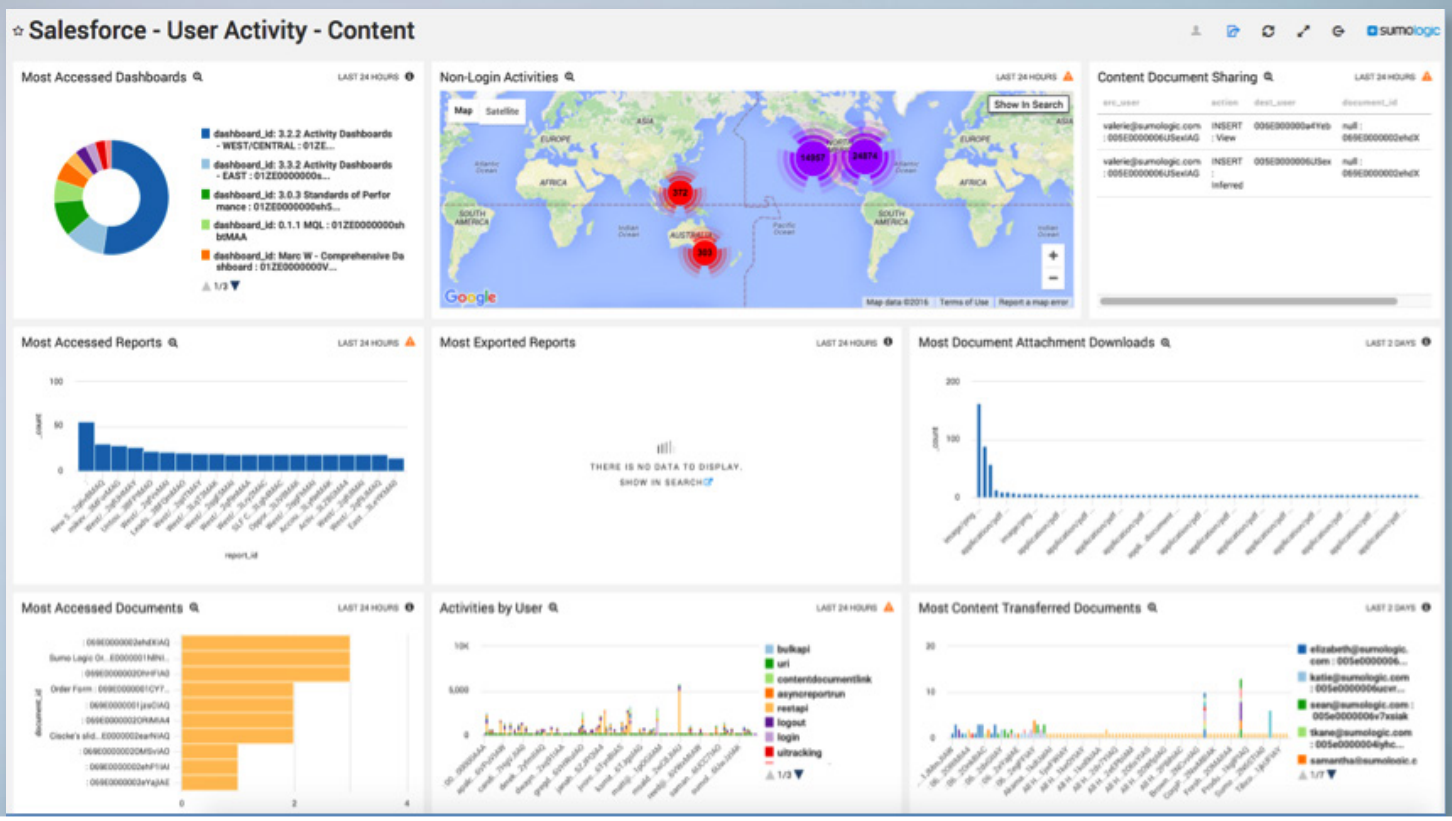
Enable cloud productivity without compromise!

Sources:

[1] Identity Theft Resource Center (ITRC) Report

[2] http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

[3] Mandiant M-Trends Report (2012 -2015)



Toll-Free: 1.855.LOG.SUMO | **Int'l:** 1.650.810.8700
305 Main Street, Redwood City, CA 9460

www.sumologic.com