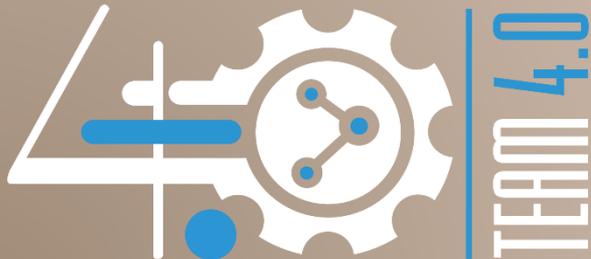




**Ing. Stefano Ferrari**

[steferbs@gmail.com](mailto:steferbs@gmail.com)

*Laureato in Ingegneria Elettronica  
Network and Security engineer*



**Ordine Ingegneri della provincia di Brescia**

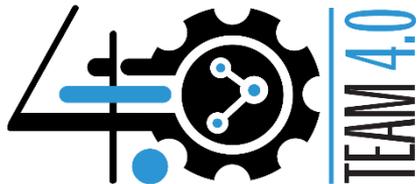
Commissione ICT



Stefano Ferrari  
[steferbs@gmail.com](mailto:steferbs@gmail.com)

# Cyber Security: quanto sono sicuri i dati nelle reti aziendali?

I rischi per la sicurezza in Industry 4.0



# AGENDA

- Security e CyberSecurity
- Industria 4.0 e CyberSecurity
- Wannacry: l'input per la Cybersecurity
- Procedure straordinarie e ordinarie di difesa
- Approccio integrato alla Cybersecurity

# Security e CyberSecurity

- \* **Sicurezza:** Prevenzione, eliminazione parziale o totale di danni, pericoli, rischi; condizione di essere al sicuro.
  - \* Si chiudono le porte blindate, ma si lasciano aperte le finestre.
- \* **CyberSecurity:** è più estesa della IT Security in quanto riguarda ogni aspetto della nostra vita
  - \* Smartwatch a basso costo che inviano i nostri dati in Cina
  - \* Smart TV che ci tengono d'occhio
  - \* Attacchi ad automobili

# Security e CyberSecurity

- \* La sicurezza è un pesante fardello di cui ci si vuole liberare.
- \* I clienti vogliono qualcuno che gli gestisca la security perché non hanno personale con un adeguato livello di competenze.
- \* Il Cloud è la panacea, la soluzione che ci libera da tutti i pensieri
  - \* Non si può mettere il dato in una scatola nera
  - \* Deve essere controllato e mandato in modo sicuro
  - \* La qualità del dato (Integrità e Disponibilità) deve essere garantita
  - \* Conoscenza dei dati sensibili

# Security e CyberSecurity

- \* Nel GDPR (General Data Protection Regulation) il dato è assimilato al trasporto di materiale pericoloso
  - \* Se tocco il dato devo avere la certezza che non si provochino danni
- \* ART.32
  - \* «Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto **misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio...**»

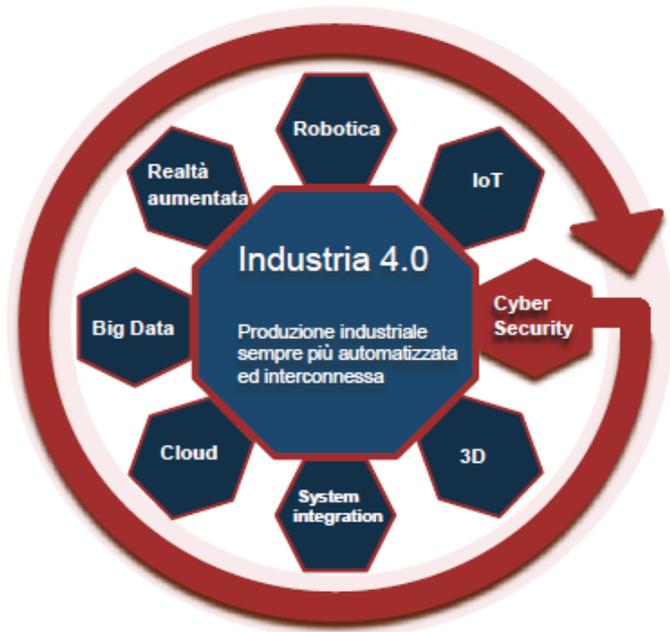
# Security e CyberSecurity

## \* ART.34

\* «In caso di violazione dei dati personali, il titolare del trattamento **notifica la violazione** all'autorità di controllo competente a norma dell'articolo 55 **senza ingiustificato ritardo** e, ove possibile, **entro 72 ore** dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo. Il **responsabile** del trattamento informa il titolare del trattamento **senza ingiustificato ritardo** dopo essere venuto a conoscenza della violazione»

\* Diventa molto importante il DLP (Data Loss Prevention) specialmente negli studi di Ingegneria

# Industria 4.0 e CyberSecurity



Sistemi di produzione non aggiornabili



Network non segmentata



Interfacce HMI vulnerabili

# Industria 4.0 e CyberSecurity

- \* Macchinari per l'automazione:
  - \* Costosi
  - \* Precisi
  - \* Manuali di migliaia di pagine dove alla voce «collegamento»:
    - \* Utilizzare un Ip pubblico per semplificare le operazioni di accesso remoto
  - \* Spesso utilizzano una piattaforma Android, uno dei maggiori vettori di attacco più popolari
  - \* Si spendono migliaia di € per i lubrificanti per non farli bloccare, ma basta un semplice software gratuito per fermare tutto....

# Industria 4.0 e CyberSecurity

- \* I device IoT sono stati progettati per funzionare con un software semplice
- \* La sicurezza è demandata ad altri
- \* Se ne parla poco nei seminari su industria 4.0
- \* In Europa il tema è molto sentito
- \* Nel 2016 si sono verificati più di 4 mila attacchi al giorno
- \* Bisogna colmare il divario di alfabetizzazione rispetto ai principali concorrenti anche in tema di cybersecurity

# Industria 4.0 e CyberSecurity

Shodan Developers Book View All... Show API Key

SHODAN [Search Bar] Explore Downloads Reports Enterprise Access Contact Us My Account Upgrade

## The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started



### Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.



### See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



### Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



### Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

# Industria 4.0 e CyberSecurity

## Explore Tag: scada

Browse saved searches with the tag: scada

### LIST SEARCHES BY

Popularity

Recently Added

### POPULAR TAGS

webcam	94
cam	74
camera	73
scada	63
ip	45
ftp	45
router	43
http	37
test	34
server	30

<b>2</b>	<b>Industrial routing</b> Product: REX 300, Ethernet Router	<b>14</b>	<b>scada</b> 123123
<b>5</b>	<b>Electro Industries GaugeTech</b> Electro Industries GaugeTech SCAD	<b>3</b>	<b>SCADA SIEMENS S7 CP</b> German SCADA SIEMENS S7 CP
<b>18</b>	<b>Climate Control</b> Climate / Water / Elec control	<b>3</b>	<b>Stulz Climate Control</b> Stulz GmbH Klimotechnik
<b>6</b>	<b>moxa</b> moxa http servers	<b>4</b>	<b>RuggedCom</b> RuggedCom devices, potentially vulnerable to the backdoor issue discovered in 2012.
		<b>4</b>	<b>Schneider PCL</b> sysdiag:factorycast@schneider

# Industria 4.0 e CyberSecurity

Exploits

Maps

Like 14

Download Results

Create Report

## TOTAL RESULTS

81

## TOP COUNTRIES



United States	27
Russian Federation	17
Taiwan, Province of China	8
France	8
Spain	4

## TOP SERVICES

SNMP	76
Modbus	2
16323	1
503	1
NetBIOS	1

## RELATED TAGS:

scada

102-40-100-140-14.ugmk-telecom.ru  
**UGMK-Telecom network**  
Added on 2017-05-04 07:07:14 GMT  
Russian Federation, Kemerovo  
[Details](#)

TELEMECANIQUE BMX P34 2020 REV0250 Modicon M340 CPU 340-20,Ethernet TCP/IP

102-201-231-05.lightspeed.rcsnbx.sbcglobal.net  
**AT&T U-verse**  
Added on 2017-05-04 03:08:15 GMT  
United States, Tyler  
[Details](#)

TELEMECANIQUE BMX P34 2020 REV0200 Modicon M340 CPU 340-20,Ethernet TCP/IP

104-185-08-208.lightspeed.frsnca.sbcglobal.net  
**Orange**  
Added on 2017-05-04 02:30:26 GMT  
France  
[Details](#)

Schneider-Electric BMX NOE 0100 REV0310 Modicon M340 Ethernet 1 Port 10/100 RJ45

104-185-08-208.lightspeed.frsnca.sbcglobal.net  
**AT&T U-verse**  
Added on 2017-05-04 00:14:00 GMT  
United States

TELEMECANIQUE BMX P34 2020 REV0250 Modicon M340 CPU 340-20,Ethernet TCP/IP

3.12

h06-112-183-12.mcsnet.ca  
**MCSNet**  
Added on 2017-05-02 06:31:55 GMT  
Canada, Camrose  
[Details](#)

ICS

Unit ID: 0

-- Device Identification: Schneider Electric BMX NOE 0100 V2.30

-- CPU module: BMX P34 2020

-- Memory card: BMXRMS008MP

-- Project information: Project - V6.1 W7-CLM-MODICON \\vboxsrv\Projects\01227\semc01227\_july\_06\_16\_v10.st

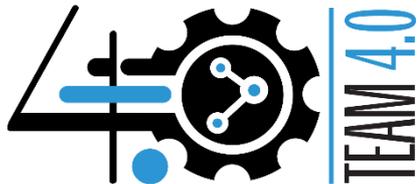
-- Project revision: 0.1.114

-- Project last modified: 2...



Stefano Ferrari  
[steferbs@gmail.com](mailto:steferbs@gmail.com)

# Wannacry: l'input per la Cybersecurity



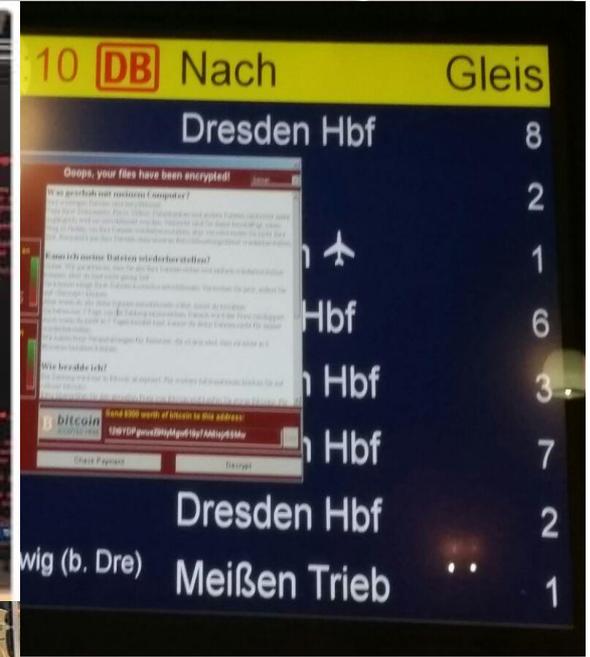
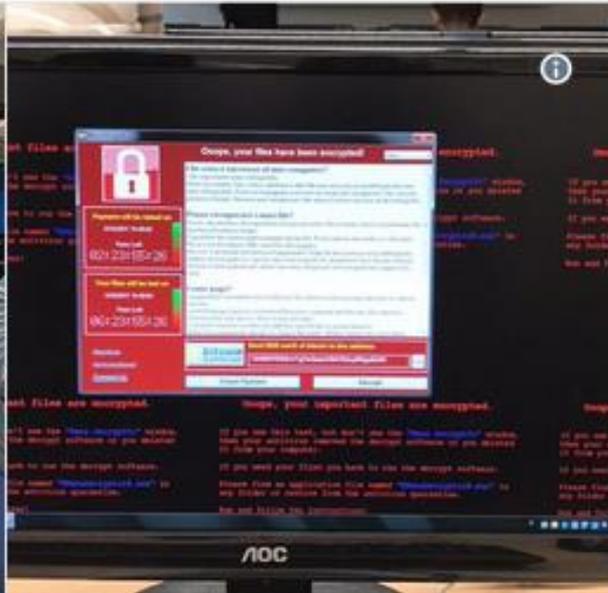
12/05/2017

- \* Si parla di crypto-ransomware, in particolare di WannaCry, un worm che ha infettato migliaia di dispositivi chiedendo un riscatto:
  - \* \$300 in Bitcoin per decryptare i file, \$400 dopo due ore, ecc...
  - \* Se “too poor to pay” allora decrypting gratis ”after 6 months”.
- \* L’attacco è stato bloccato non appena è stato attivato un kill switch:
  - \* [www.iuqerfsodp9ifjaposdfjhgosurijfaewrgwea.com](http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrgwea.com)
- \* Se i client fossero stati aggiornati non sarebbe successo niente

# Chi è stato colpito?

- \* Infrastrutture pubbliche in più di 60 nazioni
- \* Settori di healthcare, telco, gas e compagnie elettriche. Per esempio, la National Health Service in Inghilterra che ha dovuto chiudere gli ospedali e rimandare le operazioni chirurgiche. Telefonica in Spagna. Renault in Francia che ha dovuto fermare la produzione.
- \* Le nazioni più colpite inoltre sono state Russia e Cina, Francia, Taiwan, US, Ucraina e Korea del Sud.
- \* Molti si sono trovati impreparati.

# Chi è stato colpito?



TEAM

# Cos'è un Crypto-ransomware

- \* Un Ransomware è un programma che utilizza messaggi ingannevoli e allarmanti per estorcere denaro alle proprie vittime bloccandone l'utilizzo dei computer o dei dispositivi mobili fino a quando non viene pagato il riscatto
- \* Un Crypto-ransomware è un tipo di Ransomware che cifra i file sui computer e dispositivi mobili in modo che siano illeggibili dall'utilizzatore e viene richiesto di pagare un riscatto per ottenere la chiave di decifratura che è disponibile per un periodo limitato di tempo

# Cos'è un Crypto-ransomware

- \* Spesso vengono sfruttati software trafugati alle organizzazioni governative di sicurezza nazionale
  - \* In questo caso Eternal Blue, cyber arma della NSA.
- \* Viene propagato normalmente mediante un allegato nella mail o exploit kit (software malevoli che sfruttano vulnerabilità del client per iniettare codice malevolo) installati su siti web poco protetti (Waterhole)
  - \* Wana Decryptor 2.0
- \* Se il pc è in rete può infettare altri pc e di conseguenza anche i file condivisi sui server (specialmente windows xp e windows server 2003)

# Come agisce

- \* Sfrutta una falla nel Server Message Block (SMB) in Microsoft Windows che può permettere esecuzione di codice da remoto.
- \* Si è propagato automaticamente sulle reti come un worm
- \* La proliferazione di WannaCry è stata rallentata da un ricercatore britannico di 22 anni con una spesa di 10€
  - \* ha analizzato una parte del codice e ha capito che c'era un arresto di emergenza (Kill Switch), un dominio inesistente che se creato avrebbe bloccato l'epidemia
  - \* potrebbero esserci altre parti di codice senza kill switch

# Si poteva evitare?

- \* Microsoft mise a disposizione la patch già a Marzo (MS17-010), ma....
  - \* Molti non fanno gli aggiornamenti... (per evitare che alcuni sw non funzionino più, oppure perchè non la ritengono un'attività importante)
  - \* Ci sono ancora sistemi operativi legacy come XP che non sono più supportati.
  - \* Ci sono molte copie di Windows piratate che ovviamente non ricevono gli update... a differenza di chi ha software originali.
- \* Molti utenti cliccano sui link nelle mail senza pensare



Stefano Ferrari  
[steferbs@gmail.com](mailto:steferbs@gmail.com)

# Procedure straordinarie e ordinarie di difesa

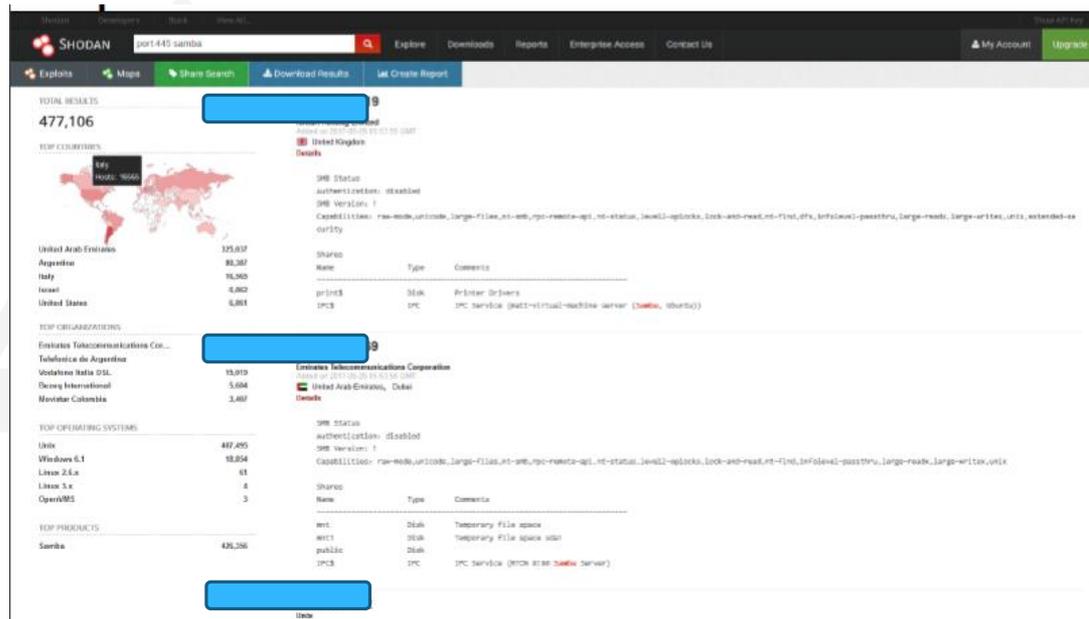


# Come difendersi nell'immediato

- \* Pagare alimenta questi tipi di attacchi e l'FBI scoraggia le vittime a farlo
  - \* Non è detto che vengano fornite le chiavi
- \* Server Windows e workstation sono ancora potenzialmente vulnerabili, le soluzioni nell'immediato:
  - \* Implementare subito le patch urgenti e quelle di emergenza messe a disposizione da Microsoft
  - \* Bloccare sui firewall le porte SMB tcp 139 e 445 e le udp 137 e 138
  - \* Disabilitare SMBv1 e v2 lasciando solo SMBv3

# 20 giorni dopo

- \* La mia azienda non verrà mai attaccata!
- \* È solo questione di tempo
- \* 20 giorni dopo la prima diffusione dell'infezione ci sono ancora in Italia oltre 16000 indirizzi IP che pubblicano su Internet la porta 445 (SMB)



# Come difendersi nel lungo periodo

- \* **Analisi dei rischi**
  - \* Management consapevole dei rischi, dei vantaggi e degli impatti economici per stabilire delle metriche chiare
  - \* Trasferimento della consapevolezza all'intera azienda impartendo regolarmente corsi di formazione e sensibilizzare gli utenti alla sicurezza
- \* **Eseguire Backup regolari**
  - \* Le copie devono risiedere cifrate su dispositivi scollegati dalla rete e/o in cloud
  - \* Fare test di ripristino
- \* **Limitare l'utilizzo di plugin pericolosi nei browser**
  - \* Ad esempio Flash o plugin non conosciuti

# Come difendersi nel lungo periodo

- \* Evitare la condivisione delle risorse di rete tra pc
- \* Non aprire allegati e di abilitare automaticamente le Macro in office
  - \* abilitare il flag di visualizzazione delle estensioni dei file
  - \* estensione del tipo: .EXE, .JS, .CMD, .BAT, .SCR, .JAR, .PIF, .COM, ecc.
  - \* documenti Microsoft Office con macro attivate (.DOCM, .DOTM, ecc.)
- \* Controllare le mail
  - \* Dominio e ragione sociale dovrebbero corrispondere
  - \* Verificare il server di provenienza e la sua reputazione
  - \* Abilitare controlli avanzati sui PTR, record MX, ecc.
- \* Segmentare la rete

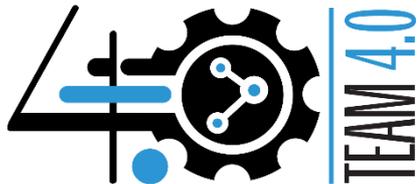
# Come difendersi nel lungo periodo

- \* Monitoraggio con sistemi predittivi
  - \* Analisi comportamentale della rete per capire movimenti trasversali anomali (traffico est-ovest)
- \* Aggiornamento costante dell'infrastruttura
  - \* Evitare che vengano sfruttate le vulnerabilità note
  - \* Eseguire valutazioni di rischio sistematiche per individuare vulnerabilità
- \* Evitare la complessità
  - \* Approccio di difesa integrata
  - \* Usare i dati analizzati per convalidare e migliorare le pratiche di sicurezza
  - \* Dotarsi di un sistema SIEM (Security information and event Management)



Stefano Ferrari  
[steferbs@gmail.com](mailto:steferbs@gmail.com)

# Approccio integrato alla cybersecurity



# Cisco's Annual Cybersecurity Report 2017

## Increasing Digital Traffic Creates a Greater Attack Surface

Global IP Traffic to Triple by 2020



2.3

ZB

Annual global IP traffic



66%

of IP traffic will be Wi-Fi and mobile devices



82%

of all consumer internet traffic will be connected devices



2x

Broadband speeds



# Cisco's Annual Cybersecurity Report 2017

## Losses After an Attack Are Real



Opportunity

23%

42% were losses >20%



Revenue

29%

38% were losses >20%



Customers

22%

38% were losses >20%



2017 Security Capabilities Benchmark Study (n=2,912)



**C.R.O.I.L.**  
CONSULTA REGIONALE ORDINI  
INGEGNERI LOMBARDA



# La cyber sicurezza

- \* Un progetto di security deve partire dal valore dei dati per arrivare ai processi di business da proteggere
- \* Approccio sistemico e non pezze a seconda delle mode o delle sensazioni
- \* Non è sufficiente analizzare il traffico perimetrale, ma bisogna avere completa visibilità della rete.
- \* I client roaming che utilizzano il cloud sono sempre di più e le semplici vpn non sono adeguate

# Come approcciarsi

- \* Come vengono rilevate e come mi proteggo dalle minacce di sicurezza?
- \* Come vengono protetti i confini della mia rete?
- \* Che livello di visibilità della rete mi offre la soluzione proposta?
- \* Il costruttore che ho scelto partecipa alla stesura degli standard industriali dell'automazione?
- \* L'hardware come viene mantenuto?

# Come approcciarsi

- \* Come contribuisce la sicurezza a farmi ottenere risultati aggiuntivi?
- \* Come si integra la soluzione con l'IT esistente?
- \* Che tipo di protocolli di autenticazione e autorizzazione sono implementati?
- \* Che crittografia utilizzo?
- \* Ho ancora in rete sistemi obsoleti?

# La visione integrata

## \* Protezione a livello DNS

- \* Protegge i device dentro e fuori la rete aziendale. Blocca le richieste DNS prima che un device possa connettersi a siti che ospitano ransomware

## \* Protezione degli Endpoint

- \* Blocca l'esecuzione dei file ransomware sugli endpoints.

## \* Protezione delle Email

- \* Blocca i ransomware spediti attraverso email di spam e phishing. Identifica allegati e URL malevoli all'interno della mail. Blocca gli attacchi prima che si diffondano.

# La visione integrata

## \* Segmentazione sofisticata

- \* Segmenta dinamicamente la rete, in modo che l'accesso ai servizi e applicazioni sia altamente sicuro indipendentemente dalla posizione.

## \* Difese avanzate per attacchi avanzati

- \* Tecnologie di sandboxing che limitino malware conosciuto e sconosciuto. Inoltre bloccano chiamate command-and-control verso host ransomware.

## \* Next Generation Firewall (NGFW)

- \* vedere chi accede alla rete e che operazioni effettua
- \* semplificare l'applicazione delle *policy*
- \* effettuare l'analisi dei flussi e l'analisi della traiettoria dei file