SECURITY LIFECYCLE REVIEW

EXECUTIVE REPORT

Acme

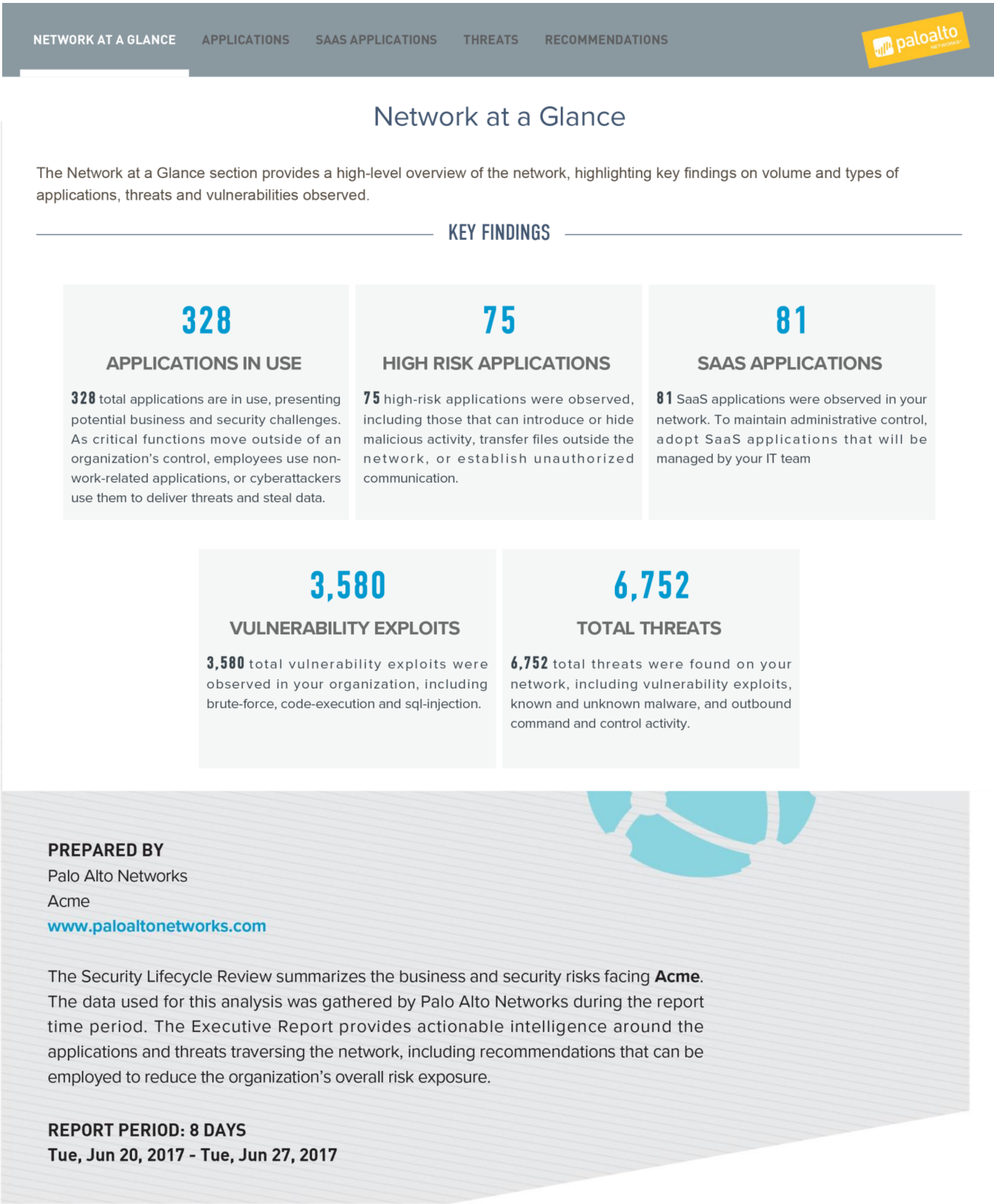
PREPARED BY

Palo Alto Networks
Acme
www.paloaltonetworks.com

The Security Lifecycle Review summarizes the business and security risks facing **Acme**. The data used for this analysis was gathered by Palo Alto Networks during the report time period. The Executive Report provides actionable intelligence around the applications and threats traversing the network, including recommendations that can be employed to reduce the organization's overall risk exposure.

REPORT PERIOD: 8 DAYS
Tue, Jun 20, 2017 - Tue, Jun 27, 2017

TABLE OF CONTENTS



Network at a Glance

The Network at a Glance section provides a high-level overview of the network, highlighting key findings on volume and types of applications, threats and vulnerabilities observed.

KEY FINDINGS

328

APPLICATIONS IN USE

328 total applications are in use, presenting potential business and security challenges. As critical functions move outside of an organization's control, employees use non-work-related applications, or cyberattackers use them to deliver threats and steal data.

75

HIGH RISK APPLICATIONS

75 high-risk applications were observed, including those that can introduce or hide malicious activity, transfer files outside the network, or establish unauthorized communication.

81

SAAS APPLICATIONS

81 SaaS applications were observed in your network. To maintain administrative control, adopt SaaS applications that will be managed by your IT team

3,580

VULNERABILITY EXPLOITS

3,580 total vulnerability exploits were observed in your organization, including brute-force, code-execution and sql-injection.

6,752

TOTAL THREATS

6,752 total threats were found on your network, including vulnerability exploits, known and unknown malware, and outbound command and control activity.

PREPARED BY
Palo Alto Networks
Acme
www.paloaltonetworks.com

The Security Lifecycle Review summarizes the business and security risks facing **Acme**. The data used for this analysis was gathered by Palo Alto Networks during the report time period. The Executive Report provides actionable intelligence around the applications and threats traversing the network, including recommendations that can be employed to reduce the organization's overall risk exposure.

REPORT PERIOD: 8 DAYS
Tue, Jun 20, 2017 - Tue, Jun 27, 2017

Grupo Smartekh

paloalto NETWORKS CPSP

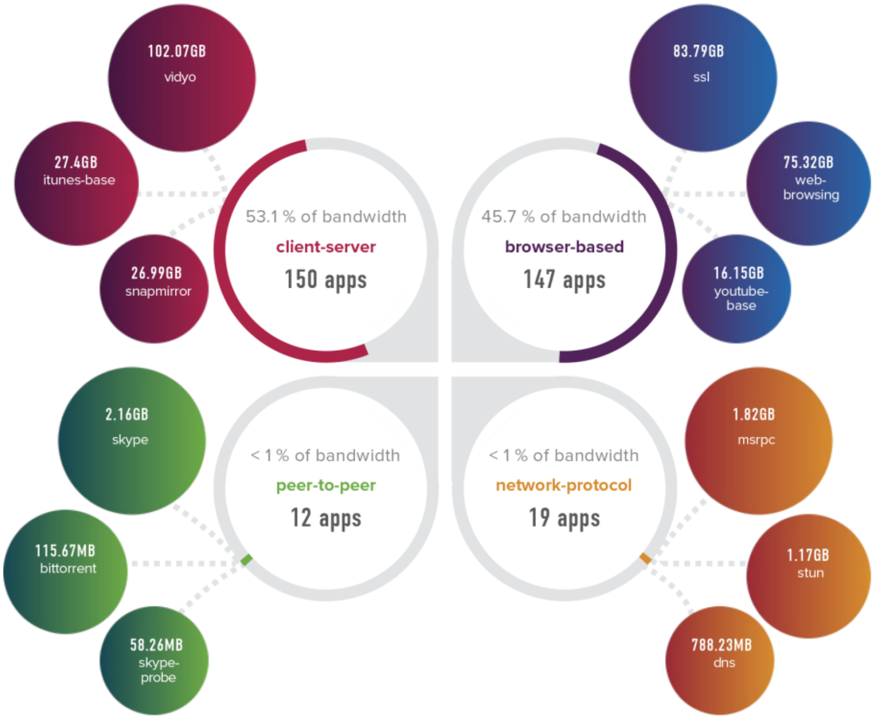
Applications

Total Bandwidth: **561.42GB** | Total Sessions: **9,873,454** | Total Applications: **328**

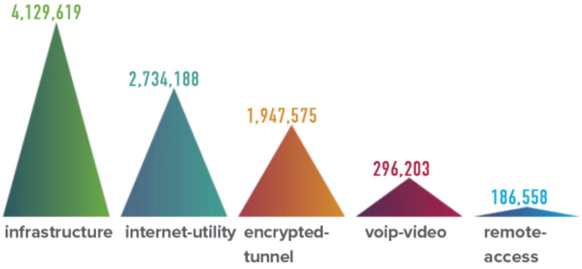
The first step to managing security and business risk is identifying which applications can be abused to cause the most harm. We recommend closely evaluating applications in these categories to ensure they are not introducing unnecessary compliance, operational, or cyber security risk.

APPLICATION BANDWIDTH BY TECHNOLOGY

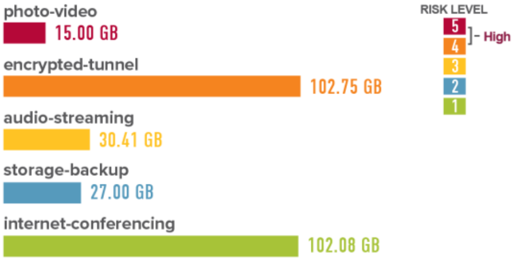
Bandwidth consumption across the technology categories along with the top applications consuming the most bandwidth from each category are shown below, followed by charts displaying the top application categories by sessions and risk level.



TOP 5 APPLICATION CATEGORIES BY SESSIONS



TOP 5 APPLICATION CATEGORIES BY RISK LEVEL



* The Palo Alto Networks research team uses the application behavioral characteristics to determine a risk rating of 1 through 5, with 5 being the highest.

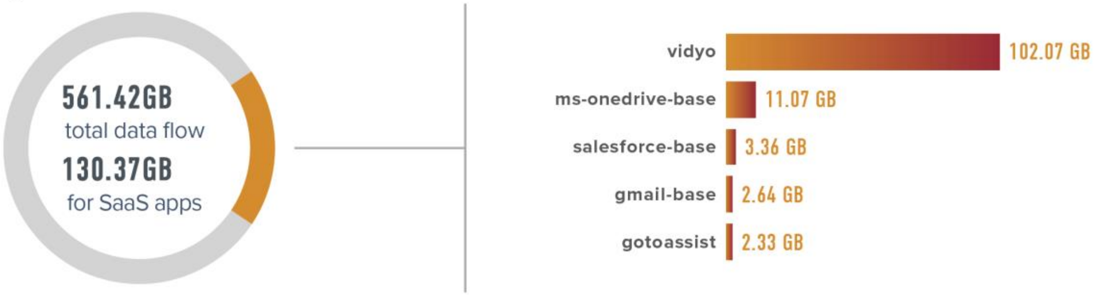
SaaS Applications

Total Bandwidth: **130.37GB** | Total Sessions: **417,141** | Total Applications: **81**

SaaS-based applications continue to redefine the network perimeter, providing critical functionality and efficiency, but at the same time introduce potential new security and data risks if not properly controlled. Often labeled "shadow IT," most of these services are adopted directly by individual users, business teams, or even entire departments. In order to minimize data security risks you need control over SaaS applications used in your network.

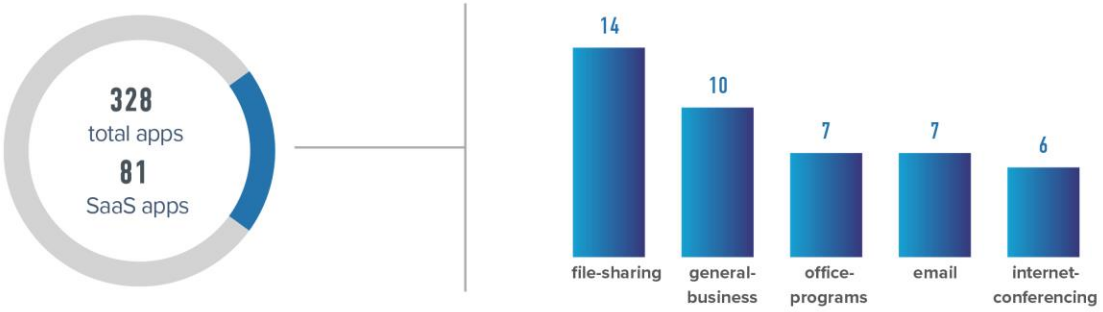
TOP 5 SAAS APPLICATION BY BANDWIDTH

The chart below displays the SaaS data movement in comparison with the total data movement in your network and highlights the top 5 SaaS applications that consume the most bandwidth.



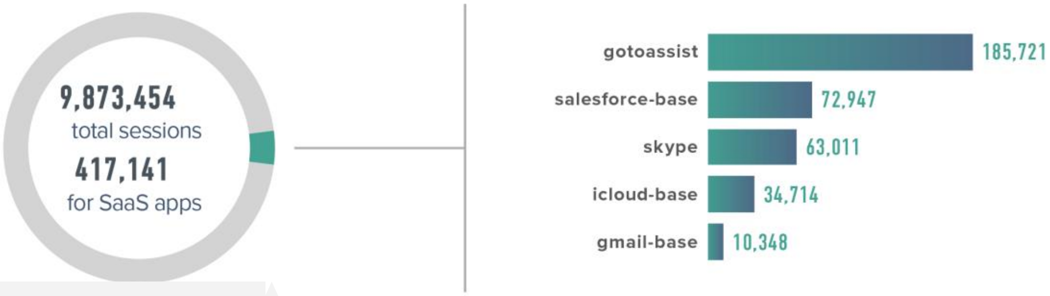
TOP 5 SAAS APPLICATION CATEGORIES BY NUMBER OF APPLICATIONS

The following chart displays the number of SaaS applications in each application category. This allows you to assess the most used SaaS applications in your organization.



TOP 5 SAAS APPLICATION BY SESSIONS

The chart below identifies the top SaaS application categories delivering the most sessions.



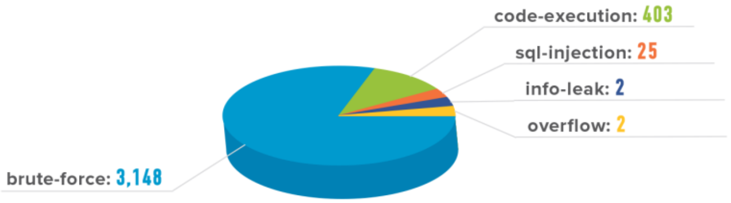
Threats

Total Vulnerability Exploits: **3,580** | Total Applications Delivering Exploits: **3** | Total Malware: **106**

Understanding your risk exposure, and how to adjust your security posture to prevent attacks, requires intelligence on the type and volume of threats used against your organization. This section displays information on vulnerability exploits, application vulnerabilities and malware, observed on your network.

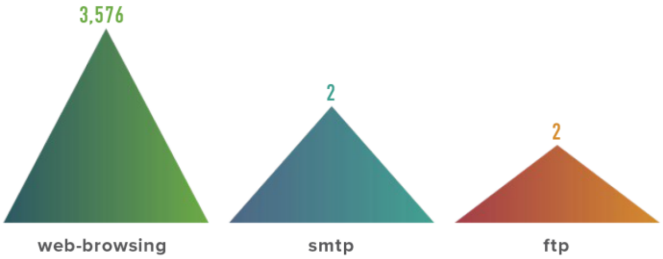
VULNERABILITY EXPLOITS

The chart below shows the number of vulnerability exploits delivered in each category including brute-force, code-execution and sql-injection.



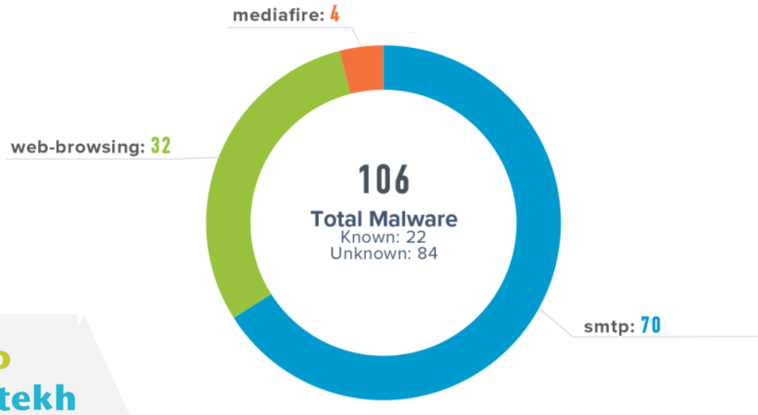
TOP APPLICATIONS DELIVERING MOST EXPLOITS

The observations below display the top application categories delivering the most exploits in your network.



TOP APPLICATIONS DELIVERING MOST MALWARE

The chart below provides information on the top application categories delivering the most malware in your network. This data allows you to prioritize your security efforts on the applications and categories used most by attackers.



Recommendations

- Implement safe application enablement polices, by only allowing the applications needed for business, and applying granular control to all others.
- Address high-risk applications with the potential for abuse, such as remote access, file sharing, or encrypted tunnels.
- Deploy a security solution that can detect and prevent threats, both known and unknown, to mitigate risk from attackers.
- Use a solution that can automatically re-program itself, creating new protections for emerging threats, sourced from a global community of other enterprise users.

CONTACT US

Grupo Smartekh

Gomathy Kannan
gkannan@paloaltonetworks.com

paloalto NETWORKS
CPSP

¡AHORA ES TU TURNO!

¿ QUÉ ESTA PASANDO EN TU RED?

RESERVA AQUÍ
TU ANÁLISIS SLR

>Conoce más

smartekh.com

Insurgentes Sur 826 P10 Col.Del Valle C.P. 03100 Ciudad de México.

Grupo Smartekh

paloalto NETWORKS®

CPSP