YOUR SECURITY SEEN FROM THE OUTSIDE

LA TUA SICUREZZA, VISTA DAL DI FUORI

Guglielmo BONDIONI,
Riccardo ZANZOTTERA

CONVEGNO ABI
BANCHE E SICUREZZA 2015
Roma – 5 Giugno 2015

FASTWEB

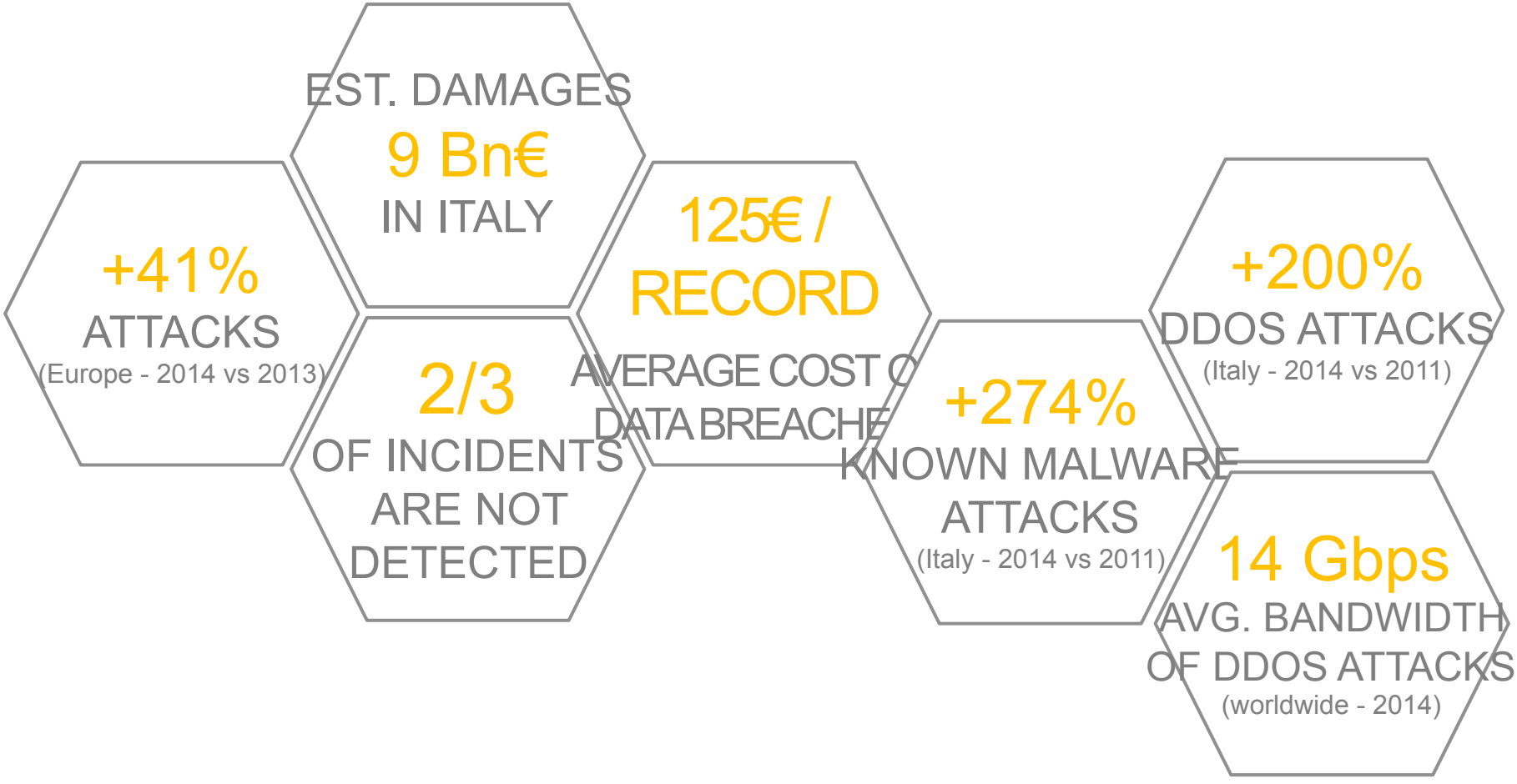
AGENDA

- **CYBERCRIME AND THE SME SCENARIO**
- **ICT SECURITY: LA VISIONE ED I SERVIZI DI FASTWEB PER LE IMPRESE**
- **CONCLUSIONI**

CYBERCRIME AND THE SME SCENARIO

GUGLIELMO BONDIONI
MANAGER OF ICT SECURITY
FASTWEB S.P.A.

CYBERCRIME IN NUMBERS



Sources: Rapporto Clusit 2015, PWC Security® Survey 2015, Ponemon Institute 2015, Akamai 2014

CYBERCRIME: WHAT WE SEE

As an ISP, Fastweb receives and manages notices about abuse and vulnerable or compromised customers, from individuals, independent organisations, partners and Government institutions.

Of these:

- **5%** are about residential customers
- **15%** are about large customers
- **80%** are about SMEs

CYBERCRIME: WHY?

Why are SMEs attacked or abused so prevalently?

SME SCENARIO: ONLINE!

You run a business.

Your business needs a website to sell or showcase its products, gather leads, or offer a service to its customers.

Or maybe you need to automate some business process.

Website and basic IT development skills are readily available and affordable.
So are computing power and network connectivity.

So **you roll your own and you're online in no time and with little expense**.

SME SCENARIO: SOMETHING'S WRONG

So far, so good: you're online and your business thrives.

Until your website stops sending email to your customers.

Or until somebody calls you and asks why your website has a page to steal credit card information from Bank X.

Or until your network becomes slow and your website goes offline.

Or until somebody calls you and says something incomprehensible about 'botnets'.

SME SCENARIO: WHAT'S GOING ON?

What happened?

By rolling out your website or service, you created something that can be reached by anybody on the Internet.

In other words, you created an **attack surface**.

After a while, somebody took advantage of that attack surface to co-opt your computers and resources into working for them.

SME SCENARIO: NOT MY BUSINESS?

But why would anyone attack my website?

My business doesn't do anything sensitive!

It isn't even that visible!

Most threats to SMEs are opportunistic:

1. they are **not** after your business
2. they use your resources to conduct illegal activity
3. they **scan the whole Internet** looking for opportunities

SME SCENARIO: WHY

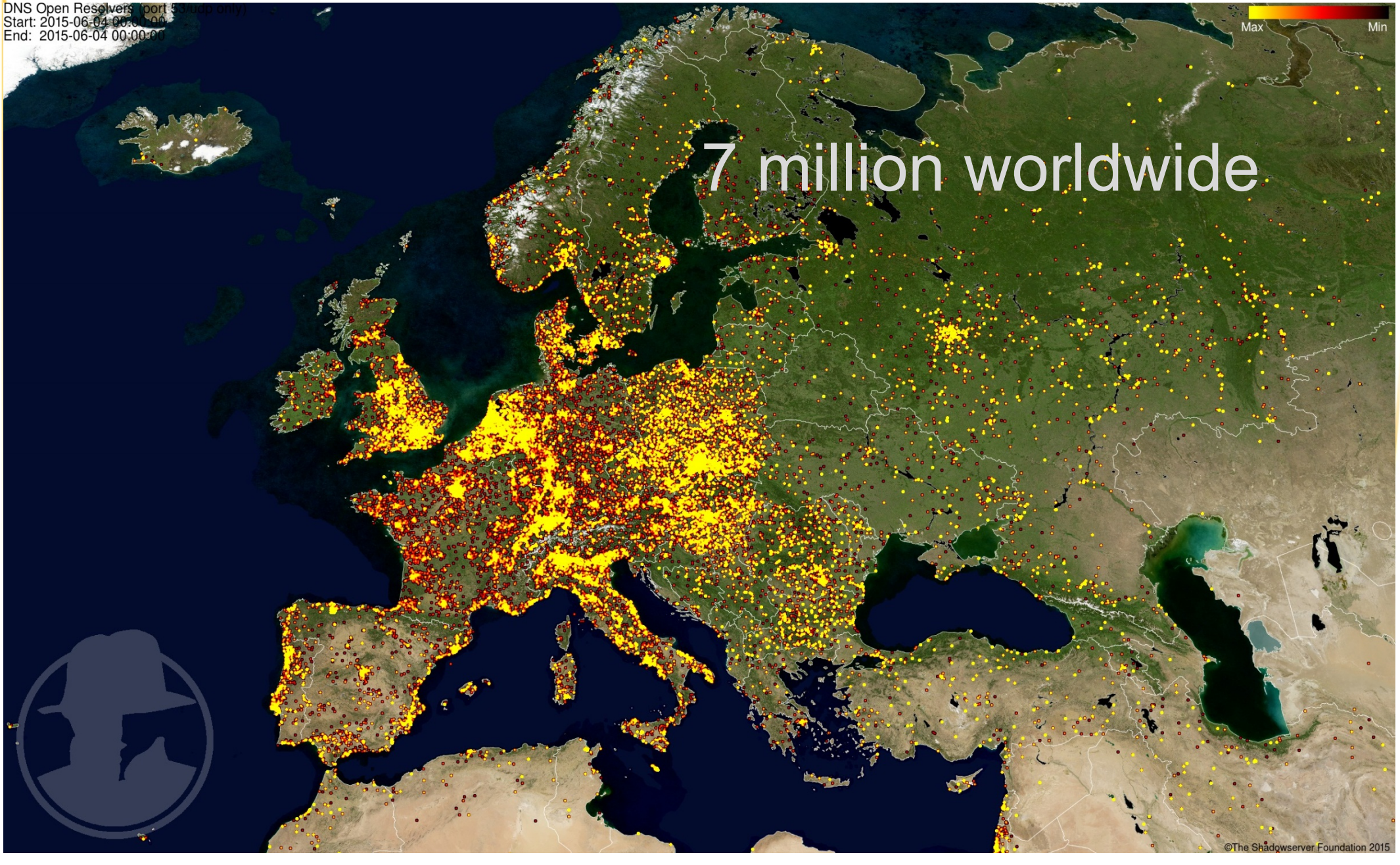
What are these opportunistic threats?

- Spam (abusing your email server to send spam email)
  - *Your website stops sending email to your customers*
- Phishing (abusing your website to steal credit card / banking info)
  - *Somebody calls you asking why*
- Denial-of-service attacks (abusing your network bandwidth to attack others)
  - *Your network gets slow and your website goes offline*
- Command & Control (abusing your computers to command thousands of other compromised ones)
  - *Somebody calls you and says something about 'botnets'*

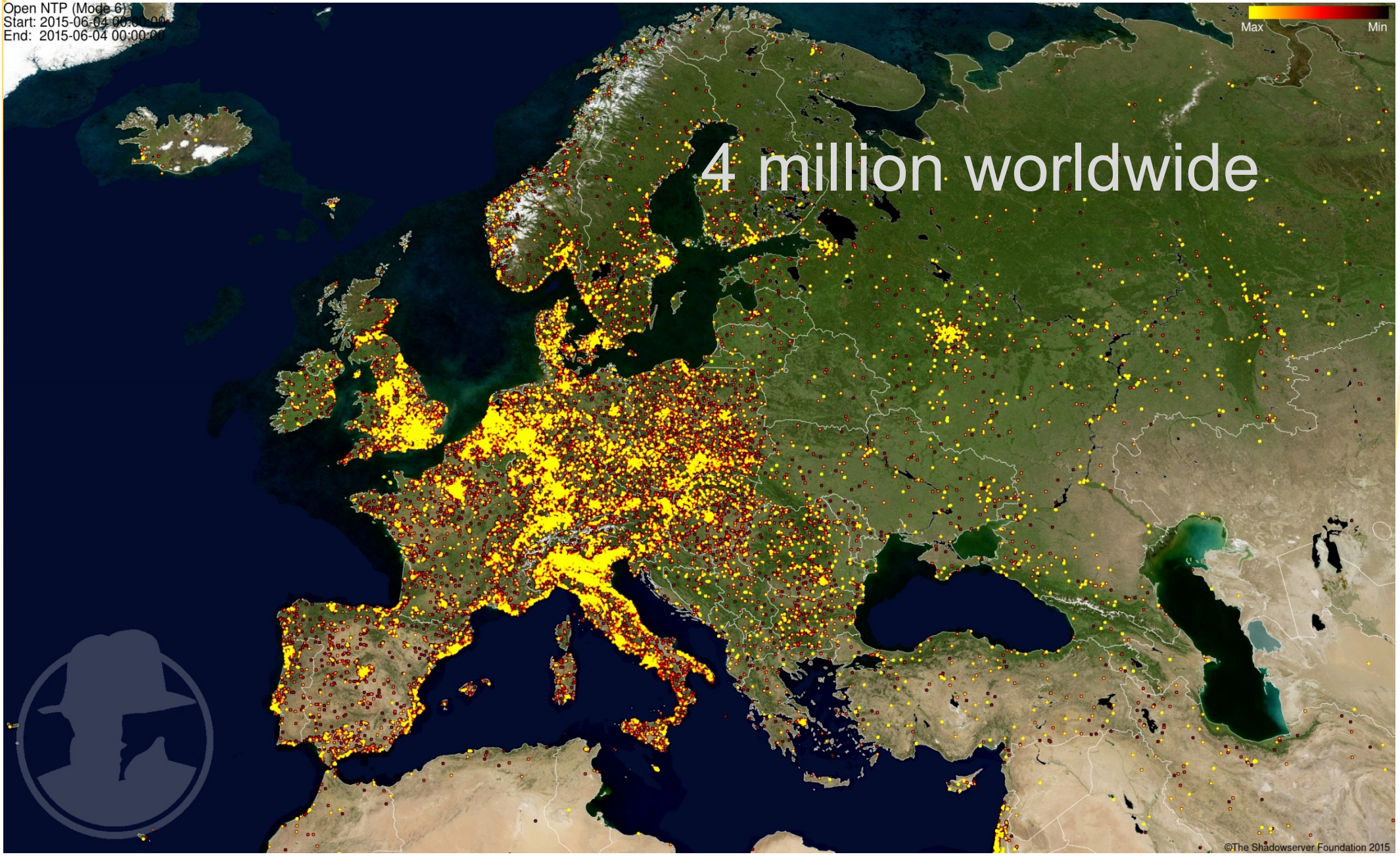
SME SCENARIO: SO COMMON?

Are these vulnerabilities actually that common?

SME SCENARIO: VULNERABLE



SME SCENARIO: VULNERABLE



SME SCENARIO: WHY SMEs?

Residential customers offer little to no attack surface to these threats.

Large organisations do have attack surfaces, but they also have processes, people and resources to manage ICT security risks.

SMEs have attack surfaces but need to focus on their business, not computer security.

Unfortunately, ICT security skills are expensive and hard to find.

But fortunately, they can be outsourced!

ICT SECURITY:
LA VISIONE ED I SERVIZI DI FASTWEB PER LE IMPRESE

RICCARDO ZANZOTTERA
MARKETING PRODUCT MANAGER
FASTWEB S.P.A.

ICT SECURITY: la visione di FASTWEB

La natura delle minacce e gli effetti rimangono costanti (e pericolosi), lo scenario evolve!

CAUSE

INTENZIONALI / MALEVOLE

ompromissione dati/funzionalit

Azioni non autorizzate

ACCIDENTALI

roblema tecnico - Errore uman

Disastro ambientale

Attacchi evoluti
on molteplici vettori d'ingresso

Identità dinamica
su internet

ud

Dati non più confinati
in ambienti segregati

EFFETTI

Furto di dati riservati

Compromissione dei sistemi ICT

Interruzione dei servizi

Concorrenza sleale

Danno d'immagine

GLI ELEMENTI CHIAVE DI UNA GESTIONE STRATEGICA DEL RISCHIO ICT

FOCUS SULLA PROTEZIONE DEL DATO IN UN AMBIENTE NON DELIMITABILE

EVOLUZIONE TECNOLOGICA CONTINUA

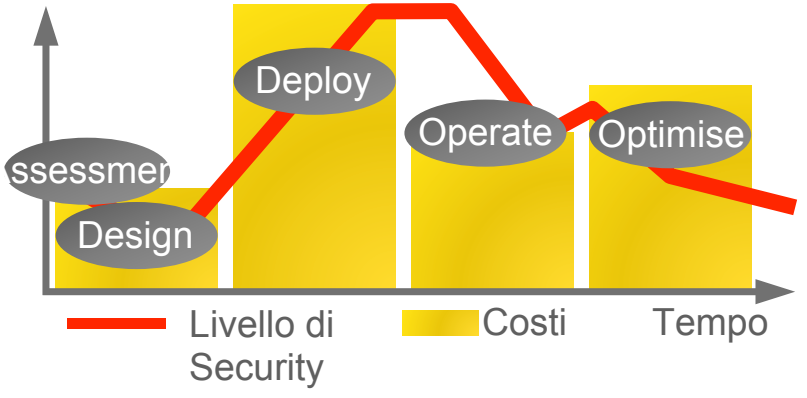
APPROCCIO ADATTATIVO

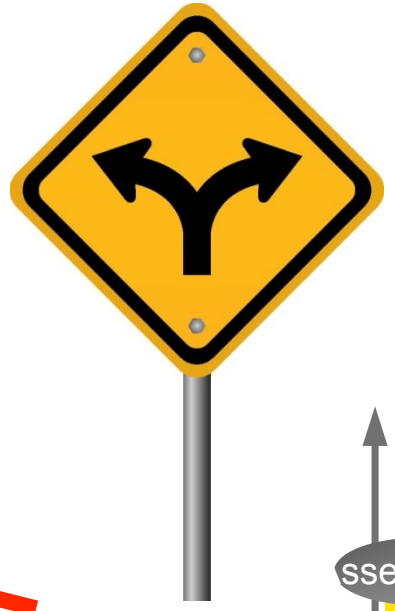
ELEVATA CAPACITA' di GOVERNANCE

IL MODELLO MANAGED SECURITY SERVICES

IN HOUSE

Governance
Processi
Competenze
Tecnologia

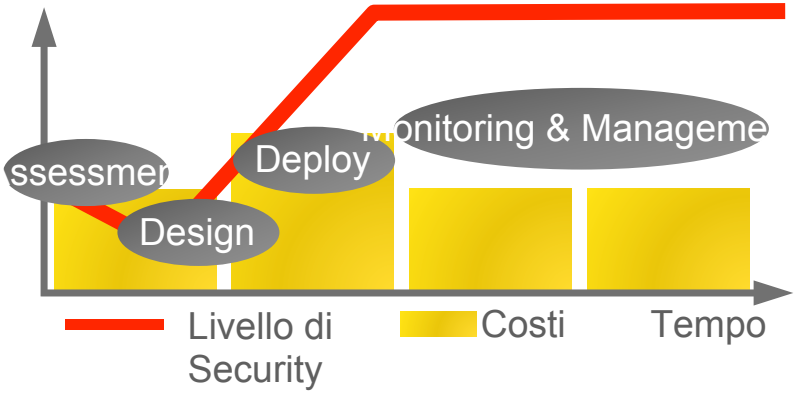




MSSP / FASTWEB

Governance

Processi
Competenze
Tecnologia



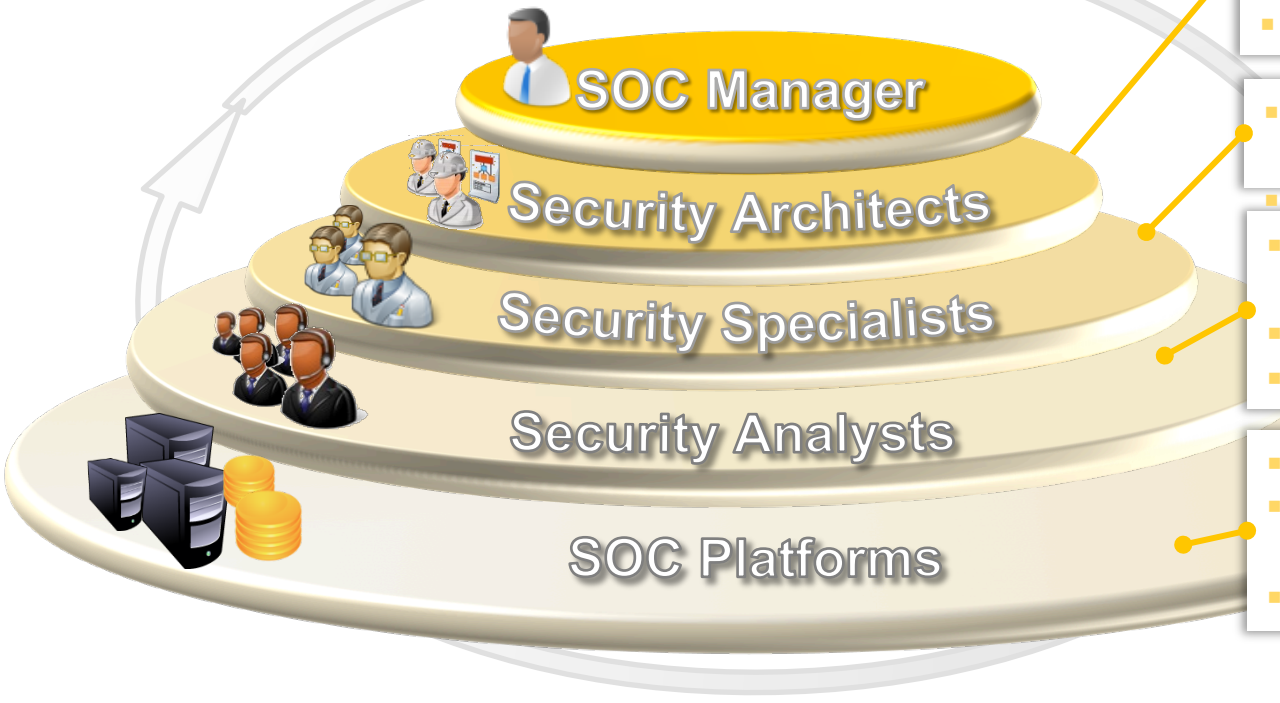
MODELLO OPERATIVO ED ASSET

Processi e procedure operative certificati

ISO/IEC 27001:2005

Personale pluricertificato in ambito security (CISP, CISM)

Copertura **H24 x 365**



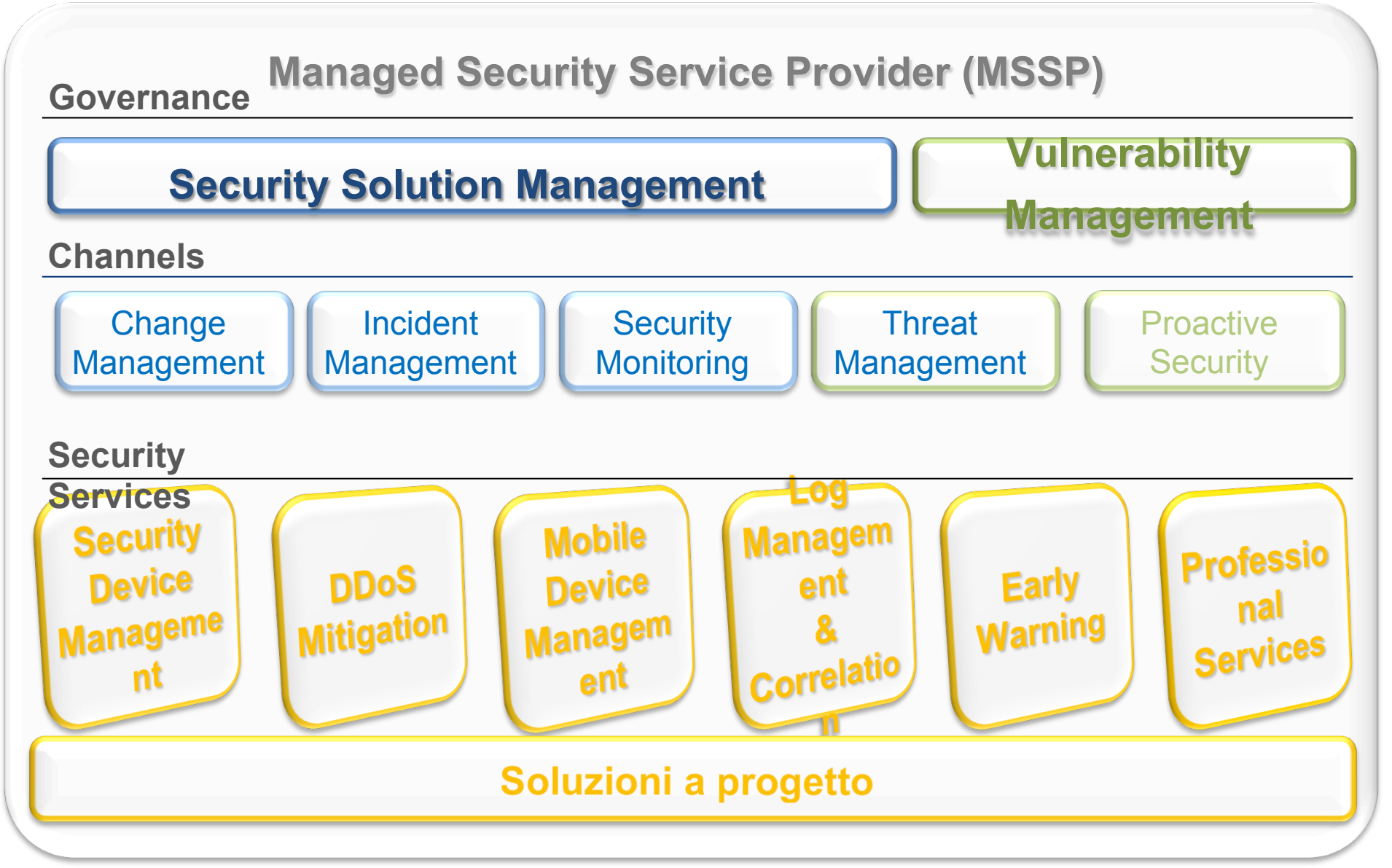
- Supporto progettazione
- Vendor Selection
- Escalation terzo livello

- Escalation secondo livello
- Incident management

- Primo punto di contatto
- Presidio H24
- Analisi Proattiva Eventi

- Piattaforma SIEM
- Infrastruttura Anti DDoS
- Sistemi di controllo e monitoraggio

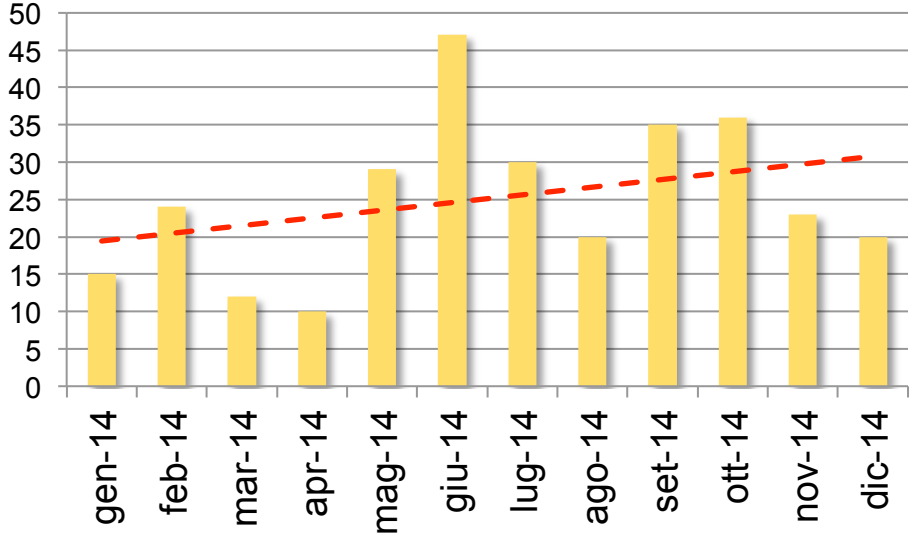
L'OFFERTA FASTWEB



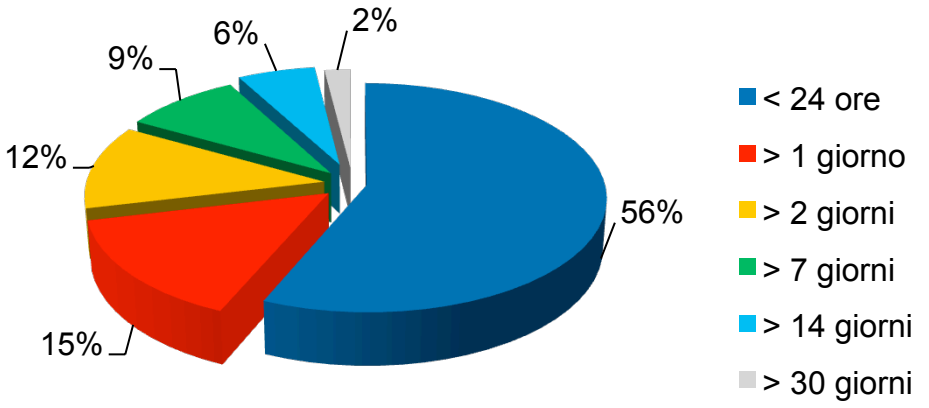
FOCUS su DDoS MITIGATION

Il punto di osservazione di chi ges FASTWEB zza

MITIGATION ATTIVATE - 2014

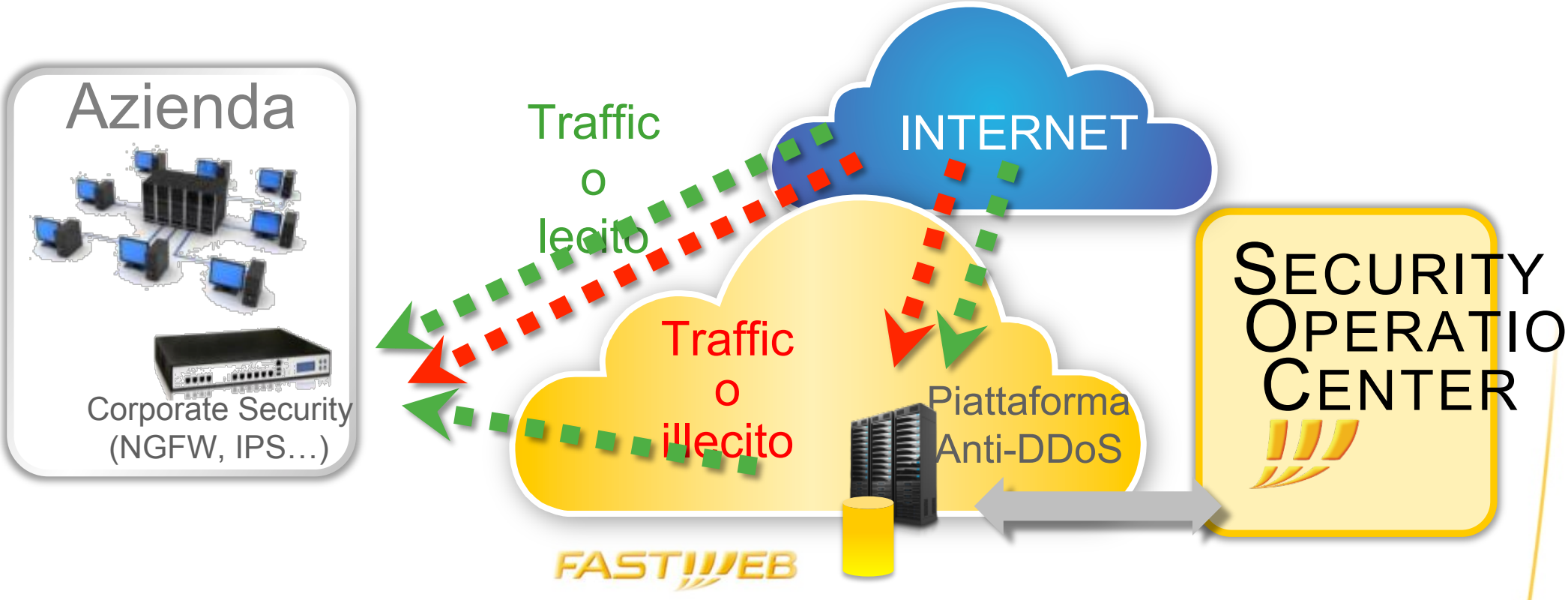


DURATA ATTACCHI DDOS - 2014



DDoS FENOMENO IN CRESCITA e SEMPRE PIU' IMPATTANTE

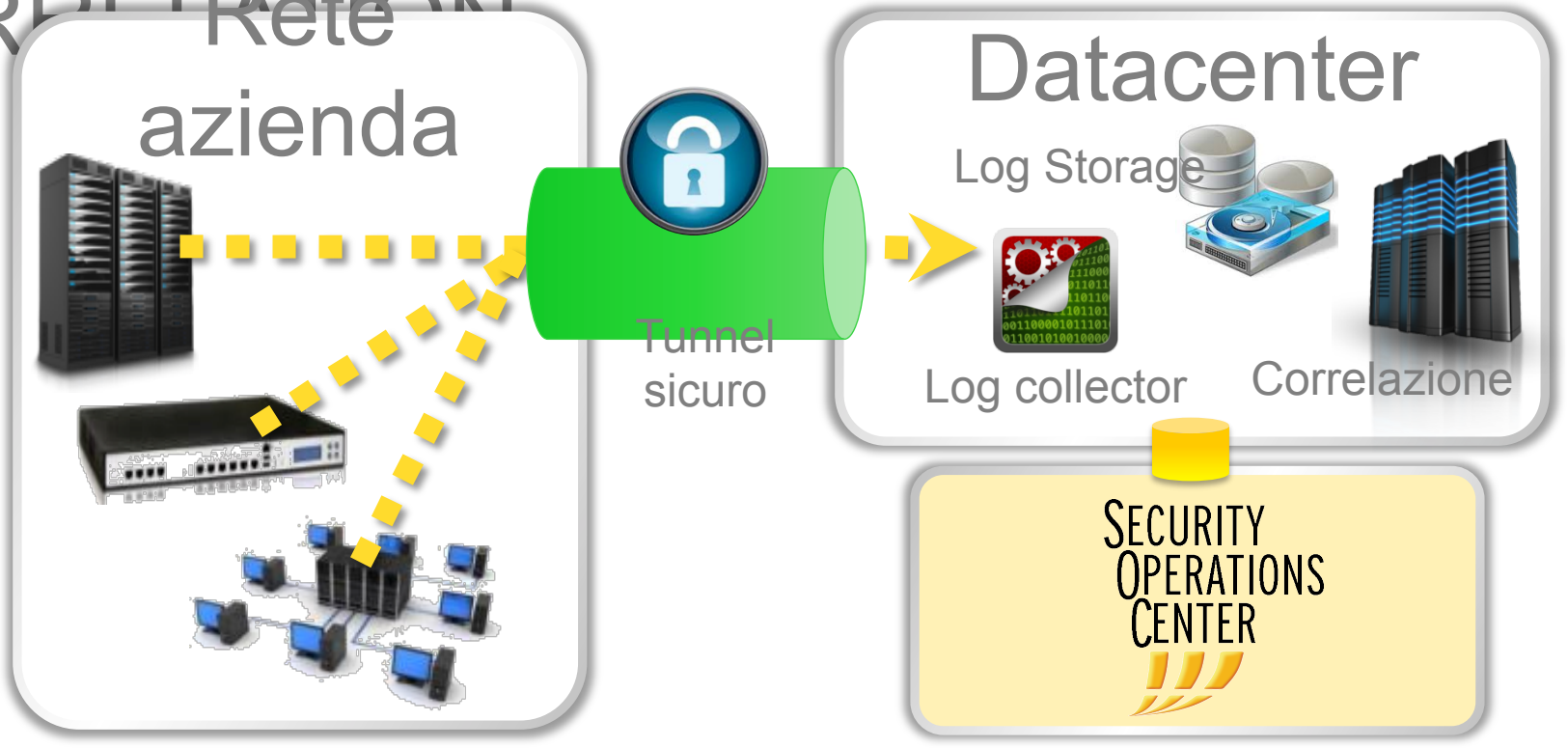
DDoS MITIGATION: come funziona



ISP + MSSP : un ruolo chiave

Controllando connettività e piattaforme tecnologiche, il Service Provider è l'unico soggetto in grado di intervenire efficacemente in quanto può operare sia presso il Cliente che a livello di accesso alla rete

FOCUS su LOG MANAGEMENT & CORRELATION



Servizi

- Raccolta e archiviazione a norma dei log
- Analisi log e reporting
- Real time Security alerting

Vantaggi

- Compliance normativa e PCI-DSS
- Supporto all'individuazione di frodi
- Presidio pro-attivo con monitoring REAL-TIME dei tentativi di intrusione

CONCLUSIONI

I NUOVI MODELLI DI BUSINESS PUNTANO SU CLOUD, SOCIAL e MOBILITY

I POSSIBILI VETTORI D'ATTACCO AUMENTANO

LA SICUREZZA PERIMETRALE NON È SUFFICIENTE

SERVE UNA DIFESA ADATTATIVA E MULTI-LIVELLO

LA SFIDA SULLA SICUREZZA NON È E NON SARÀ PIÙ SOLO SULLE TECNOLOGIE MA SULLE COMPETENZE

GRAZIE