



New Darwinism in Enterprise Security



Angelo Gentili

PartnerNET Business Development Manager

Need
to adapt

Theory of Evolution

Becoming
adept

Network and data center environments have evolved



Why businesses must act over wearable security threats now

IT and IT consumerization
HAS CHANGED...



Posted by Ben Ross on 13 January 2015



Everything pushed to web = more is up for grabs to attackers



**Enterprise
Application**



**Banking
Networks**



**Critical
Infrastructure**



Retail



Healthcare



**Government &
Research
Organizations**

Departure from “Conventional” to “Disruptive”

- Many enterprises are fighting new threats and evolved threat actors with old weapons
- Security gaps facilitate backdoors in enterprise networks, allowing attackers to feast on vulnerabilities and negligence
- And we have **EXAMPLES** that prove it...

Departure from “Conventional” to “Disruptive”



Malware mayhem and security assault continues...

2013

Year of Data breach;

*world's leading
organizations suffer
network hack and
data compromise;
face law-suits in
millions, lose trade-
secrets, equity and
customer confidence*



2014

They broke the web

From stabbing the heart of the secure Internet (SSL) to the widespread scare of ransomware, 2014 elevated security concerns and broke the web with new threats.

1. Heartbleed
2. Cryptowall
3. POODLE
4. GNU Bash a.k.a. Shellshock



Internet of Things is here

ARE WE READY?

YES

NO

There is a widening gap between what security executives believe to be true and the reality of evolved cyber-threats

Gaps that open back-doors and create blind-spots


Absence of security measures that can thwart breaches

- User provisioning
- Patching
- Monitoring and compliance
- Intrusion Prevention / malware detection & protection
- Vulnerability scanning
- Control & Visibility
- Secure network
- Security for Virtual or Cloud environment

DO YOU AGREE?

YES

NO



**WHAT SUPER
CIO_s
SHOULD DO?**

#1

SUIT UP FOR CYBER BATTLEFIELDS

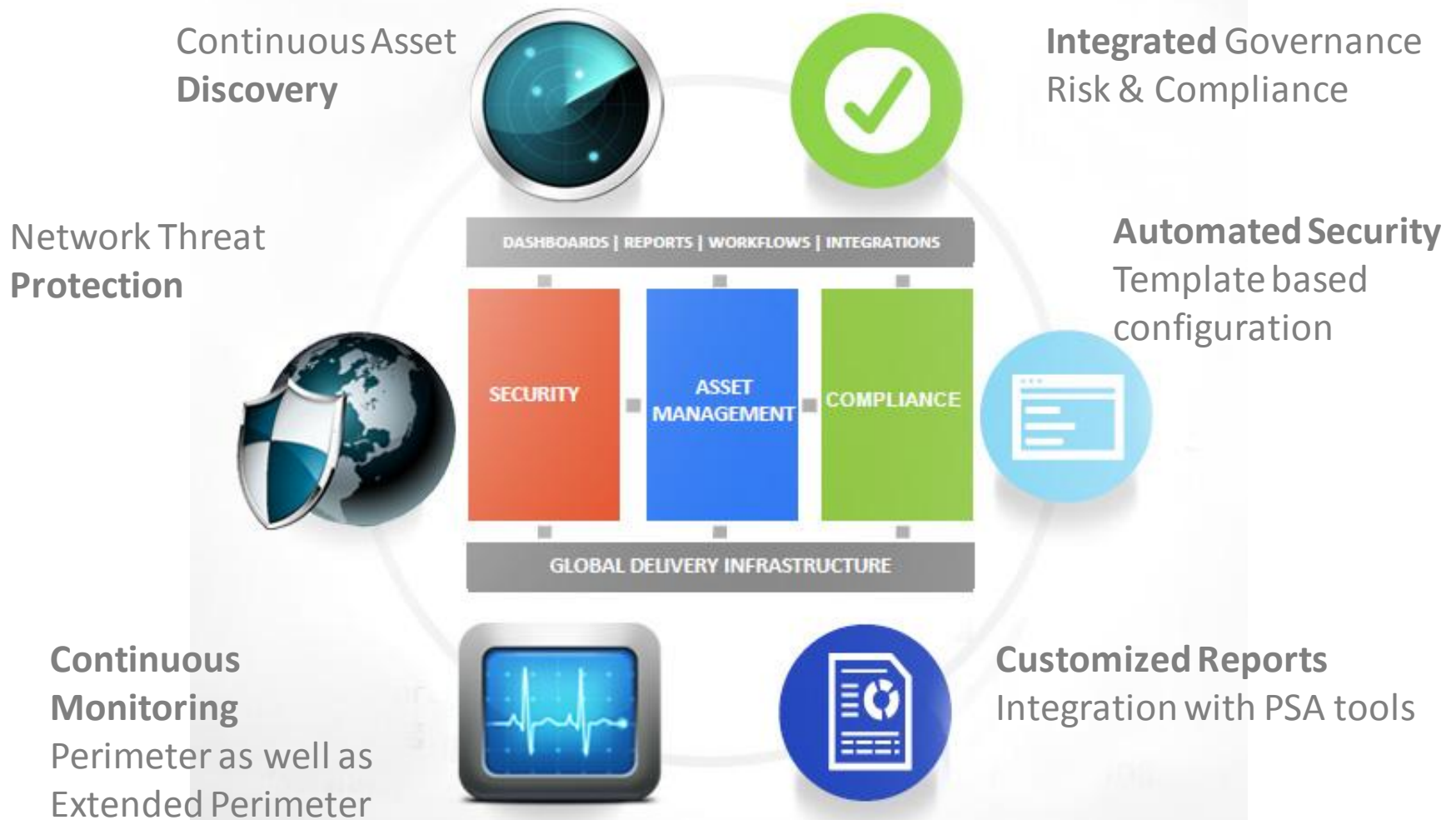
#2

EMBRACE SECURITY IN ITS NEW AVATAR



How Cyberoam has evolved Enterprise Security?

The approach goes like this...




We observe that most

- Developing the right Matrix to strengthen security and enable productivity is the REAL challenge
- Do you agree?

YES

NO



Need to transform traditional enterprise and reinvent IT

Need to ensure BYOD, Cloud and Virtualization and other trends do not widen security gap

The business goals of an organization and the security goals have to be mutually reinforcing.

Cyberoam gives CXOs the power to harmonize Security, Productivity & Compliance

DATA LEAKAGE
PREVENTION

REAL-TIME
VISIBILITY
AND CONTROL

SECURE BYOD,
CLOUD &
VIRTUALIZATION

PERFORMANCE

BUSINESS
CONTINUITY

SLAs

ZERO HOUR MALWARE
PROTECTION

REGULATORY
COMPLIANCE

ACTIONABLE
SECURITY
INTELLIGENCE

User Threat Quotient The Eagle Eye of Cyber World





Can you spot the Risky Users?

YES

NO



Spot Risky Users with UTQ

Introducing UTQ for allowed and denied web traffic

Traffic Dashboard Security Dashboard User Threat Quotient (UTQ)

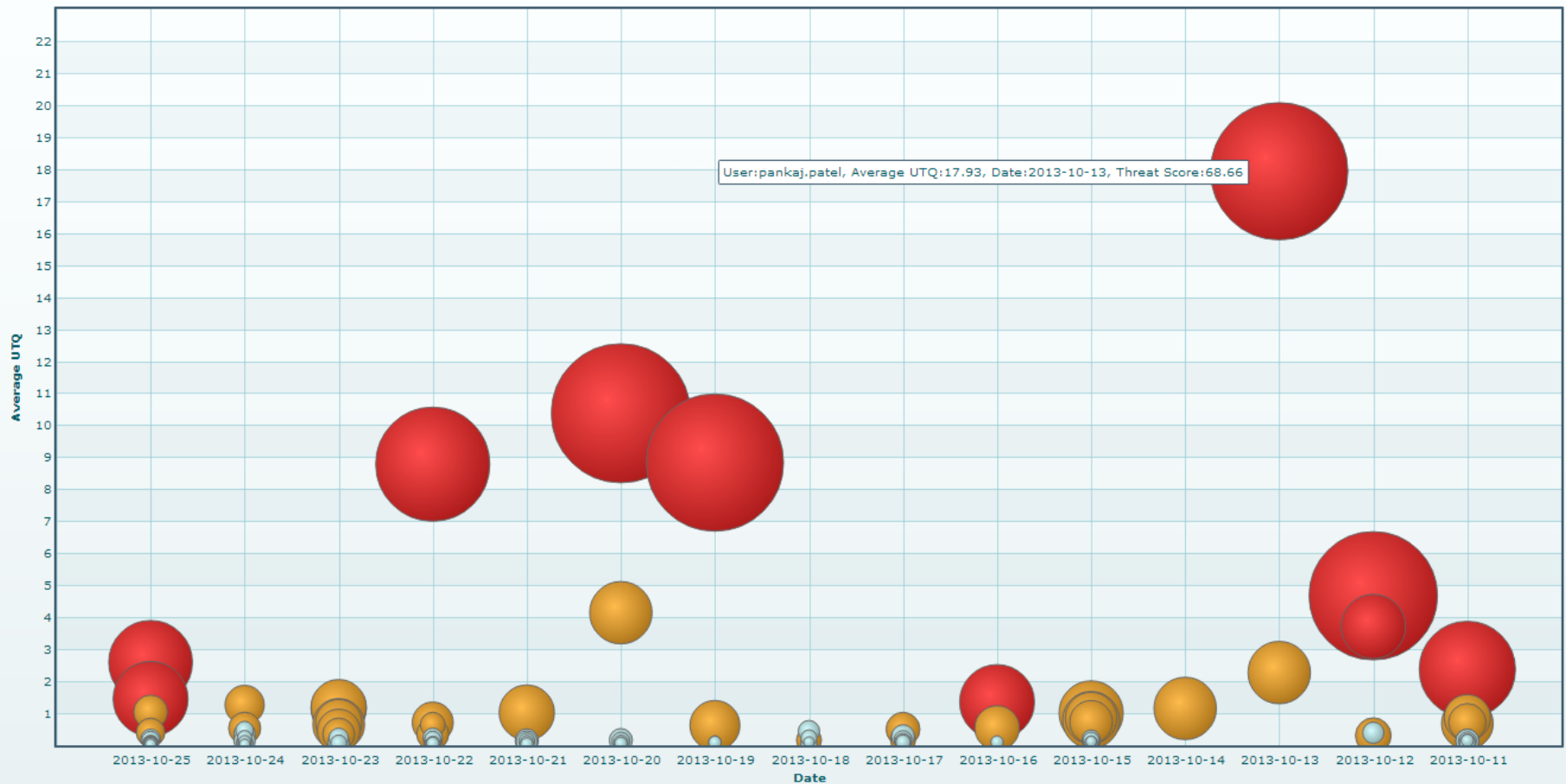


2013-10-25

Last 30 Days

Last 15 Days

Users with highest UTQ

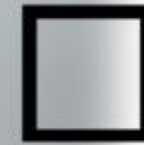


Cyberoam's Recommendations



Threat Modeling

- Identify and document critical assets in your infrastructure
- Identify and document each component in the system
- Identify and document possible points of attack
- Identify and document threats that pertain each possible attack point
- Identify and document the category and priority of the attack
- Identify and document the Mitigation solutions
- Monitor the security controls
- Re-evaluate security Controls





Partner

NET

SMART ICT DISTRIBUTION

Thank you

Presenter name: **Angelo Gentili**

Designation: **Business Development Manager**

Contact: **sales@partnernet.gr**