A CyberEdge Group White Paper

January 2016

Users Pose Greatest Threat to Enterprise Security

Embrace the Power of Security Analytics to Address the Cyber Dilemma

Licensed by:

sumologic

CYBEREDGE GROUP

EXECUTIVE SUMMARY

The number and complexity of cyberattacks penetrating today's enterprises continue to escalate. Malicious actors, increasingly sophisticated tactics, and targeted, stealthy exploits litter the cyber landscape and regularly circumvent the defenses put in place to block them. Continuously scrambling to architect a formidable response to this dynamic and daunting onslaught, security professionals add layer upon layer to the security infrastructure stack. Put another way, companies continue to spend billions of dollars on security solutions, but high-profile news stories about the latest breaches repeatedly expose the futility and struggle to mitigate these risks and improve an organization's security posture.

Today's digital ecosystem and disruptive business models empower not only the innovative enterprise, but also the enemy. Constant connectivity, cloud infrastructure, continuous delivery tools, mobile apps and big data magnify the attack surface and risk exposure. An objective look at the scorecard in the battle between adversaries and victims mandates the need for a new approach to flip the balance of power in favor of the enterprise. Savvy cybersecurity initiatives will focus on users as the most critical element of the equation. People—not systems—own the keys to the kingdom, and only through monitoring, analyzing and changing user behavior will today's enterprises start winning the war against increasingly elusive cybercriminals.

CURRENT SECURITY SOLUTIONS FALL SHORT

Many enterprises continue to invest heavily in traditional security defense technologies, but most organizations are being breached, and many experience significant damages associated with compromised data, tarnished brand reputation, diminished customer/shareholder confidence and lost revenue.

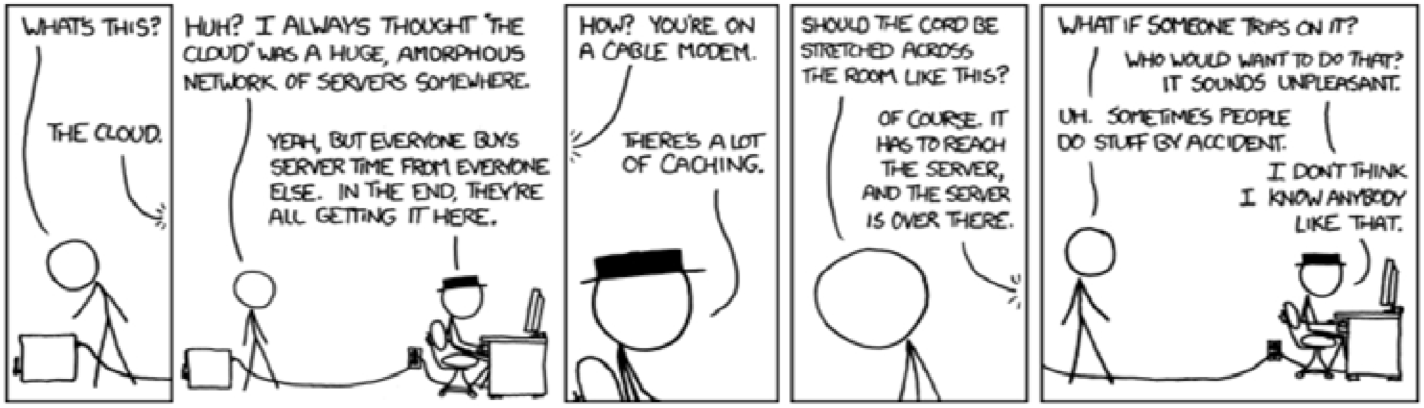
Some enterprise security teams believe that more security equals better security, or that as long as the organization adheres to regulatory requirements, it will avoid catastrophe. But adding layers to the security infrastructure doesn't necessarily correlate with a powerful cybersecurity posture. And the minimum security requirements mandated by compliance regulations are not scalable and do not encompass the comprehensive defense-in-depth strategy required to minimize damage from today's inevitable cyberattacks. In addition to this limited perspective that results in ineffective approaches to cybersecurity, many companies lack real-time threat visibility. Most enterprises do not discover breaches until months after they happen, and notifications regarding attacks typically come from third parties versus internal monitoring mechanisms. It's time to look at the cybersecurity dilemma through a new lens.

Despite security investments, the average time from infection to detection was 204 days in 2014.

-Mandiant M-Trends 2015 Report[1]

INSIDER THREAT: USERS CONTINUE TO JEOPARDIZE THE ENTERPRISE

Protecting data assets is a key component of effective cybersecurity, but people remain the weakest link in the cyber chain and the strongest magnet for hackers. With a single click, an employee can obliterate existing security mechanisms and essentially take down the organization. It only takes one person to infect a company. Even the best-intentioned users make mistakes. Typically, they inadvertently violate data protection policies and expose corporate systems to threats by downloading malware, which then moves laterally across the infrastructure looking for the most valuable data, infecting systems at it traverses the network, and often causing irreparable damage.


WHAT'S THIS?
THE CLOUD.
HUH? I ALWAYS THOUGHT "THE CLOUD" WAS A HUGE, AMORPHOUS NETWORK OF SERVERS SOMEWHERE.
YEAH, BUT EVERYONE BUYS SERVER TIME FROM EVERYONE ELSE. IN THE END, THEY'RE ALL GETTING IT HERE.
HOW? YOU'RE ON A CABLE MODEM.
THERE'S A LOT OF CACHING.
SHOULD THE CORD BE STRETCHED ACROSS THE ROOM LIKE THIS?
OF COURSE. IT HAS TO REACH THE SERVER, AND THE SERVER IS OVER THERE.
WHAT IF SOMEONE TRIPS ON IT?
WHO WOULD WANT TO DO THAT? IT SOUNDS UNPLEASANT.
UH. SOMETIMES PEOPLE DO STUFF BY ACCIDENT.
I DON'T THINK I KNOW ANYBODY LIKE THAT.

Source: xkcd[2]

Exacerbating this human error is the advent of the cloud. The ongoing competitive quest for agility, productivity and innovation is leading many businesses and millions of users to go beyond traditional on-prem boundaries and tap into the promised land of the cloud. According to the IDG Enterprise 2015 Cloud Computing Survey[3],nearly two-thirds of today's companies are using some form of cloud services.

Software-as-a-Service (SaaS) and cloud-based business applications revenue will grow from $13.5 billion in 2011 to $32.8 billion in 2016.

-Gartner's Forecast Analysis: Enterprise Application Software, Worldwide, 2011-2016[4]

Software-centric businesses are reshaping the technology landscape, driving continuous innovation, and facilitating rapid delivery cycles by leveraging cloud-based resources. Employees are using corporate systems to access cloud-based platforms and productivity apps like Office 365, Salesforce, Box and Google Apps. This exposes the enterprise to new attack vectors. Cybersecurity defense must be extended to protect sensitive data in these public cloud apps. Organizations that deploy security mechanisms to monitor user activity in the cloud and master the resulting data can confidently adopt game-changing technologies and seize the ability to continuously innovate without compromise.

"Like it or not, our architectures continue to move to the cloud. In order to secure the future, we need to understand where we are failing in securing the present, as evidenced by one-after-the-other media-worthy breaches. If we, as security practitioners, are not prepared to adopt the economics, scalability, power and embedded security offered by cloud infrastructure, we will be made irrelevant."

-Joan Pepin, Vice President of Security/CISO, Sumo Logic

How can organizations maintain contextual visibility of cloud activity to get a handle on what's happening on their systems and ensure protection of vital assets? Securing cloud activity doesn't require a radical, revolutionary approach. It's more about revisiting and enhancing fundamental measures like access controls and user monitoring to "catch up" with advanced architectures that have outgrown the security paradigms that govern them. Understanding, monitoring and controlling user behavior are the best tactics to mitigate user risk, strengthen resilience, and improve the enterprise's security posture.

USER-CENTRIC SECURITY: FOCUS ON BEHAVIOR AND ACTIVITY

Organizations must keep a finger on the pulse of all user activity—who is doing what, when, from where, and on what devices. In addressing the lurking danger within, for starters, enterprises will want to reevaluate and likely implement more stringent user access restrictions. Every individual employee, contractor, customer and partner with access to the corporate network represents a risk. What data assets are current and former employees authorized to access and/or modify? A process should be in place to ensure that system and data access for those who are no longer employed by the company ceases the moment the cord is cut.

Are current access control policies adequate for all defined roles and user groups? Each group accesses different levels and types of information, and therefore poses a different level of risk to the organization. Users must be properly restricted according to job function and responsibilities, granted access to only the "need-to-know" proprietary information required to effectively achieve their objectives. Security applications should immediately identify suspicious logins during authentication, abnormal traffic on the network, and unauthorized access to systems. Discovering who is accessing sensitive data in unusual ways helps the organization lock down critical assets.

What about outsiders who become insiders? How are privileged user credentials managed since these accounts are the most vulnerable to exploitation? It is critical to stop malicious intruders from stealing credentials, masquerading as legitimate insiders, and gaining access to valuable assets. The only way to do this is by proactively monitoring behavior to identify suspicious activity. Enterprises must do what's necessary to gain greater visibility into user activity patterns and find the bad guys faster.

"There's a universal truth regarding every cyber-attack: attack behavior never appears normal. This seemingly simple fact holds true whether the attack was executed by a first-timer or perpetrated by a nation-state and is crucial to preventing future information security breaches like Anthem's."

-Behavioral Analysis Could Have Prevented the Anthem Breach (***Forbes***, February 24, 2015)

Behavioral analysis begins with defining acceptable behavior and then monitoring users to detect unusual activity that injects unacceptable risk. This involves recognizing meaningful patterns and characteristics of expected and appropriate activity within defined user groups, enabling quick detection of anomalies that may indicate an attack and therefore require attention. Monitoring and analyzing user activity allows the enterprise to detect malicious behavior on the part of either legitimate insiders or the outsiders who mimic them. Non-malicious users can pose huge risks to the organization and distract attention from the real criminals. Rapid exposure of unacceptable behavior provides organizations with the insight needed to flag well-intentioned users for training, and hence prevent repeat offenses. Education is one of the best places to start in combatting insider threat. Training must include frequently targeted senior managers with high-privilege access, who should also be called upon to implement and enforce user policies.

"The fact that you'll always have users who will click on anything doesn't absolve you from trying to educate. In fact, current evidence shows you cannot be a successful defender without a top-notch user education program."

-Roger Grimes, *InfoWorld*[5]

ELIMINATE GUESSWORK: SIMPLIFY SECURITY MONITORING AND ASSESS RISKS IN REAL TIME

The explosive growth in volume, variety and velocity of security data has made it increasingly challenging for companies to focus on the most critical breaches and transform information into proactive business insights and opportunities. Sophisticated enterprise security analytics tools and technologies are available to help organizations extract, correlate, and harness the power of essential knowledge and actionable intelligence from the data tsunami. Robust user-centric security solutions will feature the following capabilities and characteristics.

360-Degree User Behavior Analytics and Activity Monitoring:

- Finds dynamic threats before they become intrusions using cloud-based predictive and scalable analytics platform
- Scales to ingest, integrate and analyze large volumes of data from all sources for a composite view of all on-premises devices, networks and systems, cloud and mobile apps, content delivery networks, etc.
- Displays on dashboard what users are doing and the devices they are using in real time
- Detects anomalies across environment as they occur—without relying on rules, queries or human input—and immediately notifies security teams, enabling instant response
- Employs machine learning algorithms to automatically identify changes in behavior on devices and in apps
- Automatically spots when a particular user behavior deviates from normal patterns or a device communicates on a new protocol or with an external IP address
- Reduces millions of data streams into a handful of meaningful patterns that reveal the user behavior anomalies that matter most, facilitating faster troubleshooting and resolution

- Exposes both insider and outsider impending threats by continuously monitoring activity patterns and calling out deviations based on individual user history and peer behavior
- Detects and flags potentially malicious activity
- Leverages situational awareness to rapidly detect bad actors and predict security infractions before major damage occurs
- Enables high-speed forensics to uncover evidence of unknown security incidents, preventing large-scale breaches from causing significant impact
- Identifies when former employees try to access corporate or cloud-based applications by integrating with Active Directory and other HR applications
- Continuously audits user and admin activity in the cloud, such as how Google calendars and Google Drive documents are modified and shared
- Ensures that not a single user on the network is doing anything he or she is not permitted to do

Implementing user alerts triggered by suspicious behavior raises awareness of security policies and reminds users what constitutes good and bad practice.

-12 Steps to Future Proofing Your Internal Security (IS Decisions, 2015)[6]

LEVERAGE USER-CENTRIC SECURITY TO MINIMIZE DAMAGE

Traditional networks are rapidly becoming extinct. The boundaries of the digital playground are bursting. Protecting this expansive and increasingly vulnerable distributed environment requires conceptualizing and implementing an exponentially more scalable cybersecurity paradigm. Believing the enterprise can prevent malware from penetrating critical applications and infrastructure can get you into trouble. The future is uncertain, but one thing we do know is that cyberattacks will continue to occur with growing frequency. Every large organization has been or will be breached... and will be victimized on more than one occasion. Savvy cybersecurity strategies will focus less on preventing every attack and more on deploying strategies and technologies that deliver a 360-degree, real-time view of user activity and behavior. This expanded visibility enables early detection, continuous vigilance and nonstop mitigation, preventing worst-case scenarios precipitated by cyberattacks, and protecting the enterprise from newsworthy intrusions and damage.

Footnotes

1. https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf

2. http://www.xkcd.net/908/

3. http://www.idgenterprise.com/report/2015-cloud-computing-study

4. http://www.softwarestrategiesblog.com/category/gartner/

5. http://www.infoworld.com/article/2920804/security/get-real-about-user-security-training.html

6. http://www.isdecisions.com/12-steps-to-future-proofing-your-internal-security/

About Sumo Logic

Sumo Logic is a secure, cloud-native, data analytics service, delivering real-time, continuous intelligence across an organization's entire infrastructure and application stack. Visit Sumo Logic to learn more about scalable enterprise security analytics solutions that can help quickly detect and investigate cyberattacks, as well as monitor and analyze user behavior, to ensure business growth without increasing risk to the organization.

About CyberEdge Group

CyberEdge Group is an award-winning research, marketing, and publishing firm serving the needs of information security vendors and service providers. Our expert consultants give our clients the edge they need to increase revenue, defeat the competition, and shorten sales cycles.

CYBEREDGE GROUP

CyberEdge Group, LLC
1997 Annapolis Exhange Pkwy
Suite 300
Annapolis, MD 21401

800.327.8711
info@cyber-edge.com
www.cyber-edge.com

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of CyberEdge Group, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice.