IDENTITY SOLUTIONS: Security Beyond the Perimeter
IDENTITY SOLUTIONS: Security Beyond the Perimeter

AUTHORS
John Yeoh
Hillary Baron

EDITORS:
Frank Guanco

ABOUT THE CLOUD SECURITY ALLIANCE

The Cloud Security Alliance is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. For further information, visit us at http://www.cloudsecurityalliance.org and follow us on Twitter @cloudsa.

ABOUT CENTRIFY

Centrify is a leader in securing enterprise identities against cyberthreats that target today’s hybrid IT environment of cloud, mobile and on-premises. Centrify helps protect against the leading point of attack used in data breaches—compromised credentials—by securing an enterprise’s users as well as its privileged accounts. For more information, visit https://www.centrify.com and follow us on Twitter @Centrify.
TABLE OF CONTENTS

Authors .................................................................................................................. 3

Executive Summary ............................................................................................. 5

Security Solutions ............................................................................................... 6

Protecting Users .................................................................................................. 8

Big Data Solutions ............................................................................................... 9

Data Breaches ....................................................................................................... 10

Investing In A Full Identity Security Platform .................................................... 11

Survey Respondents ........................................................................................... 12
IDENTITY SOLUTIONS: Security Beyond the Perimeter

EXECUTIVE SUMMARY

Cloud solutions continue to be adopted at a rapid rate as Cloud Service Providers offer flexible computing and storage needs, easier collaboration with internal users and customers, added security features, and more; allowing organizations to focus on their core business functions. This new cloud landscape also adds complexity with more people having access to company data. Protecting this data becomes crucial to business as the cost of a data breach is greater than ever. In addition to the value of the data lost, company reputation, legal action, financial penalties, and jobs are at stake. Thinking outside the traditional security perimeter is necessary to protect information from the growing list of threats. Controlling the access to data allows companies to embrace cloud services and technologies.

In February of 2016, the Cloud Security Alliance released “The Treacherous Twelve: Cloud Computing Top Threats in 2016” which revealed the top concerns expressed by IT security professionals in cloud computing. Data Breaches, Account Hijacking, and Malicious Insiders all rated as top threats. The enabling of these attacks can occur because of a lack of scalable identity access management systems, failure to use multifactor authentication, insufficient password use, and a lack of ongoing automated rotation of cryptographic keys, passwords, and certificates. As a result, these deficiencies can enable unauthorized access to data and potentially catastrophic damage to organizations and end users. It was not surprising to find that Insufficient Identity, Credential, and Access Management was listed as the top vulnerability in the report.

The goal of the Identity Solutions: Security Beyond the Perimeter survey was to address Insufficient Identity, Credential, and Access Management and gain a better understanding and perception of enterprise security in the evolving Information Technology (IT) world.

KEY FINDINGS INCLUDE:

- Of those who indicated their company reported a data breach, 22 percent of respondents were due to compromised credentials.
- Surprisingly, there were no significant differences in security solutions used between respondents who reported a breach and those who either did not report or did not know of a reported breach in their organizations.
- Companies embracing big data solutions also consistently adopted more perimeter and identity security solutions.
- 76 percent of internal access control policies extended to outsourced IT, vendors, and other third parties.
SECURITY SOLUTIONS

Perimeter-based security protects a company network along exit and entry access points. Generally, respondents indicated that their companies employed several of these solutions to protect their network. Only 1.5 percent of respondents indicated that they don’t know or don’t use any perimeter-based security solutions. Antivirus, email spam filter, VPN, and next-generation firewall were used by over 70 percent of respondents demonstrating that overall companies are utilizing several of these perimeter-based protections, on average companies utilize 3-4 solutions.

Notably, smaller companies ranging in size from 1-1000 employees were less likely to have MDM/EMM, Next-Generation Firewalls, VPN, and WAF than their larger counterparts. The cost of additional services may play a factor in adoption with smaller companies. As companies scale in size and user base, information has a broader reacher and protecting this information should be more of an emphasis. Adversaries don’t always target specific groups but deploy massive attacks exposing the weakest link in a security system. Exploiting sensitive data can damage all companies just the same. Additionally, individuals in the Americas (83 percent) were significantly more likely to utilize VPN than those in the APAC Region (73 percent) but ten percent.

As cloud solutions are adopted, defining a perimeter to secure becomes more difficult and protecting company data involves a new approach. With the growing level of devices and people accessing the data, data can be lost due to accidental or malicious activities. Controlling the cloud environment ensures that individuals only have access to the data they need. 93 percent of respondents use these access control solutions.

On average, companies utilized 2-3 access controls. Multi-factor authentication is utilized by 74% of companies, the remaining access controls were utilized by about 50% of the companies. Mac management was utilized by 18%. In general, these methods are used less frequently when compared with

WHAT PERIMETER-BASED SECURITY SOLUTION(S) DOES YOUR COMPANY EMPLOY TO PROTECT IT’S NETWORK? (Choose all that apply)

- Antivirus: 90%
- Email Spam Filter: 82%
- MDM/EMM: 48%
- Next-Generation Firewall: 70%
- VPN: 82%
- WAF: 40%
- Other (please specify): 10%
perimeter-based solutions.

Companies from the Americas are more likely to have web and SaaS SSO in place when compared with companies from APAC (62%, 42% respectively for a 20% difference). Unsurprisingly, companies larger than 5,000 employees were more likely to report using each of these solutions when compared with smaller companies. The only exception was Mac management which was not reported to be utilized by a larger percentage of companies of any size.

WHAT ACCESS CONTROLS/PROCESSES DOES YOUR COMPANY HAVE IN PLACE TO PROTECT END USERS? (Choose all that apply)

- Web and SaaS SSO: 55%
- Enterprise App SSO: 53%
- Multi-factor Authentication Tokens and Management: 72%
- Enterprise Mobility Management: 50%
- MAC Management: 18%
- Other (please specify): 4%
PROTECTING USERS

Access controls and processes help organizations manage users allowing proper access to company data. These solutions also allow users to access tools and collaborate easier and protect the users from outside threats. Companies frequently embrace privileged access management, but were much less likely to utilize the other available options like shared account password management, superuser password management, privileged session management, and privileged session recording and monitoring.

Larger companies with over 50,000 employees were more likely to use each of these controls when compared with companies with fewer than 30,000 employees. This was particularly true for the privileged access management and privileged session management.

For companies that implement privileged access management solutions to protect private users, only 76 percent extended this to outsourced IT, vendors, and other third parties.

WHAT ACCESS CONTROLS/PROCESSES DOES YOUR COMPANY HAVE IN PLACE TO PROTECT PRIVATE USERS? (Choose all that apply)

- Shared Account Password Management: 32%
- Superuser Password Management: 50%
- Privileged Access Management: 80%
- Privileged Session Management: 38%
- Privileged Session Recording and Monitoring: 30%
- Other (please specify): 3%

WHAT SECURITY SOLUTION(S) DOES YOUR COMPANY LEVERAGE TO GOVERN & SECURE ACCESS BY OUTSOURCED IT, VENDORS & OTHER THIRD PARTIES? (Choose all that apply)

- Local Account Provisioning: 42%
- Application-to-application password management: 25%
- Privileged Access Management: 62%
- Secure Password Storage: 32%
- Multi-factor Authentication For Servers: 48%
- Other (please specify): 3%
BIG DATA SOLUTIONS

One reason companies are adopting cloud services is to process and analyze large data sets that can bring added value to the line of business. With the growth of this science of analyzing data, big data solutions are promising the ability to process data faster and at greater volumes than ever before. Only 22% of security professionals surveyed reported that they use big data solutions. These companies use the same type of access controls/processes from above for their big data solutions. Those that embraced this technology also consistently used more security solutions across the board.

Also, once again larger companies over 50,000 employees were more likely to utilize a big data solution when compared with companies 5,000 or smaller. Companies in the Americas were more likely to utilize a big data solution than companies from EMEA.

WHAT ACCESS CONTROLS/PROCESSES DOES YOUR COMPANY HAVE IN PLACE FOR BIG DATA SOLUTIONS TO PROTEXT PRIVATE USERS? (Choose all that apply)

- Web & SaaS SSO: 62%
- Enterprise App SSO: 58%
- Multi-factor Authentication Tokens & Management: 70%
- Enterprise Mobility Management: 41%
- MAC Management: 20%
- Other (please specify): 10%
DATA BREACHES

The cost of a data breach is greater than ever. Time and resources can be significant due to monetary penalties, legal processes, intellectual property, and recovery fees can have significant financial impact. Perhaps the loss of brand reputation is even greater. However, 57 percent of companies indicated that their company had never reported a data breach. Of those that experienced a data breach, the average risk rating was low-medium at 2.84 (1 - very low, 5 - very high). Security and technology professionals in companies with over 10,000 employees were more likely to report that they were “unsure” if a breach had been reported compared to smaller companies. This could occur due to a less intimate knowledge of all events within the company.

Nearly a quarter (22%) of respondents indicated that the breach was due to compromised credentials. 65 percent of respondents indicated that the likelihood their company would experience a future breach due to compromised credentials was medium to high. Companies from the Americas were less likely to believe that this chance was “very high” compared to APAC companies.

Surprisingly, there were no significant differences in security solutions used between respondents who reported a breach and those who either did not report or did not know of a reported breach in their organizations. Addressing the low hanging fruit with traditional security measures is an important step towards but it doesn’t keep companies from being targeted. Being aware of the latest threats and building layers of access control in security may not keep adversaries away but it can limit them from getting to your most sensitive data.

HAS YOUR COMPANY EVER REPORTED A DATA BREACH?

- Yes: 17%
- No: 57%
- Unsure: 26%

WAS THE DATA BREACH YOUR COMPANY EXPERIENCED DUE TO COMPROMISED CREDENTIALS?

- Yes: 22%
- No: 53%
- Unsure: 25%
INVESTING IN A FULL IDENTITY SECURITY PLATFORM

Identity and access management practices are not new but understanding and managing identity involves many new layers in your cloud environment. Protecting an organization from the inside with access controls protects data beyond the perimeter. We asked respondents to determine what services would be worth investing in a full identity security platform. The following services received an average rating of “agree.” C-level and executive security professionals were slightly less interested in a platform that secured each of these items when compared to general staff and managers. This could be due to additional concerns such as the budget or other weak points in their security. However, in general it appears individuals would be particularly interested in a platform that secures all these items.

I WOULD INVEST IN A PLATFORM THAT SECURES

<table>
<thead>
<tr>
<th>Service</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Services</td>
<td>4.00</td>
</tr>
<tr>
<td>Enterprises</td>
<td>3.75</td>
</tr>
<tr>
<td>End Points</td>
<td>3.50</td>
</tr>
<tr>
<td>Cloud Hosted Environments</td>
<td>4.25</td>
</tr>
<tr>
<td>Cloud Apps</td>
<td>4.00</td>
</tr>
</tbody>
</table>

* scale 1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree
SURVEY RESPONDENTS

Respondents to this survey came from a variety of industries from across the globe. The below graphics examine the company size, industry, level of responsibility, and geographic location of the 325 survey respondents.

WHICH BEST DESCRIBED THE SIZE OF YOUR COMPANY

<table>
<thead>
<tr>
<th>EMPLOYEES</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1000</td>
<td>30%</td>
</tr>
<tr>
<td>1000 - 5000</td>
<td>17%</td>
</tr>
<tr>
<td>5000 - 10000</td>
<td>9%</td>
</tr>
<tr>
<td>10000 - 30000</td>
<td>15%</td>
</tr>
<tr>
<td>30000 - 50000</td>
<td>5%</td>
</tr>
<tr>
<td>+50000</td>
<td>24%</td>
</tr>
</tbody>
</table>

WHAT IS YOUR ORGANIZATION’S INDUSTRY

- Business
- Education
- Entertainment
- Financial
- Government
- Healthcare
- Manufacturing
- Technology
- Telecommunication
- Transportation
- Utilities
- Other
WHAT IS YOUR LEVEL RESPONSIBILITY?

- Manager: 48%
- C-level/Executive: 20%
- Staff: 32%

WHAT REGION OF THE WORLD DO YOU RESIDE IN?

*Most individuals come from the United States, Canada, and India

- Americas: 75%
- EMEA (Europe, Middle East, Africa): 13%
- APAC (Asian, Pacific Island): 12%