



2004 - 2008





Application Layer Security Appliances
- Hardened Hardware Appliance
- Unified Platform and Configuration Management
- IDC: Unit volume leader for Purpose-built Security Appliance

2009 - 2010



Deployment Extensions
- Virtualizing all Barracuda Appliances
- VMWare, HyperV, KVM, Proxmox … etc.

New Product Families (acquisitions + organic)
- Next Generation Firewall
- Data Security and Protection Products
- Web Application Delivery and Security

2011 - 2013

Added SAAS Offerings

- Remove the need to rack & stack, hardware or virtual
  - Email Security Service
  - Web Security Service
- Centralized Management for dispersed IT organizations
  - Barracuda Control Center for Next Generation Firewall
  - Barracuda Cloud Control
  - Barracuda Appliance Control
- Public Cloud Deployments started to emerge
  - AWS
  - Azure

2014 - 2016



Architecture Enhancements

- Microservices
  - Advanced Persistent Threat Detection, Sandboxing
  - Link Protection that protects the user at the point of click
  - IP Reputation
  - Domain Reputation
- API-enabled Solutions
  - Office 365 Graph APIs
  - Cloud native APIs for telemetry as well as instrumentation

2017 - Now

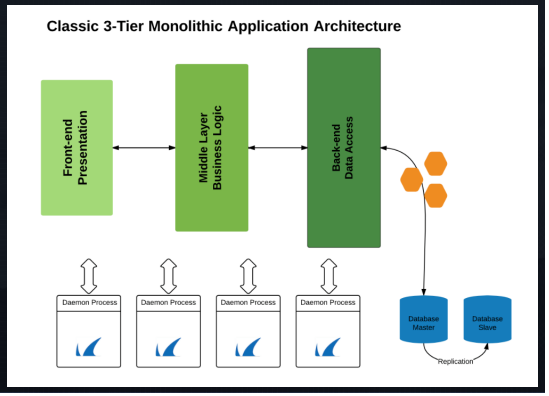
Architecture Enhancements

- Containerize
  - GCP Kubernetes
  - Platform support for Docker and Kubernetes
- Leveraging AI and Machine Learning
  - Attacks without malicious links nor attachments
  - Intent, tone analysis of conversations
  - Anomaly detection in web application protection by modeling and analyzing web traffic

Software Architecture Trends

Sample monolithic application architecture

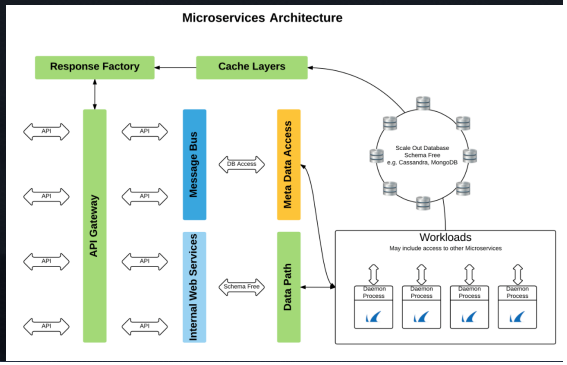
- Frontend
- Middleware
- Backend



Software Architecture Trends

Sample microservice

- API enabled
- Message bus based
- Rich cache layers
- Relational DB
  Document DB
  Distributed Access
  Eventual Consistency



State of Cybersecurity In 5 Areas

Email

Web Application

Secured Connectivity

Cloud Security

Data

Stats and more stats

$172B

Amount consumers who were victims of cybercrime globally lost

30%

Of all organizations were infected by ransomware

61%

Organizations that have experienced an IoT security incident

16M

MOBILE DEVICES INFECTED WORLDWIDE

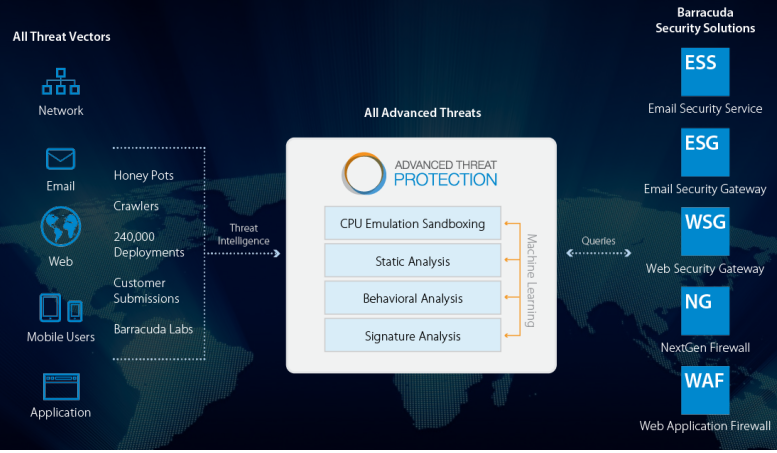
191

Average days it takes to identify a data breach

88%

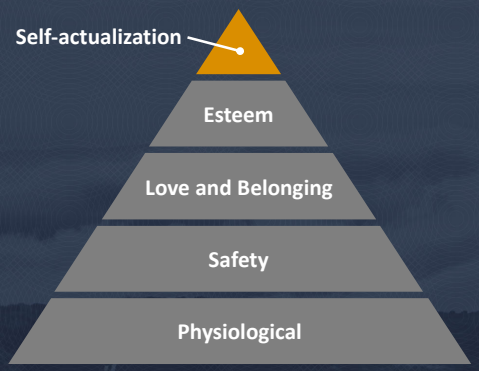
Companies that spent more than $1MM on GDPR preparation

Barracuda's ATP

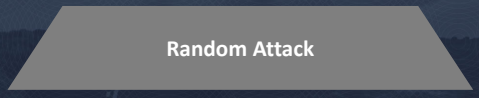




Maslow's hierarchy of needs



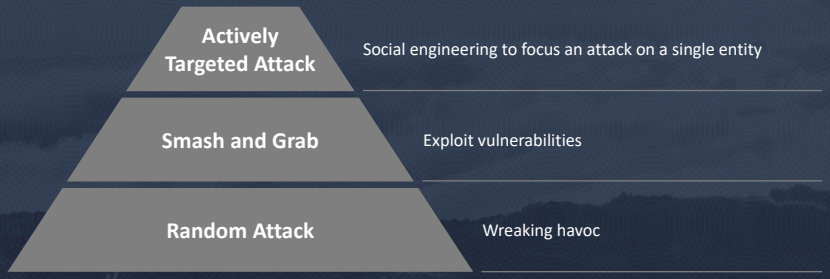
Hierarchy of security threats



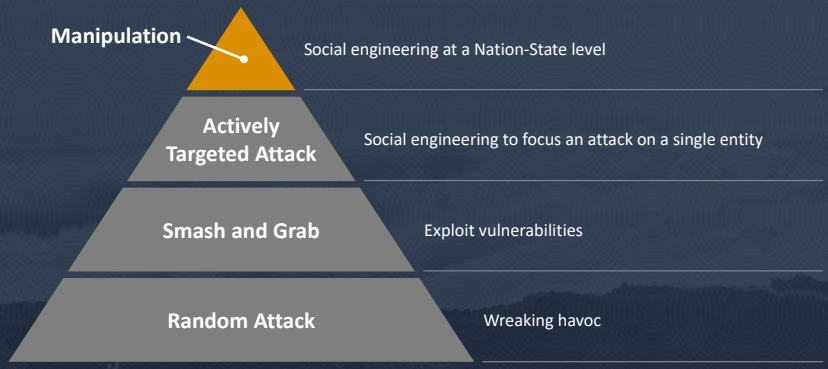
Hierarchy of security threats



Hierarchy of security threats



Hierarchy of security threats





Petya

When: March 2016 (First Seen)

What: A class of Ransomware

NotPetya

When: Reported on Tuesday, 27.June.2017

What: Wiper Malware

Origin: EternalBlue exploit

Leaked by: Team System DZ

Impact: >2,000 reported infections

Initial Target: Organizations in the Ukraine

How does it spread?

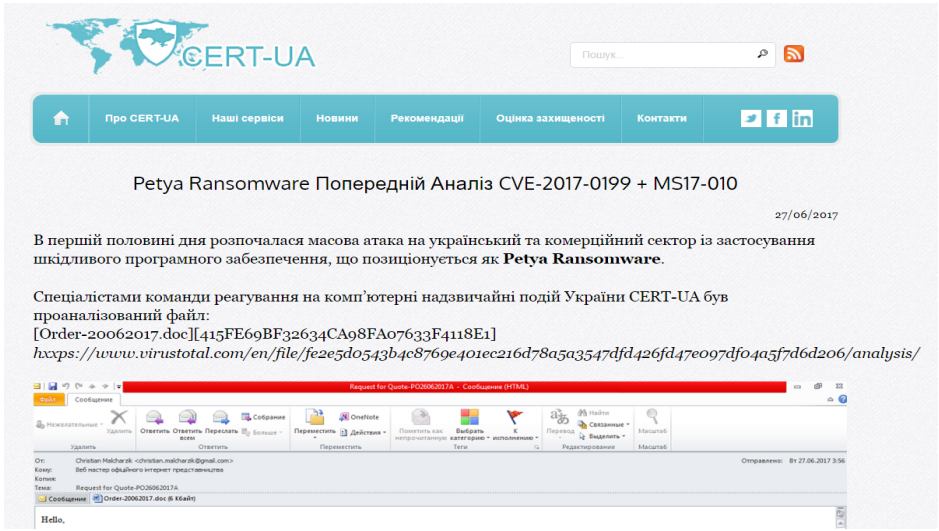
Method of delivery: M.E.Doc software update, Email Vector

Cause: EternalBlue exploit

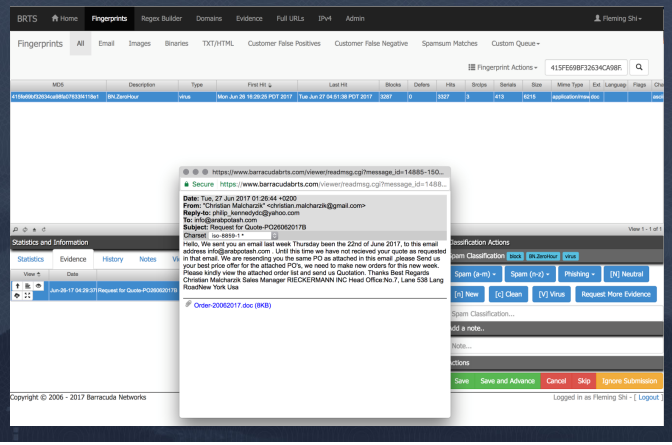
Effect: Has the ability to worm through computer networks gathering passwords and credentials to spread itself

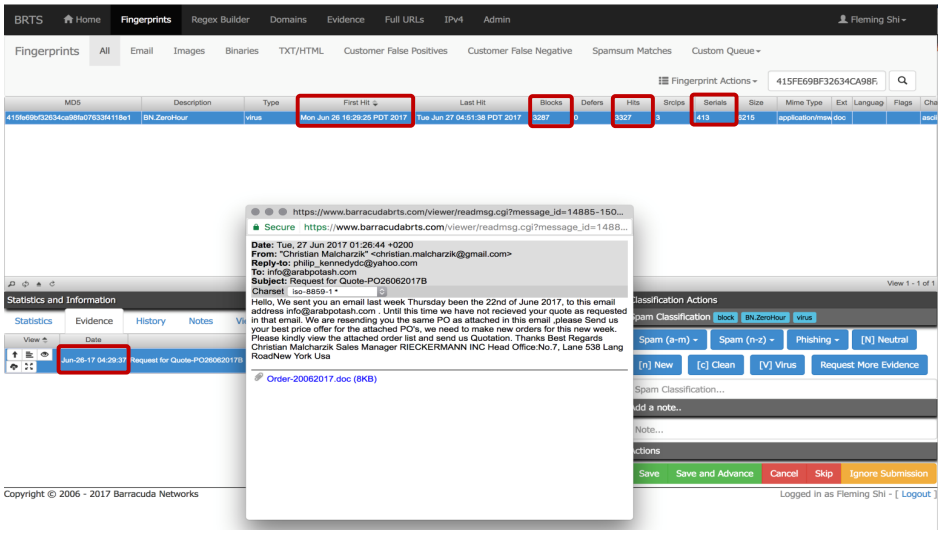
Infection:

- Unrecoverable encryption and damage of system MBR/MFT (master file table)



The Evidence in BRTS





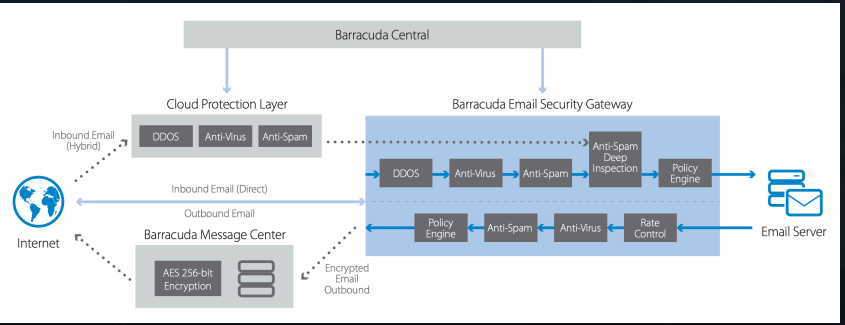
Attacks Executed

Attack 1 :
Auto Update

Attack 2:
Email

Attack 0:
Content Injection

Highlight the technology





File Threat Statistics

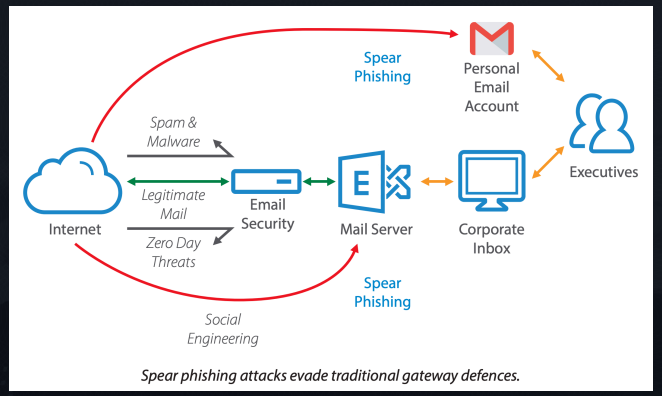
	Clean		Malicious		Suspicious	
File Type	Count	%	Count	%	Count	%
PDF	452168896	85.52	29781	0.01	76524712	14.47
MS Office	94583578	90.99	38882	0.04	9331928	8.98
Compressed	6274124	99.68	18767	0.30	1440	0.02
Markup	3319530	100.00	83	0.00	71	0.00
Portable Executable	1303995	92.72	96085	6.83	6299	0.45
Data	864888	100.00	0	0.00	0	0.00
Script	140261	89.24	0	0.00	16907	10.76

1D 1W 1M 4M

Beyond APT, Phishing, Spear Phishing

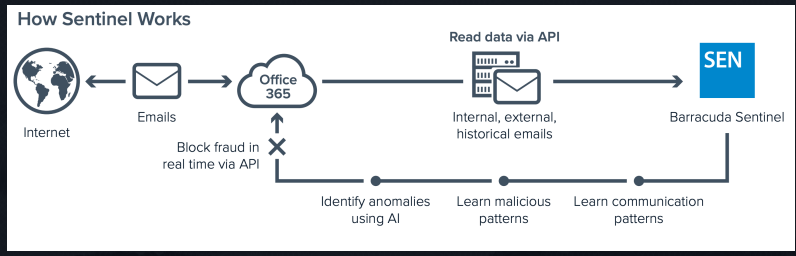
Detail	Phishing	Spear Phishing
Contains link(s) to a malicious site	●	–
Sent to many people	●	–
Personalized	–	●
Primary goal	Steal credentials or credit card information	Wire transfer, SSNs, credentials

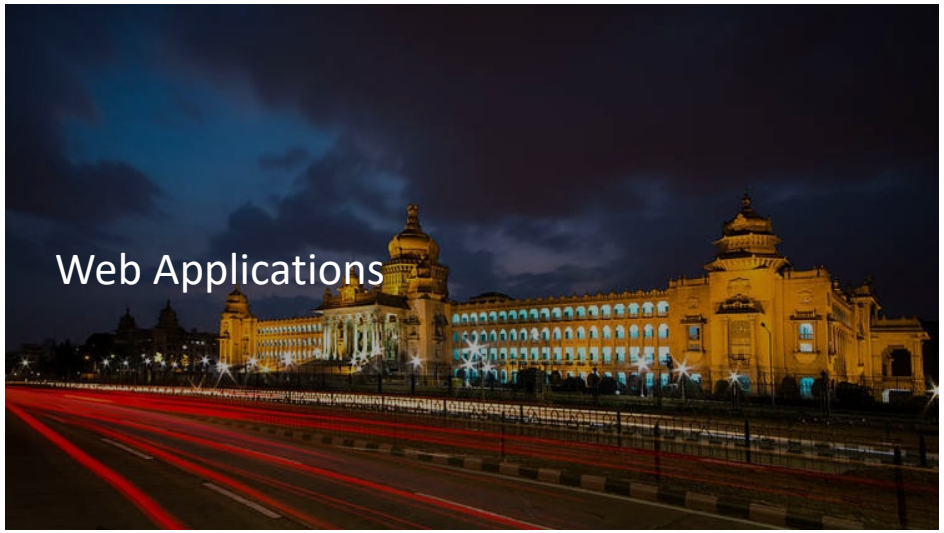
Spear Phishing, Tougher to Defend



Spear phishing attacks evade traditional gateway defences.

Our Answer to Spear Phishing





Misunderstood, inadequately covered

10 % of apps are protected by WAFs today

Web applications are the **#1 attack vector** leading to data breaches

- Verizon DBIR

Back to “NotPetya”

When: Reported on Tuesday, 27.June.2017

What: Wiper Malware

Origin: EternalBlue exploit

Leaked by: Team System DZ

Impact: >2,000 reported infections

Initial Target: Organizations in the Ukraine

Attacks Executed

Attack 1 :
Auto Update



Attack 2:
Email



Attack 0:
Content Injection

me doc
МІЙ ЕЛЕКТРОННИЙ ДОКУМЕНТ

OWASP Top 10

When: March 2016 (First Seen)

What: A class of Ransomware

NotPetya

When: Reported on Tuesday, 27.June.2017

What: Wiper Malware

Origin: EternalBlue exploit

Leaked by: Team System DZ

Impact: >2,000 reported infections

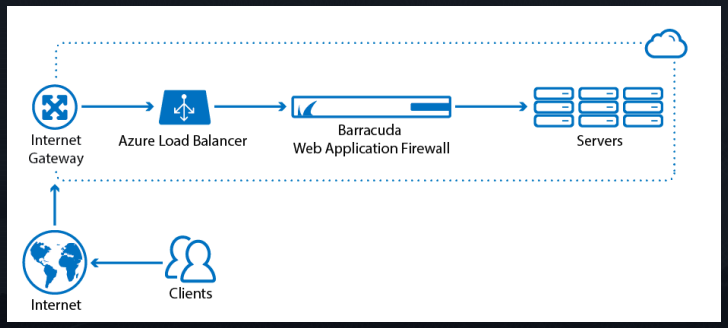
Initial Target: Organizations in the Ukraine

OWASP Top 10

2017

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging and Monitoring

Highlight the technology





Back to “NotPetya”

When: Reported on Tuesday, 27.June.2017

What: Wiper Malware

Origin: EternalBlue exploit

Leaked by: Team System DZ

Impact: >2,000 reported infections

Initial Target: Organizations in the Ukraine

Attacks Executed

Attack 1 :
Auto Update

Attack 2:
Email

Attack 0:
Content Injection

Review: Attacks Executed

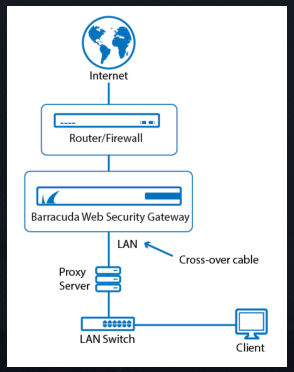
Attack 1 :
Auto Update

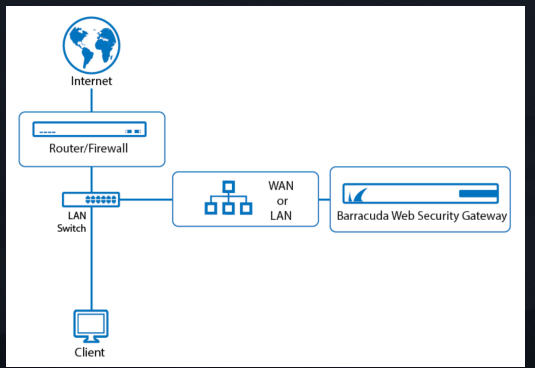
Attack 2:
Email

Attack 0:
Content Injection

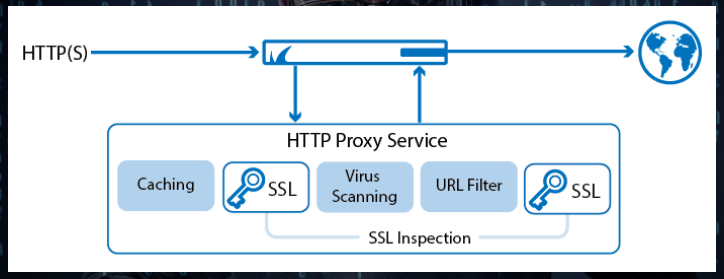
me doc
МІЙ ЕЛЕКТРОННИЙ ДОКУМЕНТ

How do you scan for malware





How about Encrypted Traffic



IoT beyond your household smart devices

Explosive Evolution of IoT

IoTs talk to the Service Mesh

- Million of entry points
- Networking from home, ISP to Central Service to other homes

Industrial IoT maybe running antiquated OSs

- Automated updates can cause systems to be vulnerable
- Reluctance in upgrades due to production needs
- Ransomware attacks can disable the entire production line

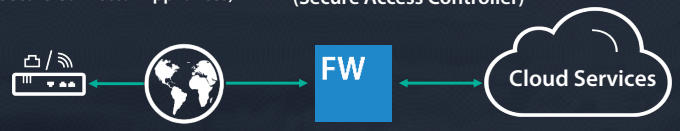
Barracuda Security Solution for IIoT



IIoT / OT „Edge Device“
(Secure Connector Appliances)

IIoT „Hub“
(Secure Access Controller)

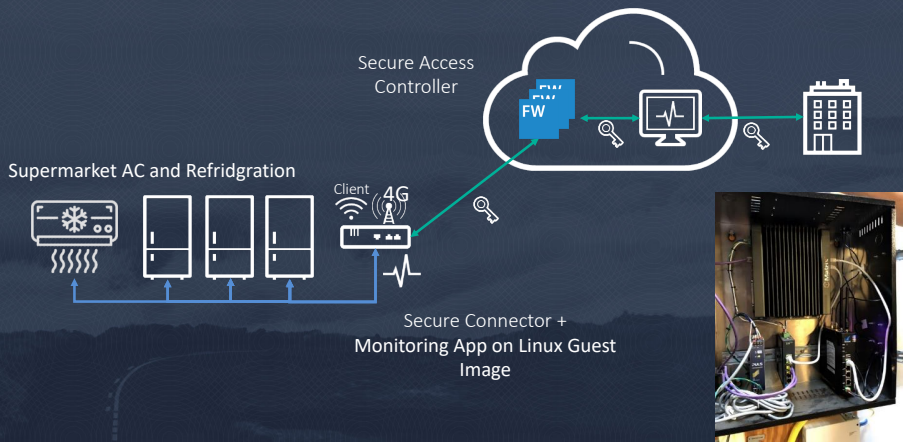
Control Application



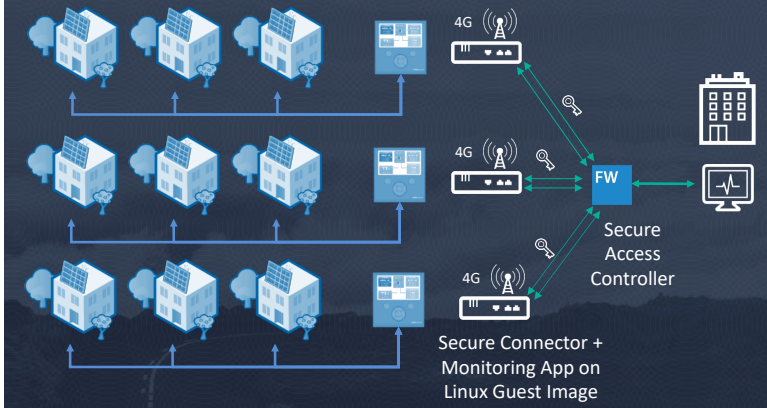
Edge Computing
Predictable Maintenance
Shielding/Cloaking
Strong Authentication
Secure Communication
Zero Touch Deployment

Access Security Broker
Access Control
Anti-Malware
Advanced Threat Protection
Protocol Analysis
Audit Trail

US/NL Airconditioning as a Service

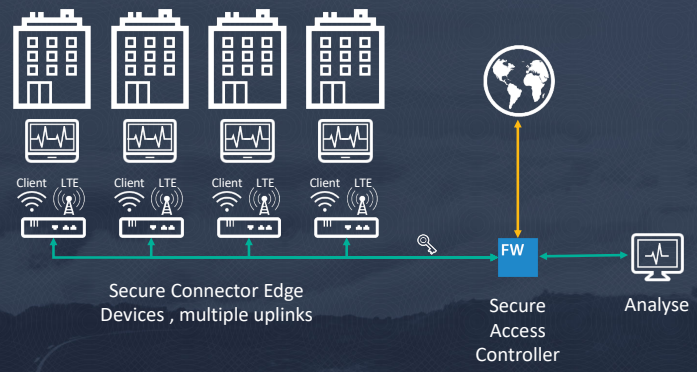


DE: Power Grid Monitoring





DE: Smart City Project





Cloud presents new challenges

IaaS AWS, Azure, GCP and OCI

- Inherent Complexity
- Visibility of Assets
- IAM
- Configuration Drifts

Can you trust your infrastructure

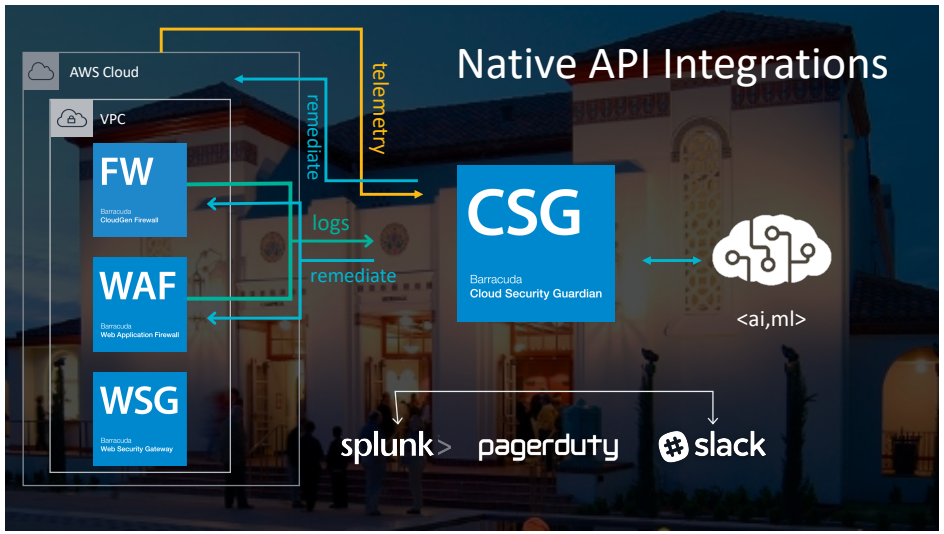
- Native controls
- Rehydration if you can afford to

} “dev:sec:ops” // Information Security

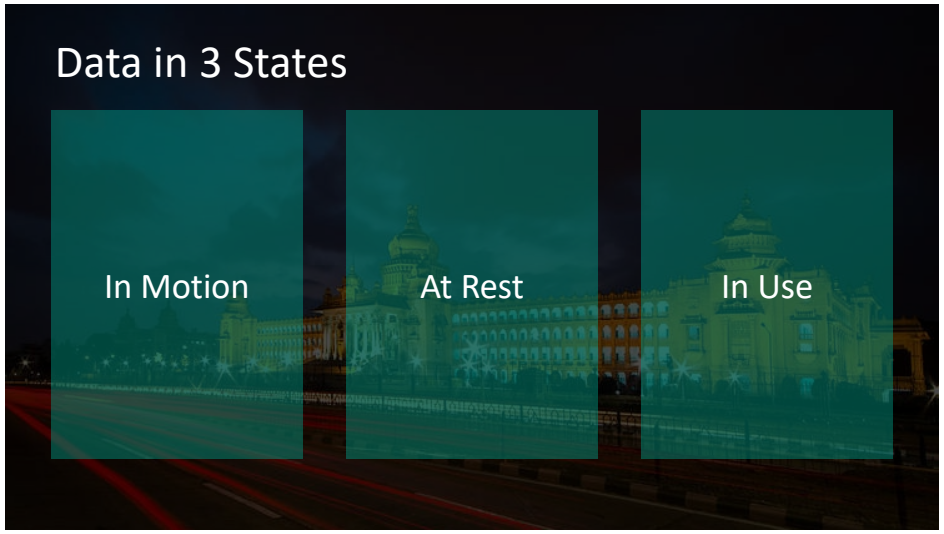


Software engineer	Risk professional
Cloud expertise, no security	‘Cloud challenged’, sec pros
API only interface	GUI with centralized management
Open source tools	Established ISVs
Hard to reach	Well established Marketing channel
Self-consumption of products (marketplace) open PO	POs through established channel
Metered-billing	Licenses



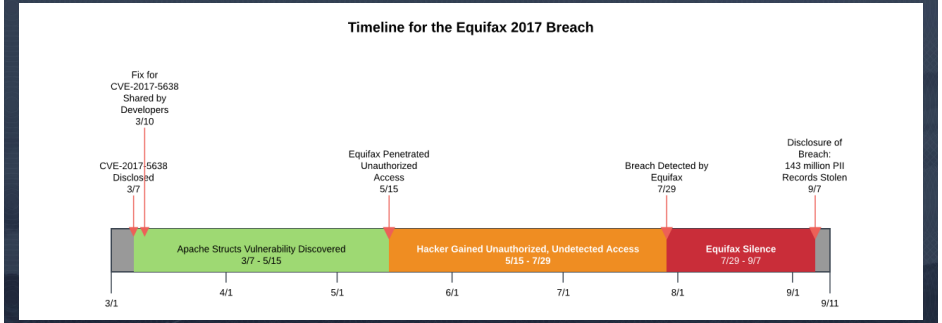

Native API Integrations
AWS Cloud
VPC
FW
Barracuda
CloudGen Firewall
WAF
Barracuda
Web Application Firewall
WSG
Barracuda
Web Security Gateway
telemetry
remediate
logs
remediate
CSG
Barracuda
Cloud Security Guardian
<ai,ml>
splunk>
pagerduty
slack


Data
MICHIGAN
STOP

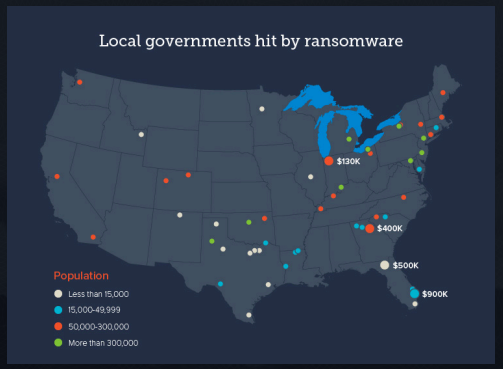

Data in 3 States
In Motion
At Rest
In Use


What happened at Equifax?

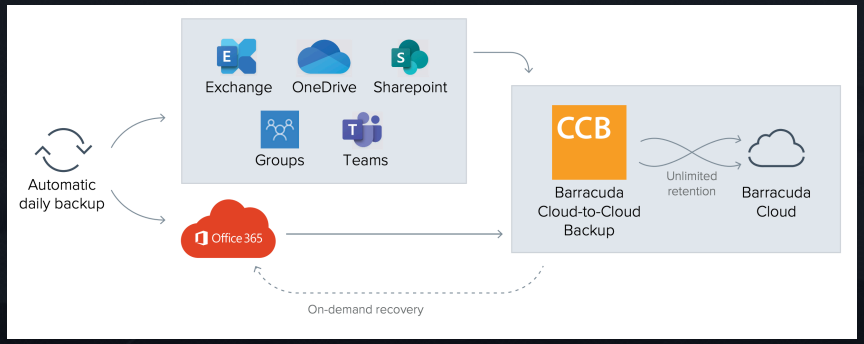
Equifax



Ransomware against Municipalities



Recovery from Ransomware Attacks



And now a story



Kongming (諸葛亮)

Imperial Chancellor

Han Dynasty, 181AD -234AD



Red Cliff (赤壁)

The Battle of Red Cliffs

草船借箭

AD 208-209

