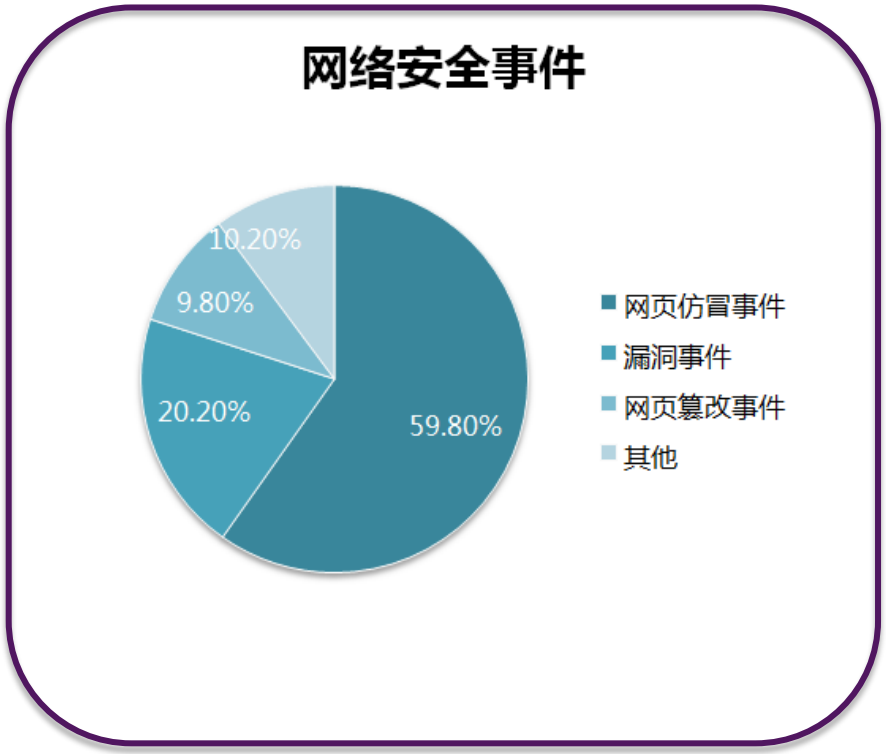
互联网+时代的
网络安全挑战及应对策略

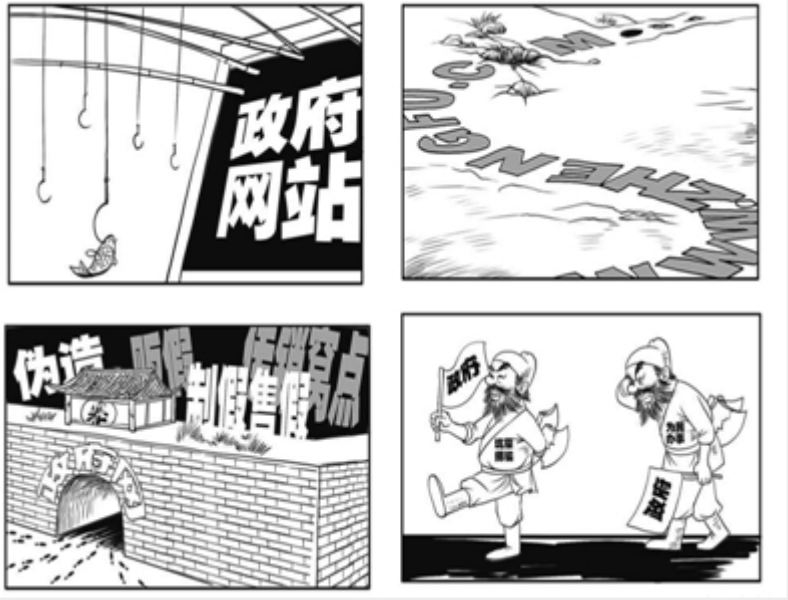
尹东梅
China Channel Sales Manager
mia.yin@entrustdatacard.com

《2015年中国互联网网络安全报告》



国家互联网应急中心于2016年5月25日发布了《2015年中国互联网网络安全报告》。报告显示，2015年互联网应急中心发现网络安全事件超过12万起，较2014年增长125.9%。其中，境内报告网络安全事件126424起，较2014年增长了128.6%，境外报告网络安全事件492起，较2014年下降43.9%。发现的网络安全事件中，数量排前三位的类型分别是网页仿冒事件（占59.8%）、漏洞事件（占20.2%）和网页篡改事件（占9.8%）。2015年，互联网应急中心共成功处理各类网络安全事件125815起，较2014年的56072起增长124.4%。

网站仿冒



新攻击方式及漏洞频现

Heartbleed

- Exploit of Heartbeat extension in OpenSSL 1.0.1. (widely used in web servers, O/S's) - Anything with OpenSSL is vulnerable

Fix:

- Update your version of OpenSSL
- Replace any keys and certificates on those machines
- Ask users to change passwords

Remaining vulnerabilities:

- Many certificates replaced without replacing keys!!

POODLE

- **P**adding **O**racle **O**n **D**owngraded **L**egacy **E**ncryption
- Attacker can downgrade SSL/TLS session

Fix:

- Stop supporting SSL 3.0 (Browsers already doing this)
- Patch servers to avoid TLS vulnerabilities

Remaining vulnerabilities:

- Check your server at entrust.ssllabs.com

DROWN

- ***Decrypting RSA using Obsolete and Weakened eNcryption***
- Adapts an old SSLv2 vulnerability
- Can be used against any TLS protocol with same RSA key

Fix:

- *SSL v2 needs to be disabled* ***everywhere****, without* ***exception***. But, this has always been the case, given that we've known about the various SSL v2 vulnerabilities for more than 20 years now

FREAK

- **F**actoring **R**SA **E**xport (**A**ndroid) **K**eys
- A MITM attack that forces browser to use weaker encryption key, providing attacker access to all encrypted info
- Result of US gov't policy preventing stronger encryption from being exported

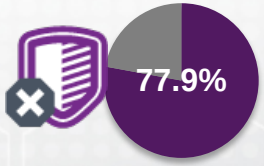
Fix:

- At server, disable support for insecure ciphers
- Check your server at entrust.ssllabs.com

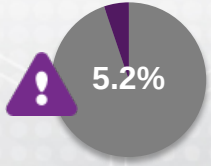
Remaining vulnerabilities:

- 36% of servers still accept "export grade crypto"

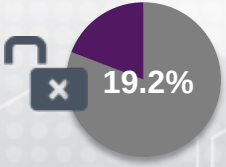
无处不在的安全隐患



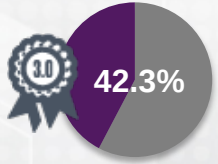
77.9% of sites are HTTP



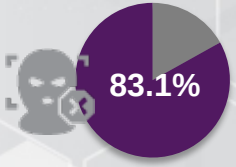
5.2% have an incomplete chain



19.2% support weak/insecure cipher suites

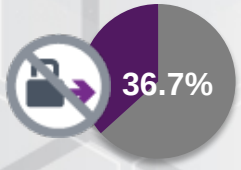


42.3% support SSL 3.0



83.1% vulnerable to BEAST attack

5.5% vulnerable to CRIME attack



36.7% do not support Forward Secrecy

https://www.trustworthyinternet.org/ssl-pulse/

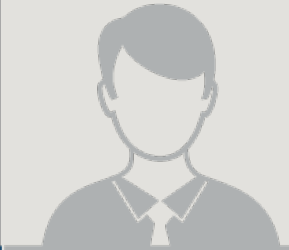
现状

Business Disruption

- ✓ Slow website performance
- ✓ Improperly installed certificates
- ✓ Expired certificates
- ✓ Misconfigured server
- ✓ User security warnings

Threats

- ✓ FREAK
- ✓ SuperFish
- ✓ POODLE
- ✓ Heartbleed
- ✓ BEAST
- ✓ CRIME
- ✓ Lucky Thirteen



Evolving Technology

- ✓ SHA1→SHA2
- ✓ OCSP Stapling
- ✓ CAA
- ✓ CT
- ✓ TLS 1.2
- ✓ ECC
- ✓ HTTP/2

Compliance

- ✓ PCI
- ✓ HIPAA
- ✓ SHA1→SHA2
- ✓ Security Policy
- ✓ SSL3 deprecation

Resource Constraints

- ✓ Do more with less
- ✓ Consolidate vendors
- ✓ Implementation costs
- ✓ De-focused staff
- ✓ Limited training
- ✓ Rapid deployment

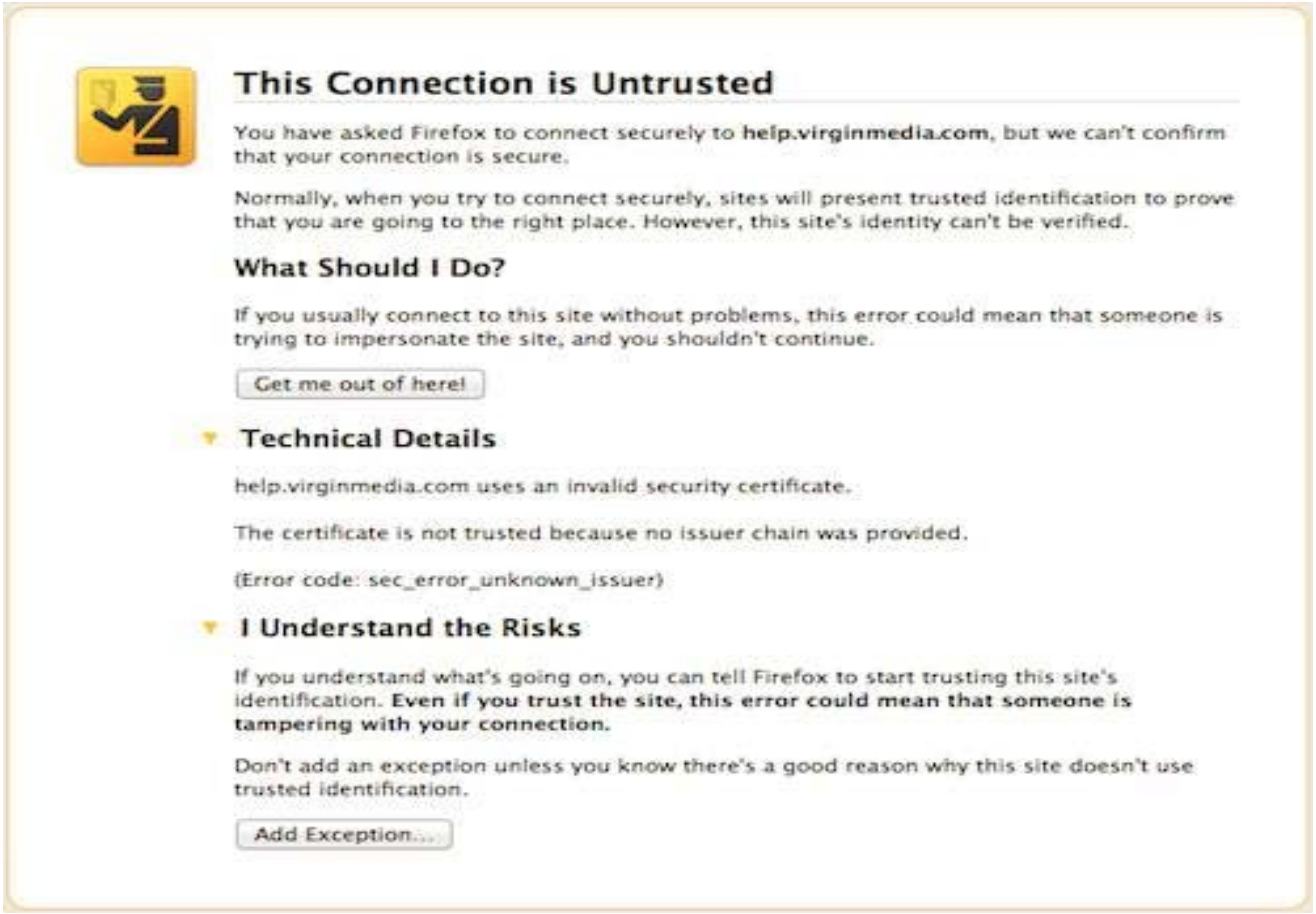
Brand Damage

- ✓ Site outage/performance
- ✓ Data breach
- ✓ SPAM blacklist
- ✓ Search engine blacklist
- ✓ Malicious impersonation

谷歌发起数字安全羞辱活动

- Google 发起此项活动，将安全问题更加严肃对待
  - 如果网站没有采取正当的安全措施，将向用户进行相关危险提示及展示
    - Mixed content
    - SHA1 still in use
    - Certificate transparency (public list) for EV certificates
    - Future: Warnings for non-SSL pages, RC4, Non-OCSP Stapling

未采用HTTPS报警提示



行业要求及变化

Non-FQDN Certificates

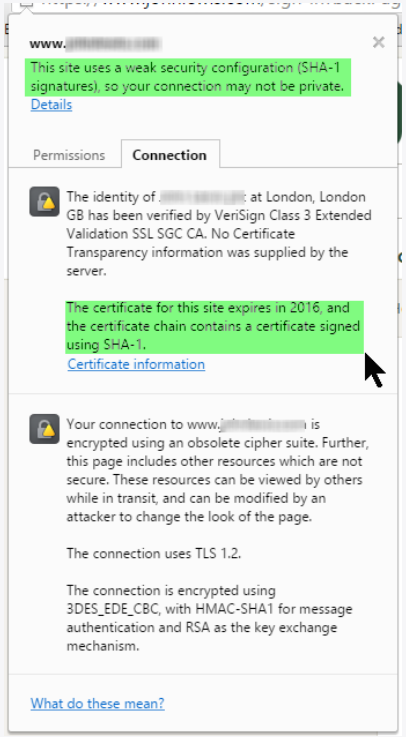
- CAs will stop issuing public trust certificates with unregistered domains as of 1 November 2015
- CAs will revoke these certificate by 1 October 2016
- What can Customers do?
  - Stop using non-FQDNs
  - Change names to FQDNs
  - Use Private SSL where we issue certificates with customer reserved non-FQDNs

3 Year Certificate Lifetime Max

- As of 1 April 2015, the maximum validity for SSL certificates is 39 months
- Pooling certificates have dropped from maximum 50 months to 39 months
- Non-pooling and Retail certificates have dropped from maximum 4 years to 3 years
- EV SSL certificates remain at a maximum of 27 months

SHA-1向SHA-2迁移

- CAs must not issue SHA-1 after 1 January 2016
- Maximum lifetime for SHA-1 is 31 December 2016
- Windows will stop supporting SHA-1 signatures in 2017
- All supported browser and operating systems support SHA-2
- Customers must ensure that other applications also support SHA-2



Chrome Version	Earliest Release Date	SHA-1 Expires Jan.- May 2016	SHA-1 Expires June - Dec. 2016	SHA-1 Expires After 2016
39	3 Nov. 2014	No Change	No Change	Yellow Triangle Over Lock
40	15 Dec. 2014	No Change	Yellow Triangle Over Lock	Blank Page, No Lock
41	26 Jan. 2015	Yellow Triangle Over Lock (sub resources will also trigger icon)	Yellow Triangle Over Lock (sub resources will also trigger icon)	Red X Over Lock (sub resources trigger yellow icon)

Entrust Datacard

SHA1向SHA2过渡

- SHA1 is a secure hashing algorithm that puts a unique identity in the signature for a certificate that “cannot be duplicated” for another certificate
- SHA1 is showing weakness and is being replaced with SHA2
  - In 2005 it was cracked 2000 times faster than predicated
  - Predicated cost to forge a SHA-1 certificate to come down from

    $2m in 2012 to $43K in 2021
- Operating System and Browser Vendors are pushing for SHA1 deprecation and migration from SHA1 to SHA2

SSL 数字证书应用场景

信用卡在线交易

系统登录

任何线上敏感信息
接入入口

邮箱接入

虚拟桌面登录

基于Https 及FTP的
网络文件传输服务

云及移动应用

内网通信
(如networks,
文件共享，等)

VPN登录

什么是SSL？ SECURE SOCKET LAYER

SSL — 标准的信息安全技术，在浏览器 与服务器之间提供身份认证 及加密数据传输

网络安全面临的问题

–如何为网站访问者提供身份及数据加密服务？

–如何保护服务器之间数据传输？

–如何确保数据安全传输？

SSL 针对上述问题的解决方案

–身份 ~对服务器及设备提供身份认证

–隐私 ~ 提供加密服务

经SSL加密后展示

SSL 证书的两大主要作用

数据加密 & 身份认证

DV
Domain Validation

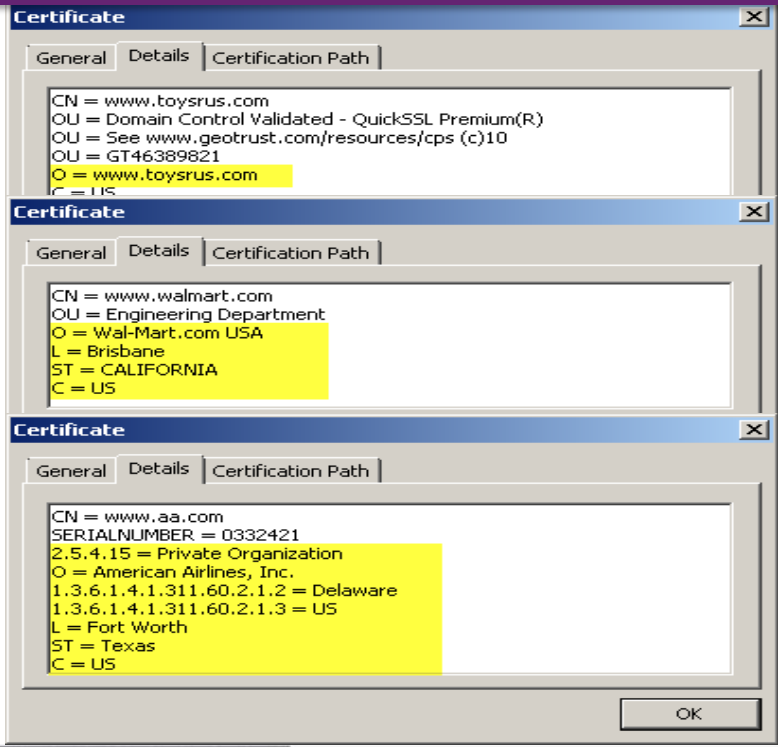
Low

OV
Organizational Validation

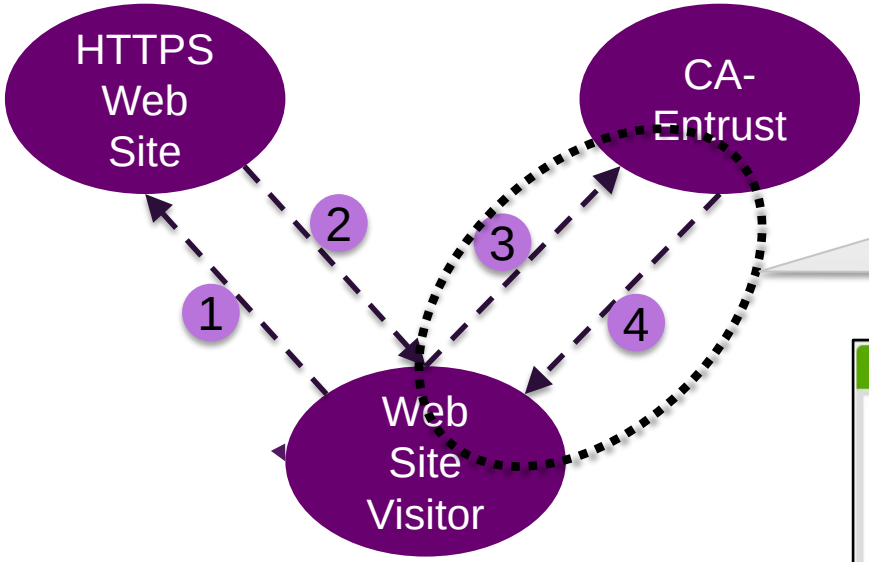
Med

EV
Extended Validation

High

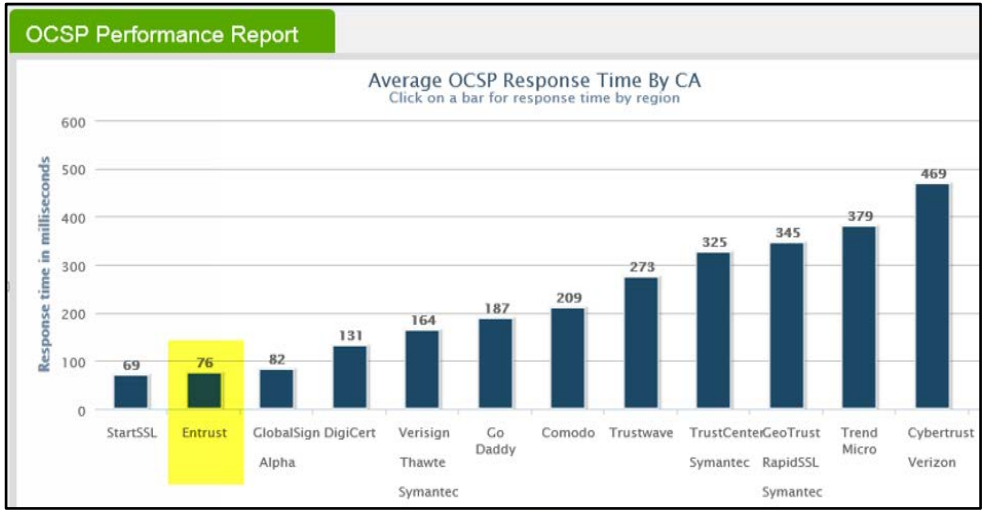


WEB SITE PERFORMANCE MATTERS!



- Entrust takes less than ~80 ms
- Many competitors take ~200+ ms
- Usually 2 checks minimum req'd
- *Impacts speed AND availability!*

1. Visitor hits web site
2. Web site returns certificate, browser checks validity (dates) and trust (is root in browser)
3. Browser checks revocation status with CA
4. CA returns a Yes/No response
5. Web site completes rendering



ENTRUST CLOUD证书类型

SSL 类证书

OV SSL Certificates

Standard

Advantage

Wildcard

UC Multi-Domain

Private SSL

Entrust/Sitelock

Basic Website Security bundle

Enhanced Website Security bundle

EV SSL Certificates

EV Multi-Domain

Entrust/SSL Labs

Website Configuration Tests

电子签名类证书

代码签名证书

Code Signing

Supports Authenticode, VB & Macros, Java & A dobe AIR, Kernel Mode Signing

EV Code Signing

Supports Windows 10 Kernel Mode Signing

文件签名证书

Individual

Group

Enterprise Lite & Pro

用户类证书

安全邮件证书

个人版

企业版

设备类证书

Mobile Device Certs

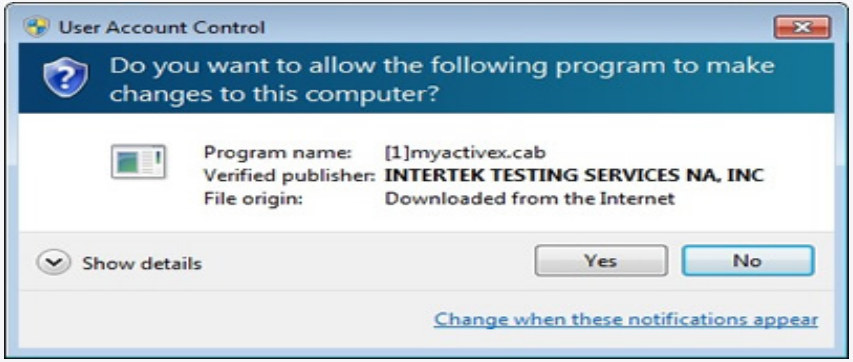
Entrust Certificate Discovery and Management

文档签名证书

- Creates trusted digital signatures
- Compatible with Adobe, Microsoft Office, OpenOffice, and LibreOffice
- Provides authentication, non-repudiation and verification that the file was not altered
- Entrust Document Signing digital signatures comply with the U.S. Federal ESIGN Act and many other international laws making documents legally binding
- Supports multiple signature workflow – manual and automatic

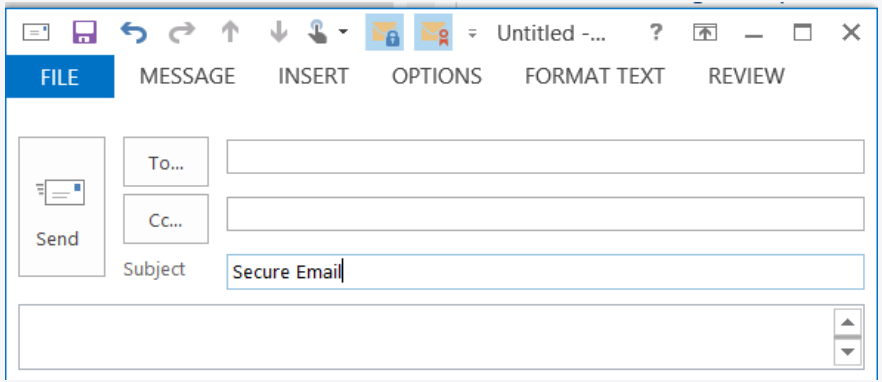
代码签名证书

- Digitally sign applications and software distributed over the internet
- Includes the name of the publisher and assurance that the code hasn't been tampered with since being published
- Users can confirm the identity of the software author and gain assurance that the code has not been altered or corrupted since it was signed
- EV Code Signing certificates required for signing Windows 10 drivers



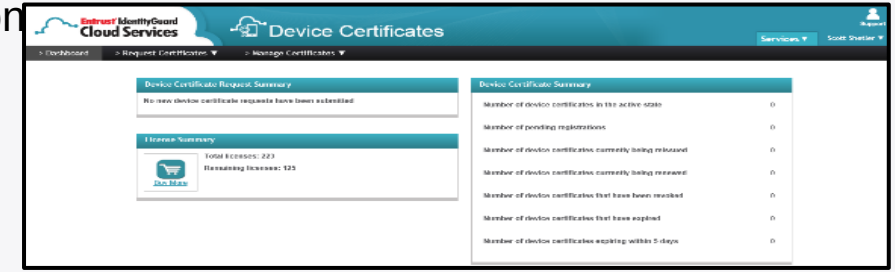
安全邮件证书

- Encryption of email and it’s contents
- Assures the recipient that the email content has not been tampered
- Ensures message privacy and keeps sensitive information from falling into the wrong hands.
- Proves who sent the email



移动设备证书

- Allows secure and transparent authentication to WiFi and VPN networks from mobile devices
- Enables Audit of mobile networks
- Protects IP and network assets



- Same audience as those who buy and manage SSL certificates – IT/Security Directors, IT/Security Administrators and Operations, VP of IT
- Organizations with mid-sized mobile device deployments, with no MDM

增值工具—— ENTRUST DISCOVERY

Business Problems

Application Outages
(due to unexpected expiry of certificates)

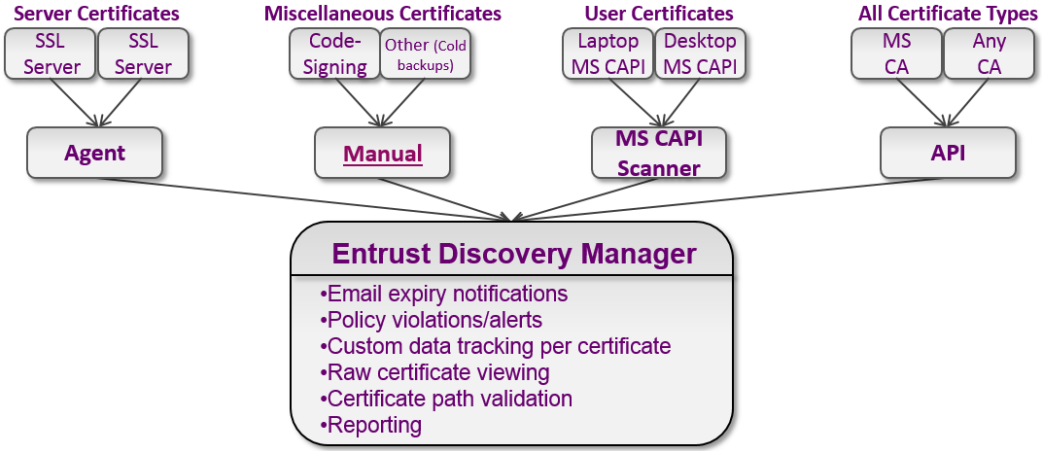
Compliance Concerns
(due to inability to inventory certificate population)

Complexity of Certificate Management
(due to certificates from multiple sources)

Discovery is the Solution!

Scan your network for certificates
- *from any vendor*
- *any type*
- *public or private*

Manage all your certificates
- *Multi-person, multi-level email notifications*
- *Policy management*
- *Custom tracking data w/ auto-population rules*



DISCOVERY TO FIND ROGUE CERTIFICATES

What is it?

Scans ALL your internal or external webservers to inventory your SSL Certificate population. Results are auto-populated in the Entrust Cloud certificate management portal.

Value Proposition

- **Avoids application outages** by notifying customers when certificates are close to expiry, where they are located, and if they are installed in multiple locations
- **Avoids data breach** by highlighting issues with deployed certs, like weak crypto
- **Helps with compliance** reporting, by providing an inventory and reporting tools on your certificate population
- **Facilitates certificate management** by providing a single interface to manage certificates from ANY VENDOR

增值工具—— ENTRUST TURBO

What is it?

A client software installed on the web server, that makes it easier to request the CSR and install the certificate, without relying on human knowledge.

Value Proposition

- **Saves time and money** installing certificates, by having less touches on the web server and automating the process
- **Reduces human error** installing the chain certificates, potentially preventing possible outages
- **Easy to use** due to one-click interface and one time installation

附加网站安全服务

What is it?

Every Entrust Public SSL certificate comes with a free website security bundle, which mainly provides a remote web-based malware scanning and reputation monitoring capabilities

Value Proposition

- **Protects customers brand** by helping them find malware before it's distributed to unsuspecting customers
- **Immediately highlights existing issues** with your brand by monitoring Search Engine and Email blacklists
- Helps **ensure website continuity** by avoiding being blacklisted
- Provides an **effective, low-cost** means of web site scanning for common vulnerabilities

您有义务向用户提供安全可靠的网站!

SSL/TLS Protocol	
Defense	Evolving Standards
Ex.	POODLE
Responsibility	IETF

Protocol Implementation	
Defense	Bug free deployment
Ex.	Heartbleed
Responsibility	Server Browser vendors

CA Implementation	
Defense	Evolving CA Rqmts
Ex.	DigiNotar
Responsibility	CA Browser Forum, Browsers and CA's

SERVER IMPLEMENTATION

Responsibility= **YOU**

ENTRUST DATACARD

- Datacard 成立于1969年，总部位于美国Minnesota的Shakopee
- 2014年Datacard 收购Entrust，新公司名称变更为Entrust Datacard
- 年收入6亿美金
- 在全球34个国家拥有分支机构及办事处，全球雇员超过2000人
- 全球合作伙伴超过250家，业务覆盖150多个国家

10M+ Identity and Payment Credentials Issued Daily

Billions of Transactions Managed Annually

市场聚焦——可信身份及安全数据传输

ENTRUST 产品线

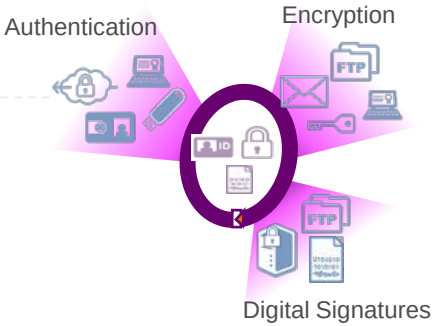
Identity & Access Management

Entrust GetAccess — Web access control and single sign-on for online transactions

Entrust IdentityGuard — Extensible software authentication platform for mobile, cloud and physical and logical environments

Entrust TransactionGuard — Transaction monitoring, fraud detection, behavior and identity analytics

Public Key Infrastructure (PKI)



Entrust Authority — PKI Certification Authority; digital certificate issuance

Entrust Entelligence — Secure, encrypted file sharing and communication

SMART CREDENTIALS — Obtain Smart Credentials in one of several form factors

PKI — User-based certificates and enrollment capabilities

Entrust Cloud

SSL — Obtain SSL and other certificates that are trusted globally!

DEVICE CERTIFICATES — Obtain Device Certificates to enable network access

DISCOVERY — Scan your network to find and report on expiring or out-of-policy certificates.

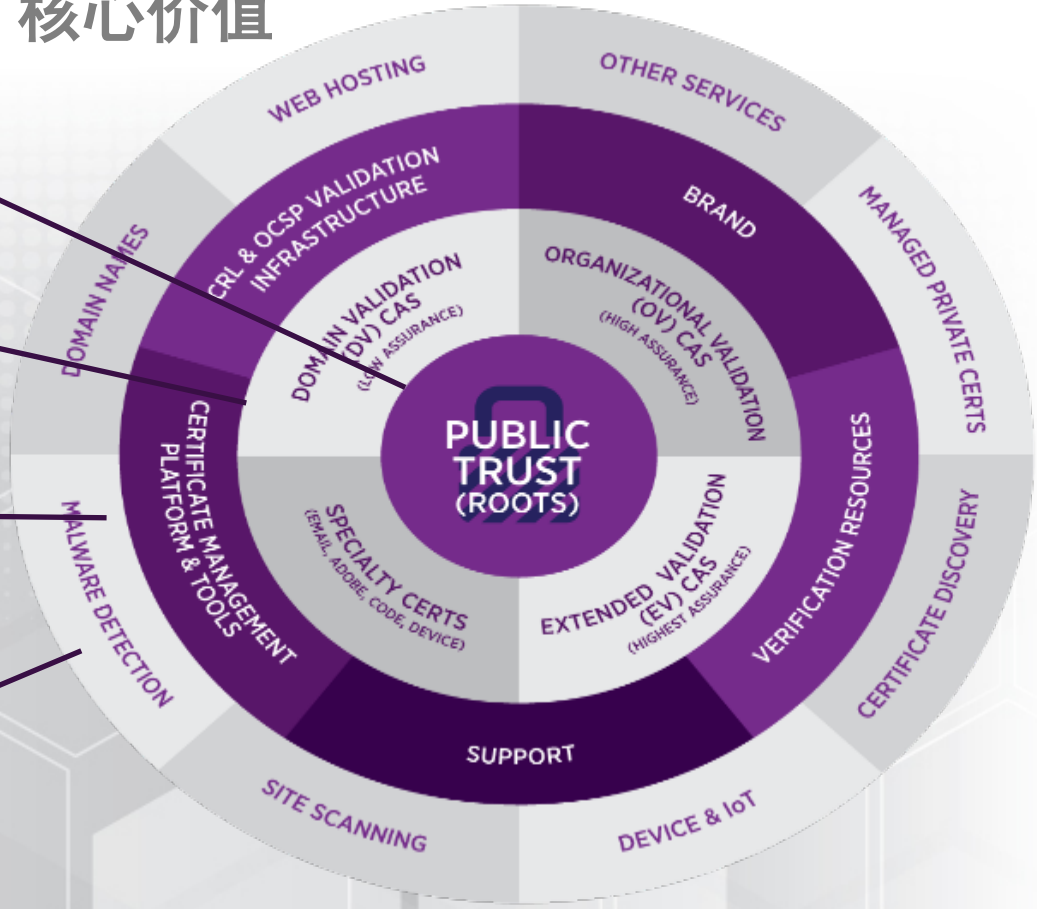
ENTRUST DATACARD SSL 核心价值

Core (Public Trust)
Continuous investment in embedding roots
Compliance with requirements

Product (SSL Certs)
Enhance OV and EV certs
Invest more in specialty certs
Investigate DV offering

Services and Differentiators
Cloud Platform
Advanced Cert Management
Verification Automation

Adjacent Services & Value Adds
Discovery Integration
Website Security Services
CT Monitoring



ENTRUST DATACARD 全球众多客户的选择

- 17 of top 22 Global e-Governments
- 7 of top 10 Global Commercial Savings Banks
- 8 of top 10 Global Telecom Companies
- 7 of top 10 Global Pharmaceuticals
- 8 of top 10 Global Aerospace & Defence
- 4 of top 5 Global Petroleum

ENTRUST DATACARD携手与您共筑安全 “诺亚方舟”

- Noah’s Ark
- 引用大会主办方的一句话“没有网络安全就没有国家安全，没有信息化就没有现代化”。
- 网络安全人人有责，让我们共筑安全“诺亚方舟”，续航百年企业。

谢 谢！