California Law Enforcement Telecommunications System Advisory Committee

Standing Strategic Planning Subcommittee

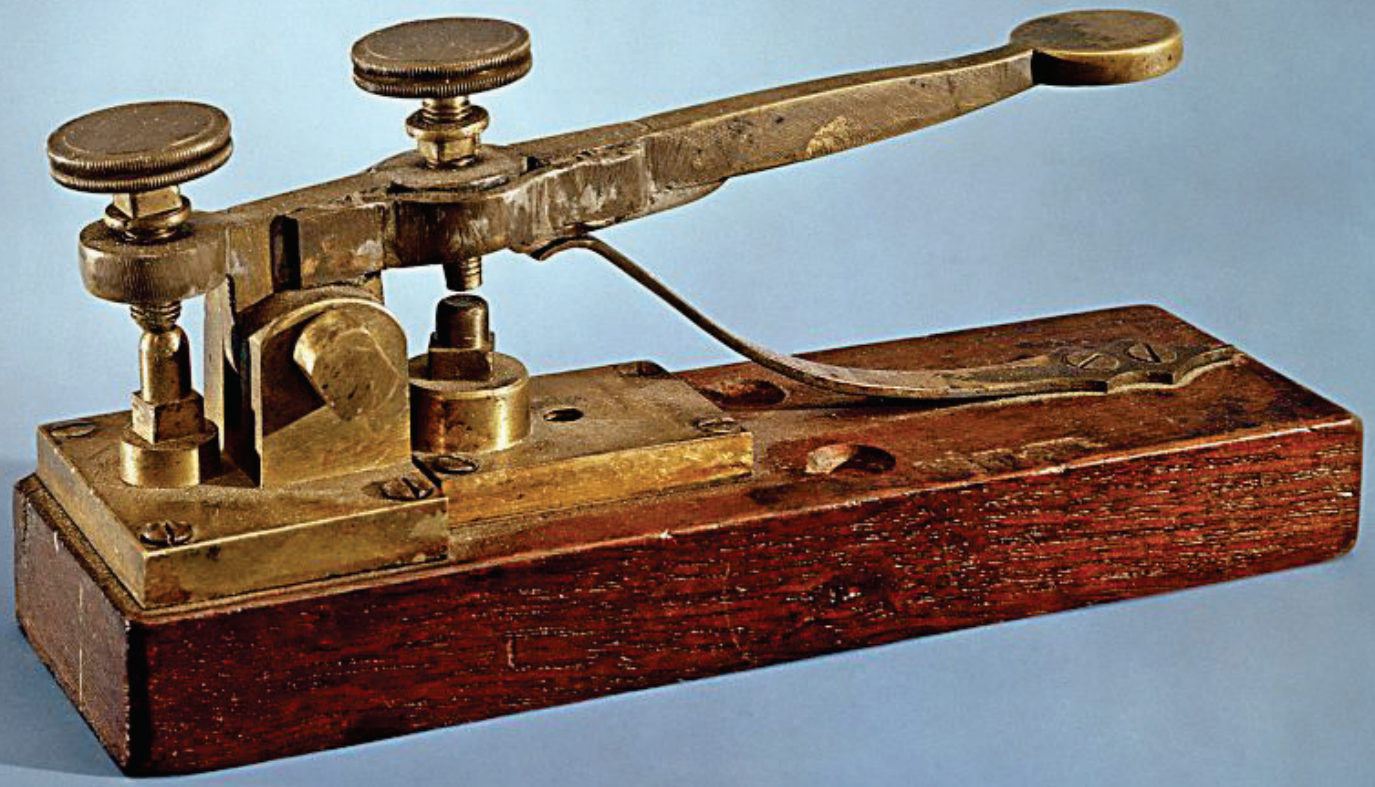
Folsom Police Department
November 19, 2015

Stuart McKee
Chief Technology Officer
State/Local Government

Microsoft

Microsoft

What hath God Wrought?



Samuel Morse 1844

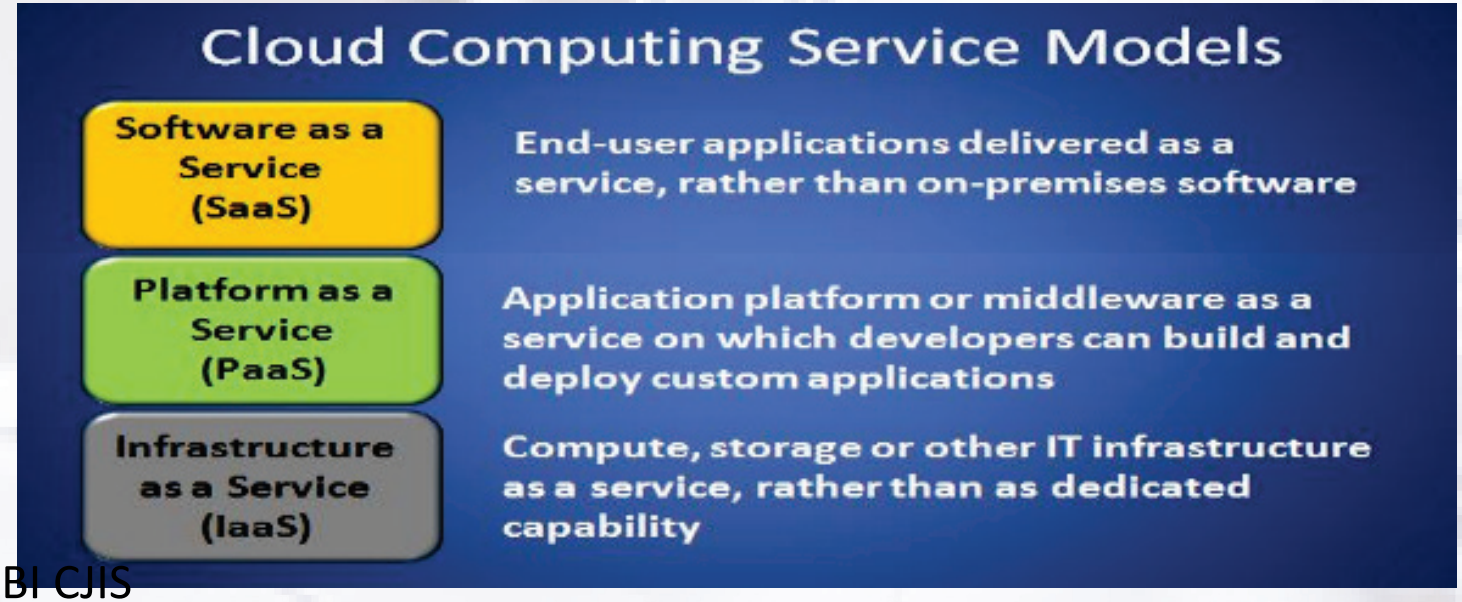
1961


DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

2015

CLOUD COMPUTING

A distributed, elastic, self provisioning, computing model that permits on-demand network access from anywhere to a shared pool of resources and information.



* Credit to George White FBI CJIS


LAPD
LAPD


POLICE


Microsoft Azure
Microsoft
Windows
Microsoft
Office 365


tait

Should I Be Worried About My Data?

How committed to compliance is your chosen provider?

- HIPAA
- FISMA
- SOX
- PCI DSS

What services are you moving to the cloud?

- Searchable Records
- Back Office Services (e-mail, collaboration, working files)
- Web Portal

Which/what cloud service model(s) are you leveraging?

- SaaS
- PaaS
- IaaS

What is the data sensitivity?

- PII
- IP
- CJI
- Financial
- Health Records

* Credit to George White FBI CJIS

CLOUD COMPUTING

Some Cloud Service Provider Must-Haves

- Transparency
- Encryption at rest and in transport
- Personnel security screening
- Customer or 3rd party audit
- Responsiveness to E-Discovery
- Clear access control mechanisms
- Granular breach response
- Exit Strategy

* Credit to George White FBI CJIS

Not All Clouds Are Created Equal

The Microsoft Cloud

200+ cloud services
1+ million servers
$15B+ infrastructure investment

1 billion customers
127 countries worldwide

OUR **UNIQUE** PERSPECTIVE

300B user authentications each month

1B Windows devices updated

200B emails analyzed for spam and malware

The Microsoft Government Community Cloud

Microsoft Azure

Office 365

Microsoft Dynamics

Approaching

3,000,000

O365 Gov Users

1,200,000

SQL databases in Azure

>30 Trillion

Storage objects in Azure

350 Million

Azure Active Directory users

>18 Billion

Azure Active Directory authentications/week

>2 Million

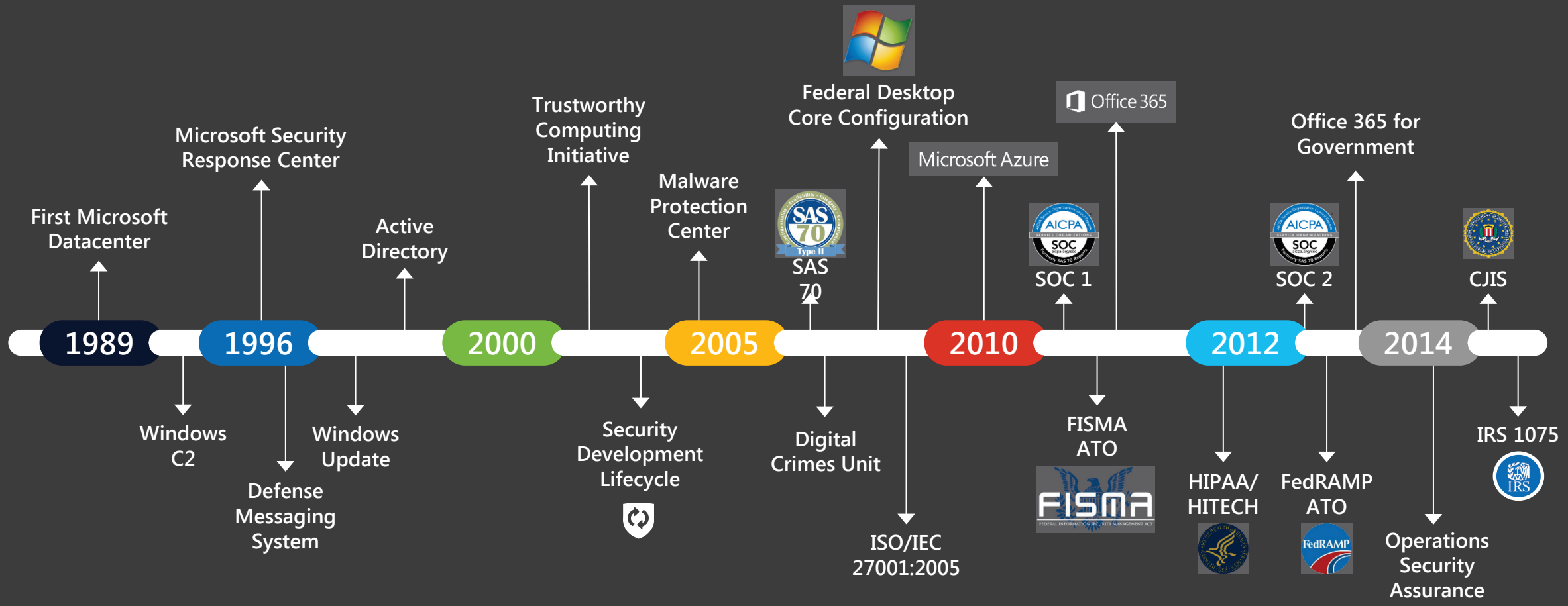
Developers registered with Visual Studio Online

+10% growth MoM

>60%

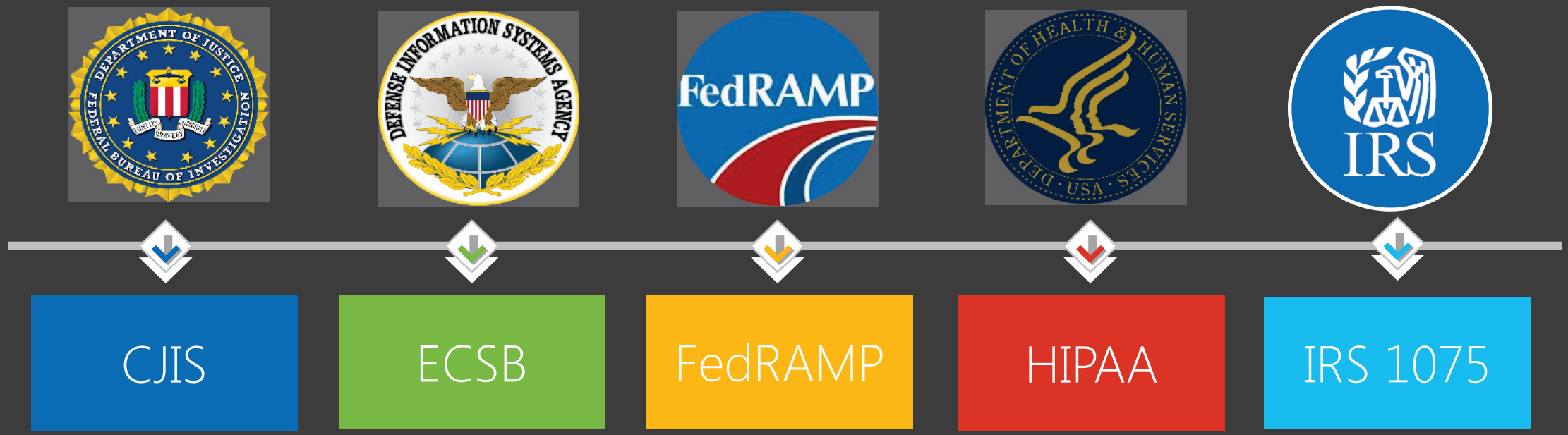
Customers using higher level services

Heritage of security and compliance



Commitment to industry-leading compliance

Microsoft offers unrivaled industry leadership through its commitment to compliance.



Microsoft is the first and only hyperscale cloud provider to meet CJIS security requirements for infrastructure and productivity.

Comprehensive
Compliance

Protecting YOUR data

CJIS

Employee Background Checks

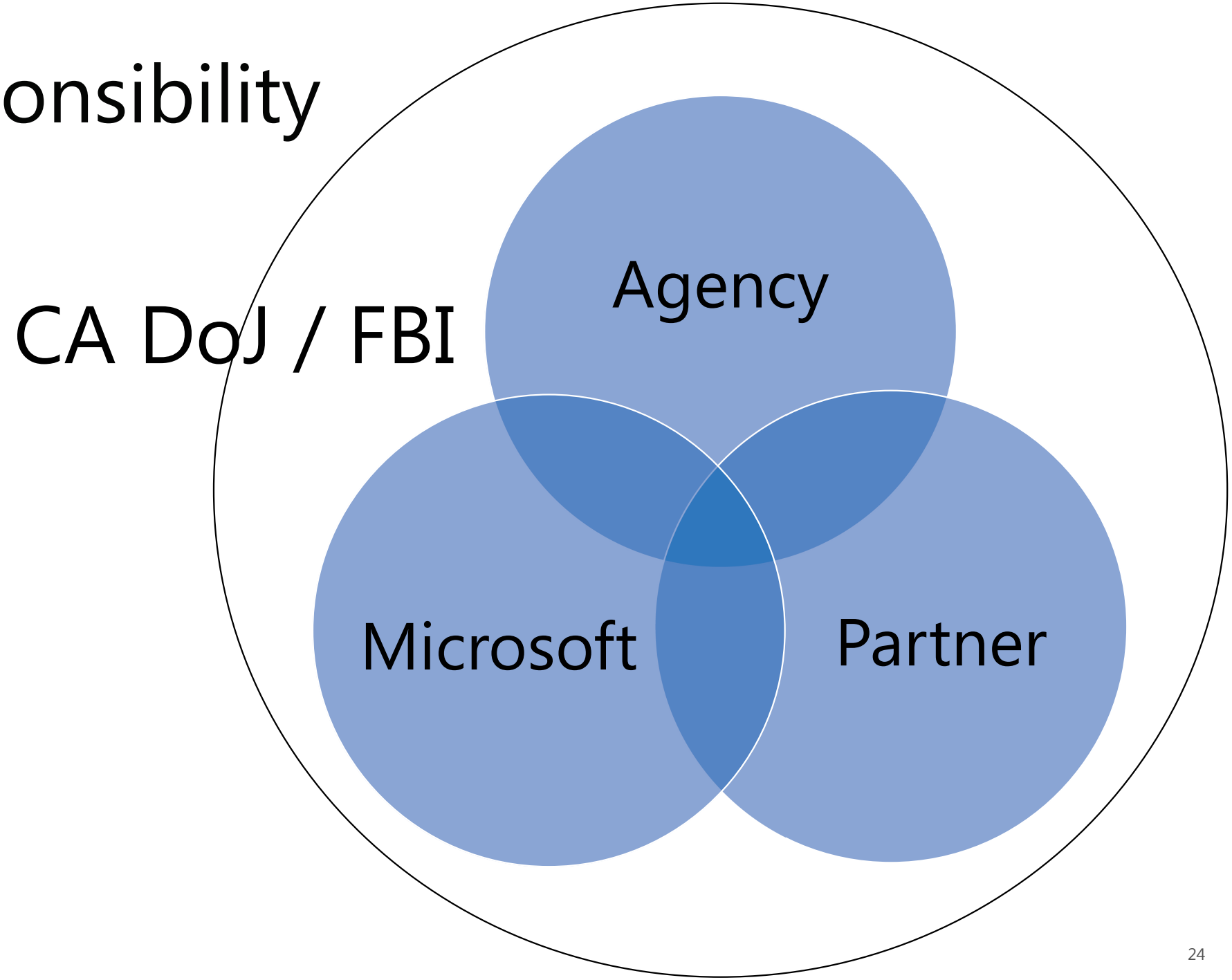
IRS 1075

Audits

HIPAA

Sign on the dotted line

Shared Responsibility



Agency interactions depend on nature of Cloud service

On Premises	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
Applications	Applications	Applications	Application
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

Managed by:

- Customer
- Vendor

Microsoft Azure

Office 365

Microsoft Dynamics CRM

Cyber Defense Operations Center

Office 365

Microsoft

This website has been classified as malicious.

www.spamlink.contoso.com

We recommend that you close this web page and not continue to this website. Learn more about Malware

Close this page.

Continue to this website (not recommended).

Security Center

Filter

PREVENTION

Resources health

Virtual Machines
Networking
SQL
Applications

HIGH SEVERITY 14
MEDIUM SEVERITY 26
LOW SEVERITY 2

Recommendations

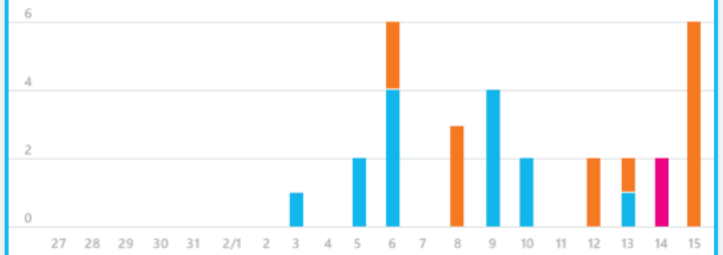
12 TOTAL

Security policy

QUICKSTART

DETECTION

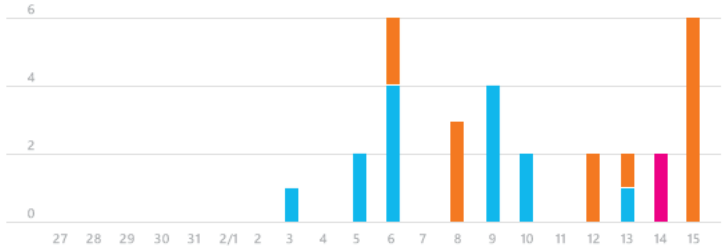
Security alerts



HIGH SEVERITY 2
MID SEVERITY 14
MID SEVERITY 14

Security alerts

Filter



HIGH SEVERITY 2
MEDIUM SEVERITY 14
LOW SEVERITY 14

ALERT	COUNT	DETECTED BY	DATE	STATE	SEVERITY
Suspicious process found	6	Microsoft	7/15	Open	
Traffic to malicious IP 90.150.112.27	1	Microsoft	7/14	Open	
Brute force attempts were detecte...	1	Microsoft	7/14	Open	
SQL injection attempt from 90.15...	1	Barracuda WAF	7/13	Open	
A user account password has been...	1	Microsoft	7/13	Open	
Critical malware action failed	1	Trend micro	7/12	Open	
Exploitable process detected (sql-s...	1	Microsoft	7/12	Open	
Non-critical malware action failed	1	Trend micro	7/10	Open	
Traffic to malicious IP 104.12.112.1...	1	Microsoft	7/10	Open	
SQL injection attempt from 103.33...	4	Microsoft	7/9	Open	
Traffic to malicious IP 121.14.112.3...	1	Microsoft	7/8	Open	
Brute force attempts were detect.e..	2	F5 Network	7/8	Open	
DDOS attack from 103.14.120.12.3...	2	Barracuda WAF	7/6	Open	
SQL injection attempt from 103.3...	4	Barracuda WAF	7/6	Open	
Non-critical malware action failed	2	Trend micro	7/5	Open	
Traffic to malicious IP 103.14.120.9...	1	Microsoft	7/3	Open	

Traffic to malicious IP 90.150.112.27

VIRTUAL MACHINE 1

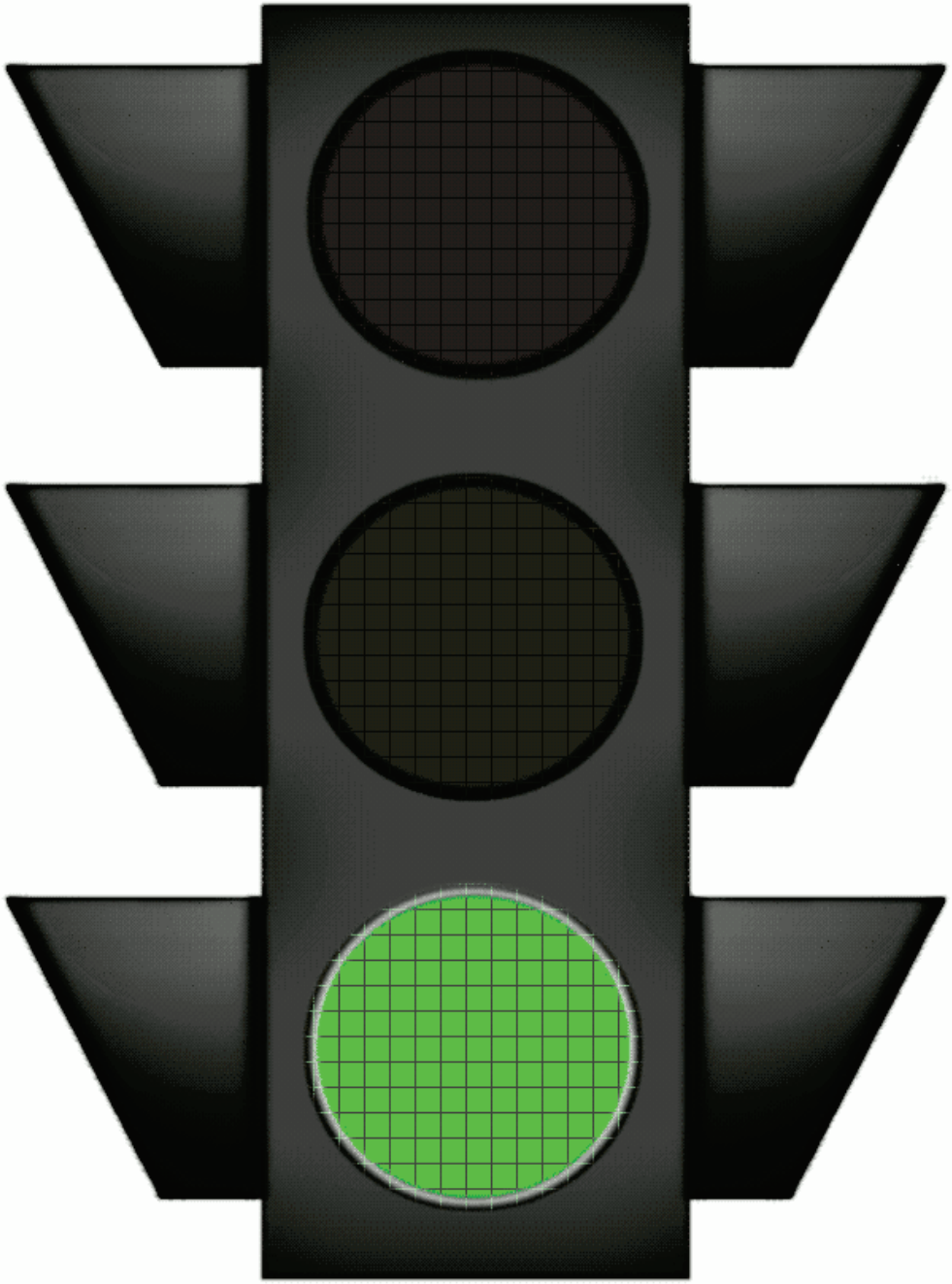
Traffic to malicious IP 90.150.112.27 was detected originating from IP 138.91.9.51 (Virtual Machine 1). IP 90.150.112.27 is known to be part of the Simda botnet. Remediate by running an anti-virus scan and blacklisting IP 90.150.112.27 in the ACL

ALERT	Traffic to malicious IP 90.150.112.27
TIMESTAMP	Tuesday, July 14th, 2015 12:03:55 AM
COUNT	1
DETECTED BY	Microsoft
SEVERITY	High
ACTION TAKEN	Detected
ATTACKED RESOURCE	Virtual Machine 1
RESOURCE VIP	138.91.9.51
RESOURCE LOCATION	West US
ATTACKER IP	90.150.112.27
ATTACKER LOCATION	Russia

Threat map

Moving Forward

Discussion



Thank you

stuartm@microsoft.com