ENDPOINT NETWORK CLOUD

Smart Working & Cybersecurity

Evoluzione della cybersecurity nei giorni della pandemia da COVID-19: in uno scenario mutato, qual' è stata la risposta degli Hacker e come va gestito oggi un rischio più distribuito

Denis Valter Cassinerio Regional Sales Director SEUR

Bitdefender

WWW.BITDEFENDER.COM

AGENDA

- «Psicologia» ed «economia dell'attacco»
- Cosa ci dice la Telemetria
- Economia dell'attacco: si diversificano i «vettori»
- Policy e «Controlli di Nuova Generazione»
- Bitdefender Ultra PLUS

«Psicologia» ed «economia dell'attacco»

Come cambiano gli attacchi

I Cyber Criminali sfruttano le nostre incertezze e le nostre preoccupazioni…

La realizzazione della «Home Enterprise»

La realizzazione della «Home Enterprise»

COVID-19

La realizzazione della «Home Enterprise»

COVID-19

CONFINAMENTO

La realizzazione della «Home Enterprise»

COVID-19

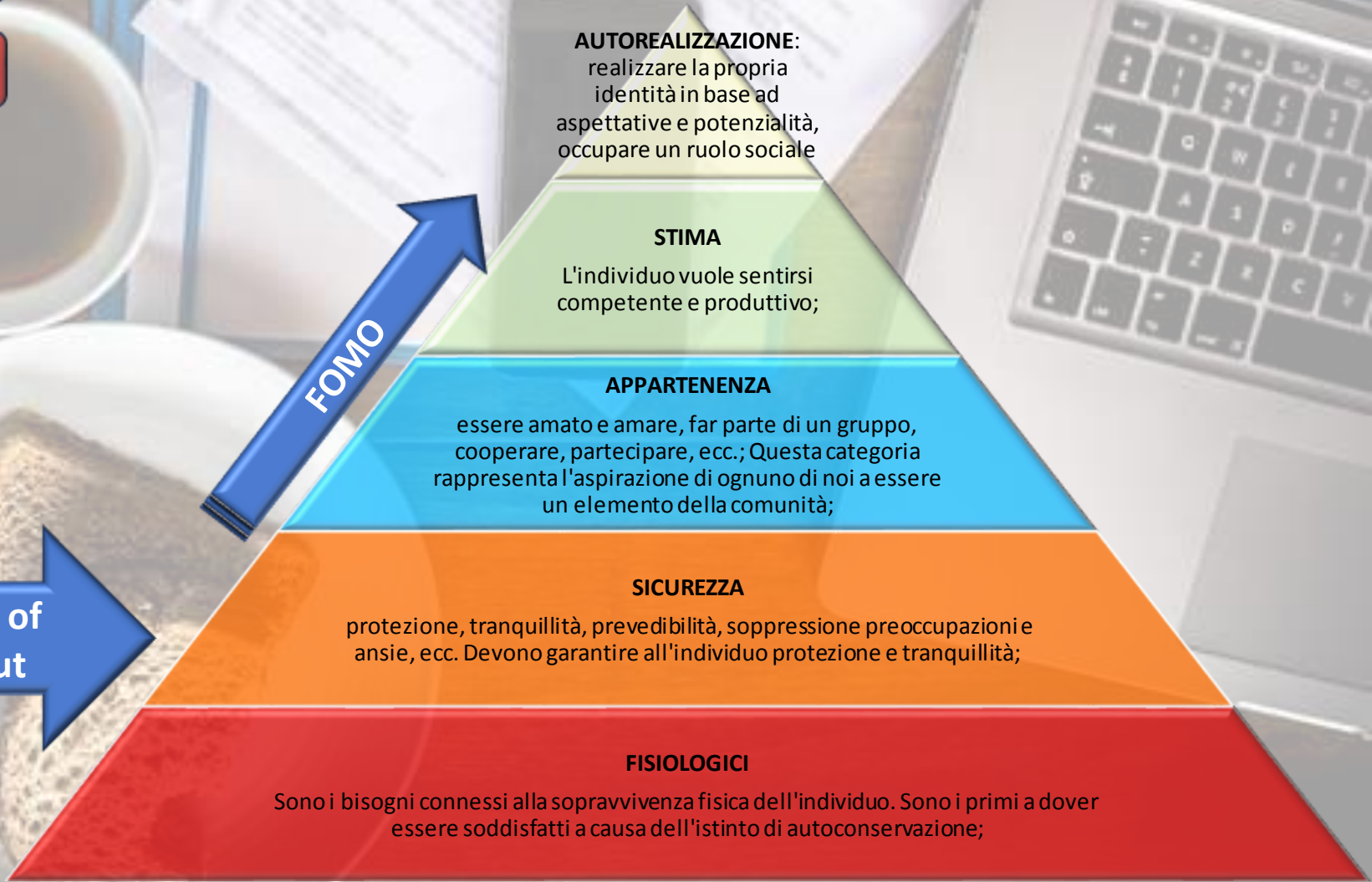
CONFINAMENTO

PSICOLOGIA

Casa = Sicurezza

FOMO Fear of Moving Out

FOMO



Source: Abraham Maslow (1947)

La realizzazione della «Home Enterprise»

COVID-19

CONFINAMENTO

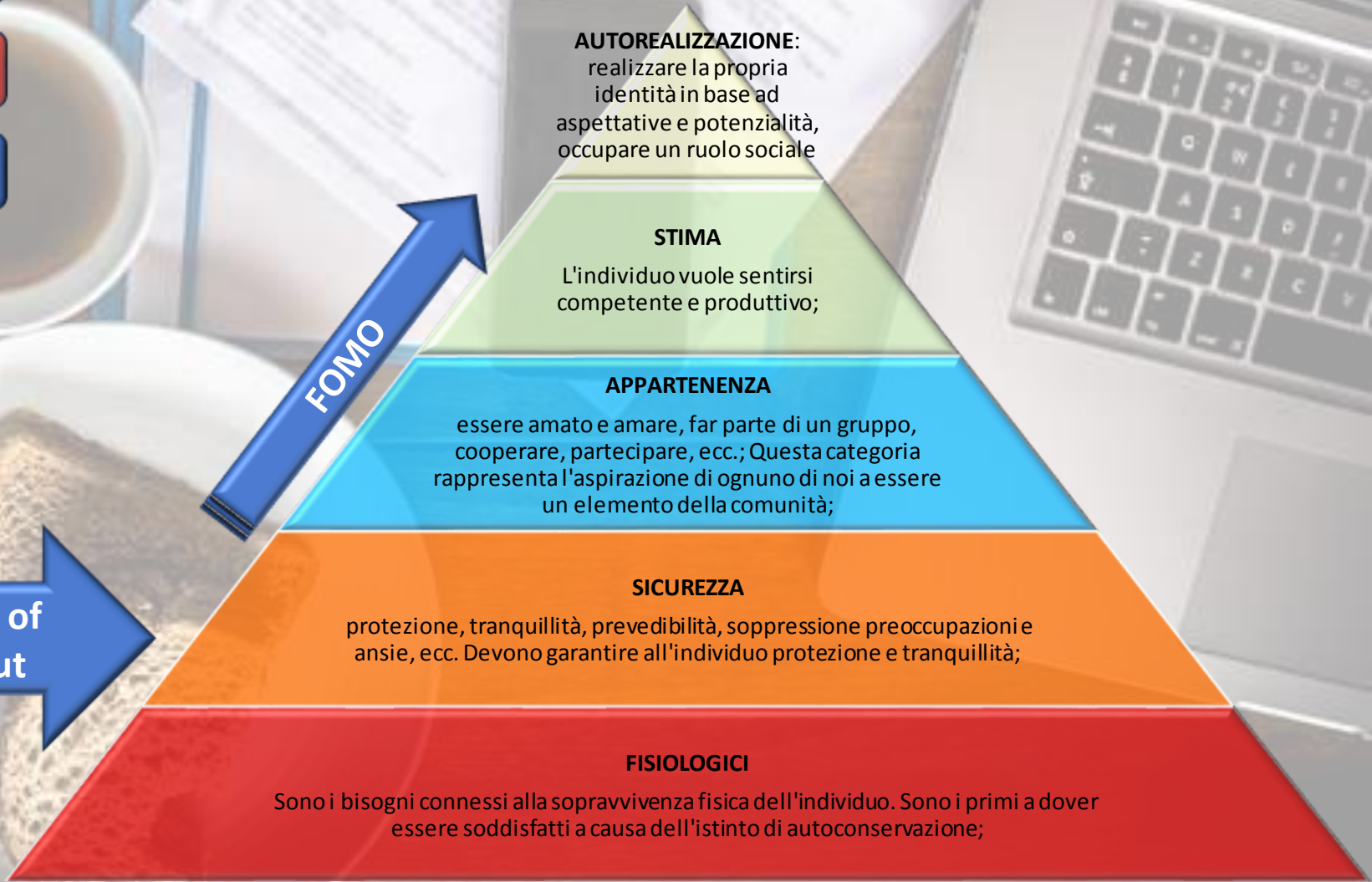
PSICOLOGIA

SMARTWORKING

Casa = Sicurezza

FOMO Fear of Moving Out

FOMO



Source: Abraham Maslow (1947)

La realizzazione della «Home Enterprise»

COVID-19

CONFINAMENTO

PSICOLOGIA

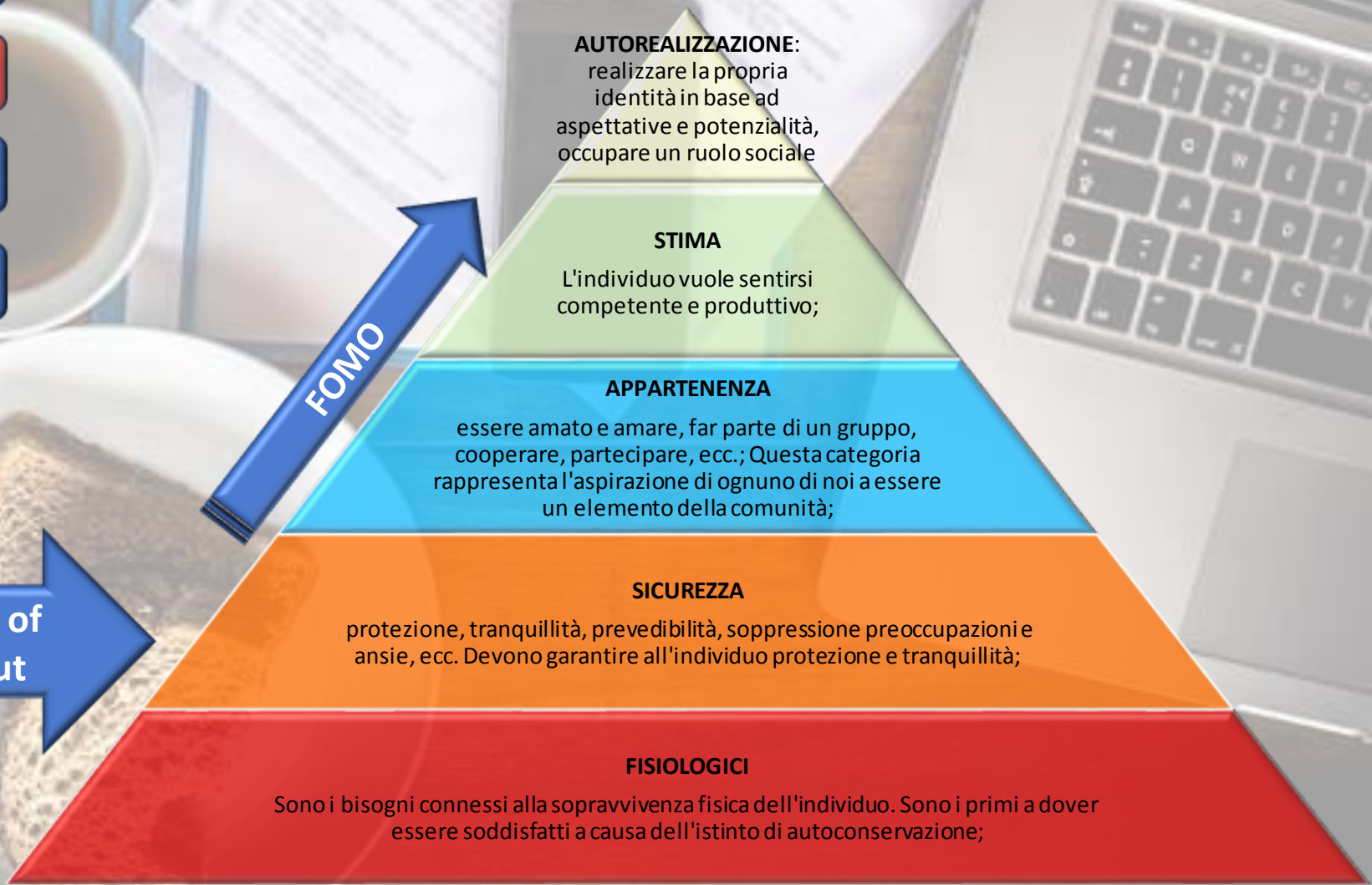
SMARTWORKING

ECONOMIA REALE

Casa = Sicurezza

FOMO Fear of Moving Out

FOMO



Source: Abraham Maslow (1947)

La realizzazione della «Home Enterprise»

COVID-19

CONFINAMENTO

PSICOLOGIA

SMARTWORKING

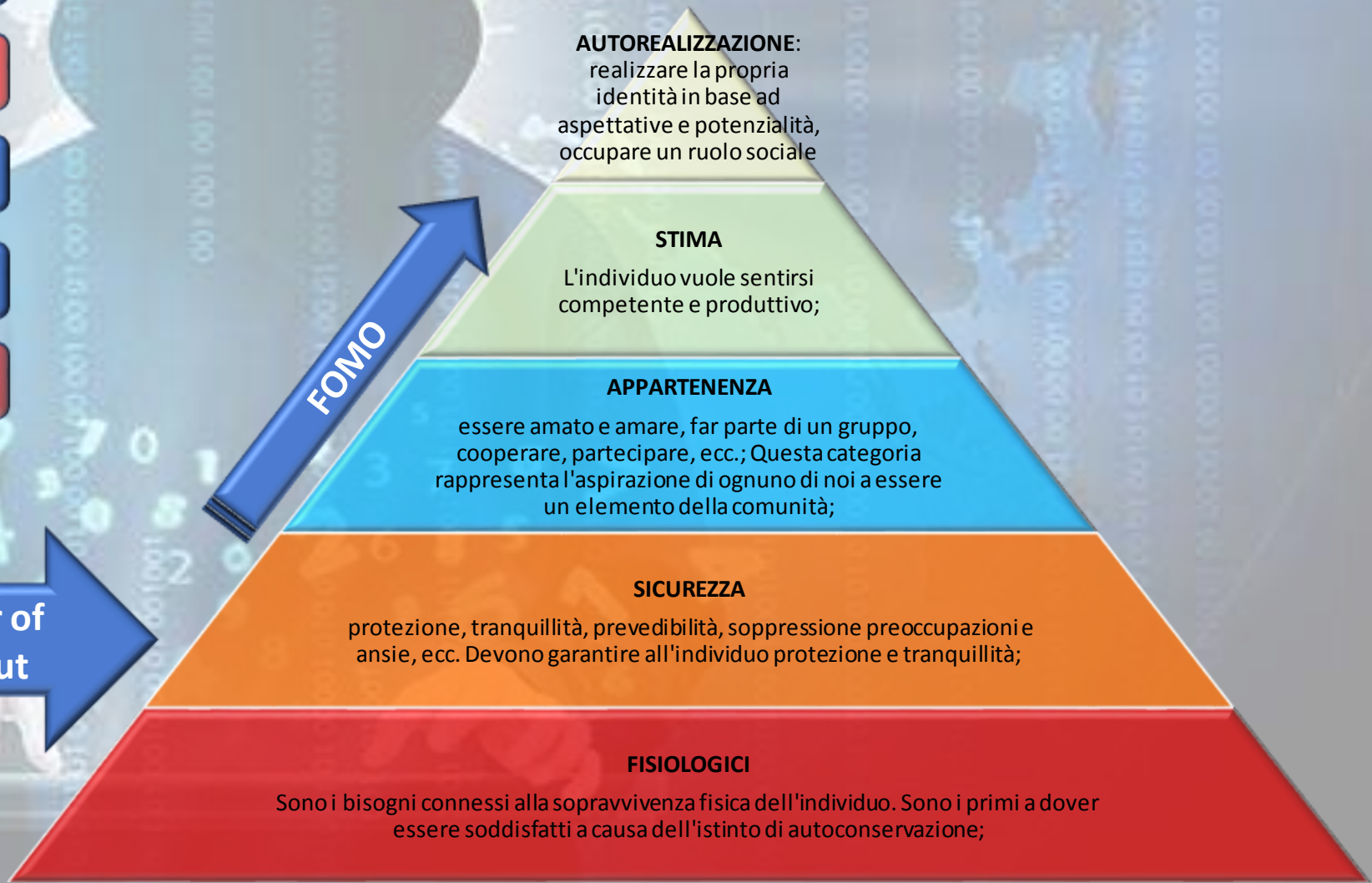
ECONOMIA REALE

ECONOMIA ATTACCO

Casa = Sicurezza

FOMO Fear of Moving Out

FOMO



Source: Abraham Maslow (1947)

Cosa ci dice la Telemetria

Bitdefender CYBERTHREAT REAL-TIME MAP

TELEMETRIA DEGLI ATTACCHI

LEGEND

- ATTACKS
- INFECTIONS
- SPAM

LIVE ATTACKS

TIME	ATTACK	ATTACK TYPE	ATTACK COUNTRY	TARGET COUNTRY
THU 9 APR 11:49:…	N/A	ATTACK	UNITED STATES	UNITED STATES
THU 9 APR 11:50:…	#REGSVR32.EXE:00…	INFECTION	ITALY	N/A
THU 9 APR 11:50:…	N/A	SPAM	GREECE	N/A
THU 9 APR 11:49:…	N/A	SPAM	JAPAN	N/A
THU 9 APR 11:50:…	N/A	SPAM	NEW ZEALAND	N/A
THU 9 APR 11:50:…	TROJAN.REDIRECT.W	INFECTION	SPAIN	N/A
THU 9 APR 11:50:…	N/A	SPAM	UNITED STATES	N/A

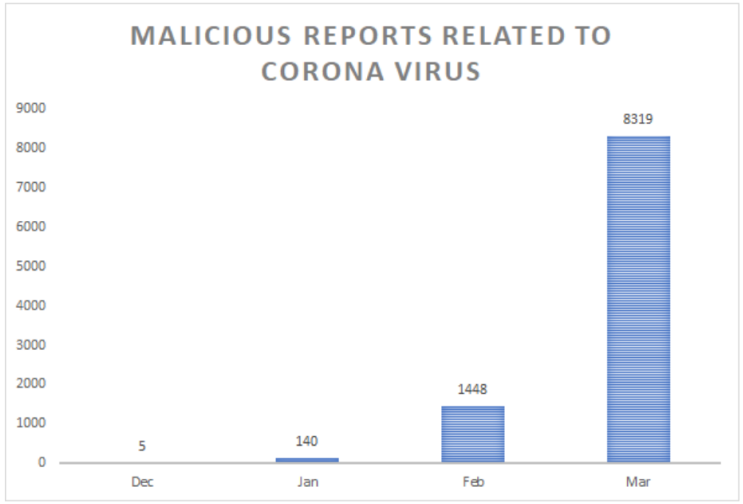
LOCATIONS

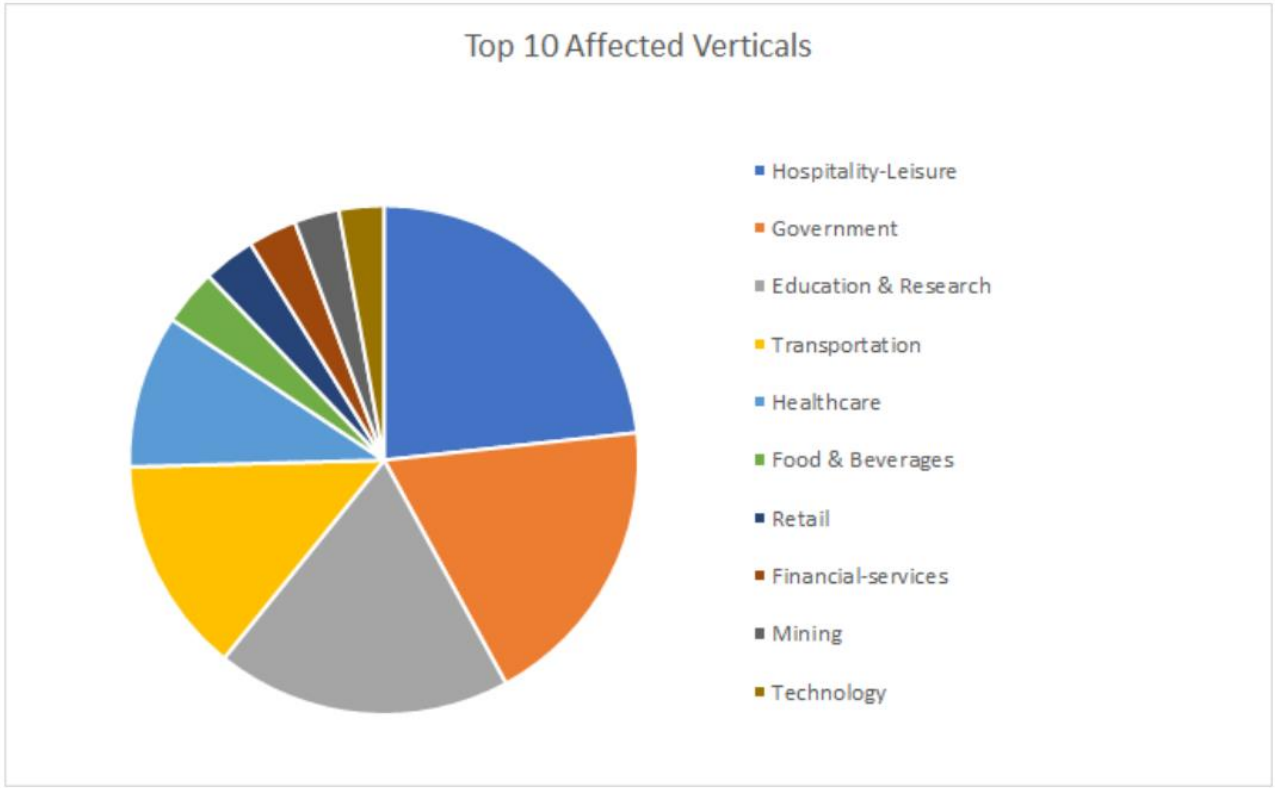
- UNITED STATES
- UNITED KINGDOM
- GERMANY
- ITALY
- FRANCE
- JAPAN
- INDIA
- ROMANIA
- CHINA

Come cambiano gli attacchi informatici: I nuovi (e vecchi) scenari di attacco

Malicious Reports Soar in March

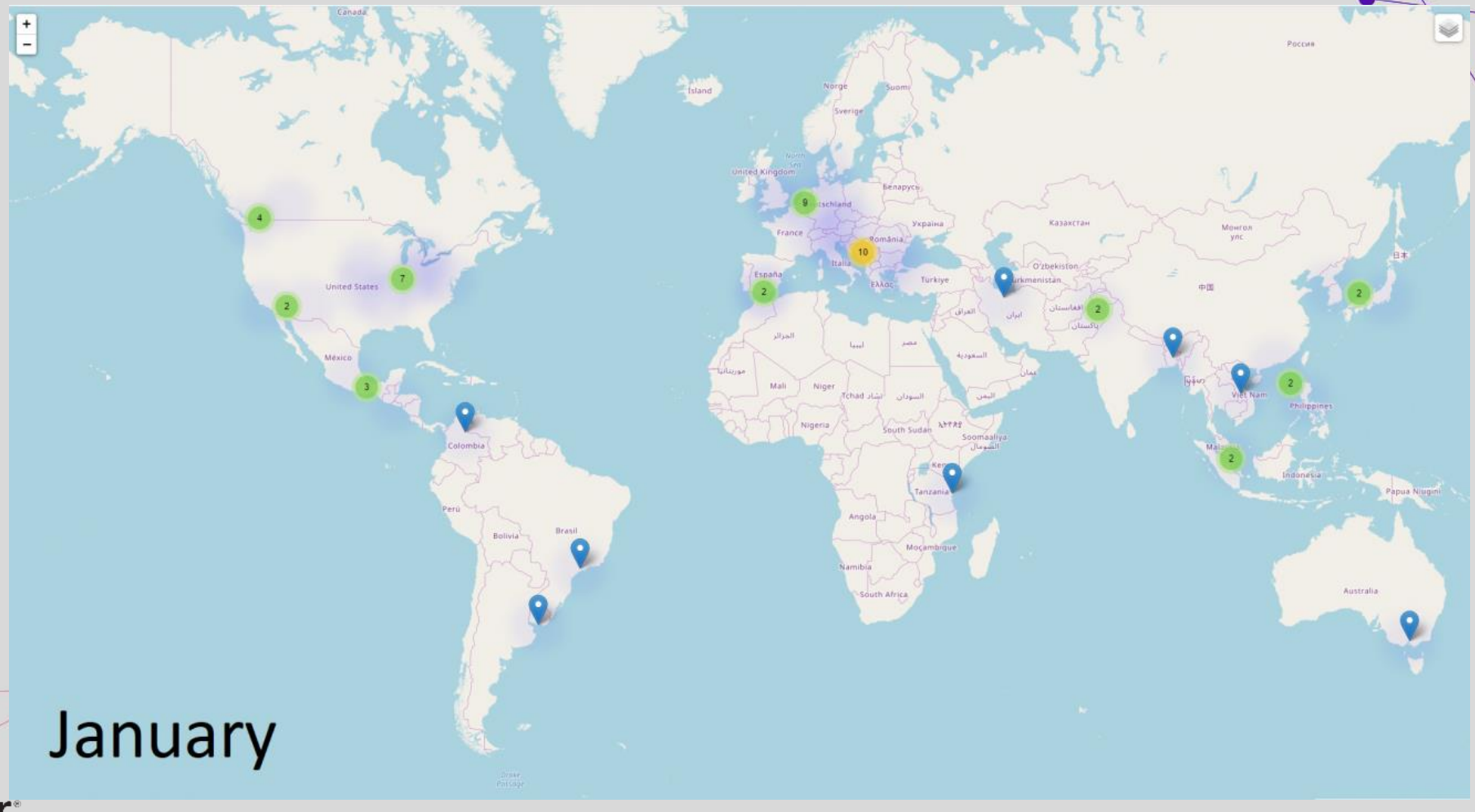
From 1,448 malicious reports in February to 8,319 reports until March 16th, the number has sharply increased, as the real COVID-19 virus spreads aggressively around the world.





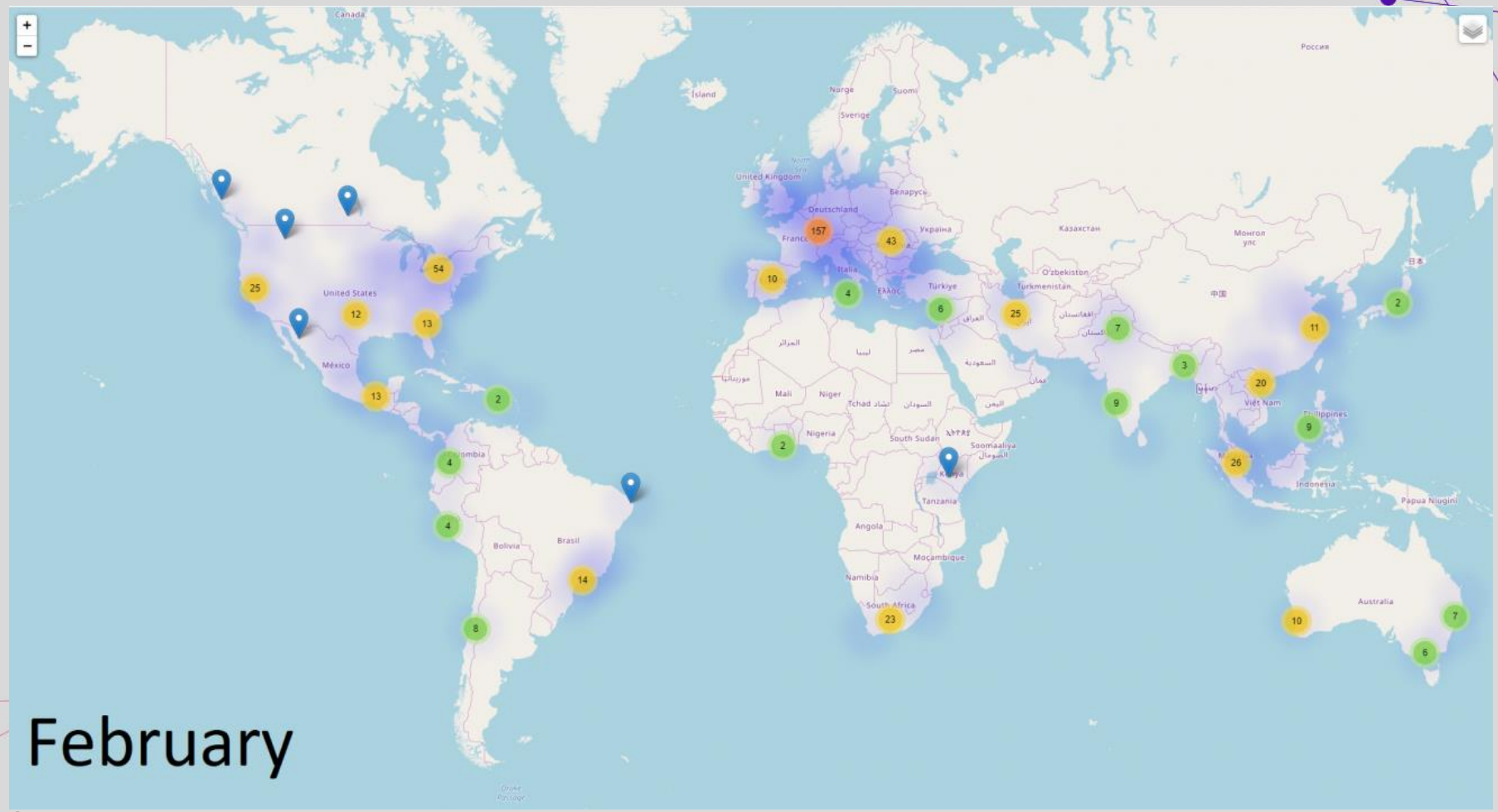
(Fonte: Bitdefender Labs)

Come cambiano gli attacchi informatici: I nuovi (e vecchi) scenari di attacco



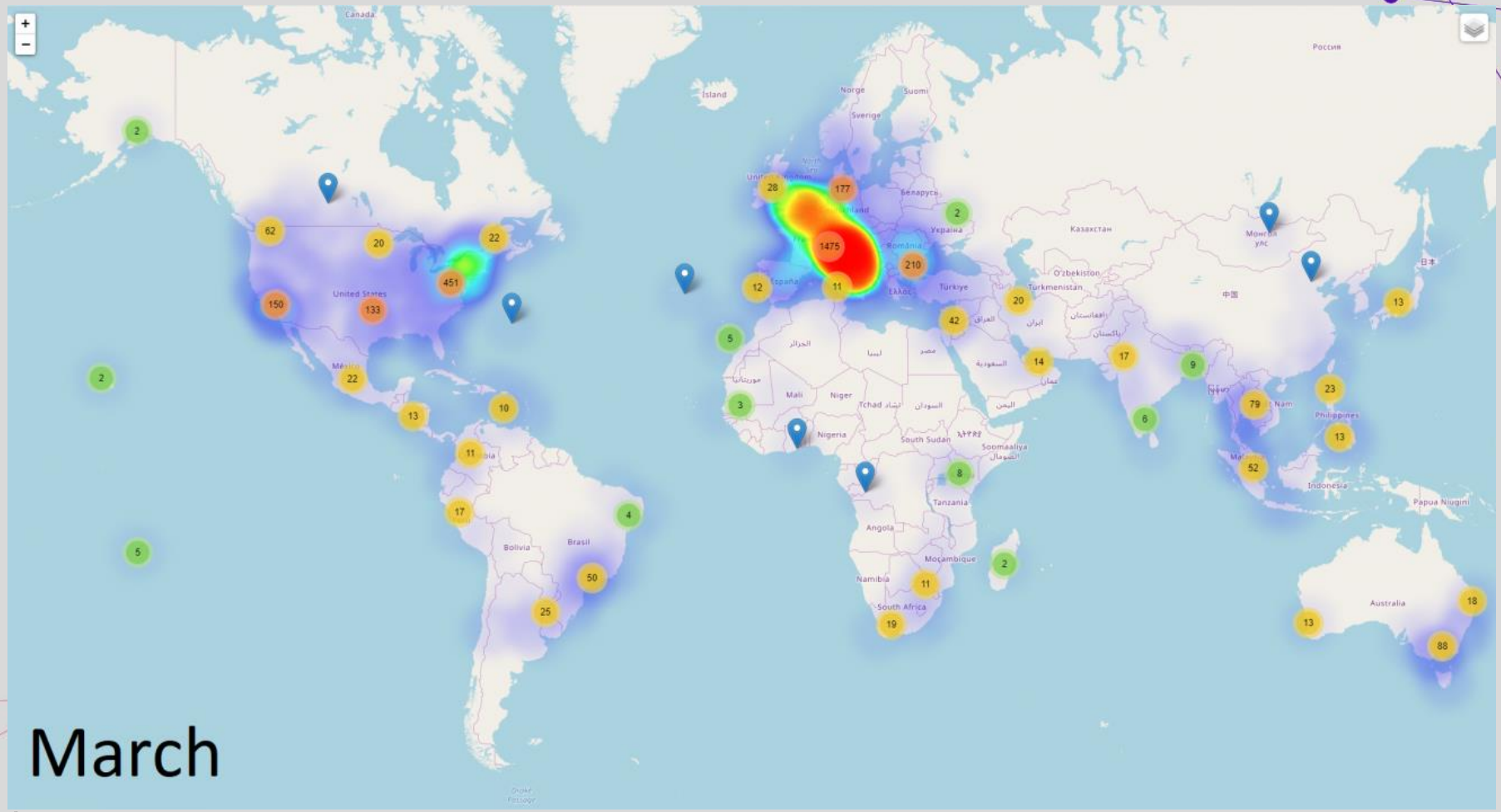
(Fonte: Bitdefender Labs)

Come cambiano gli attacchi informatici: I nuovi (e vecchi) scenari di attacco



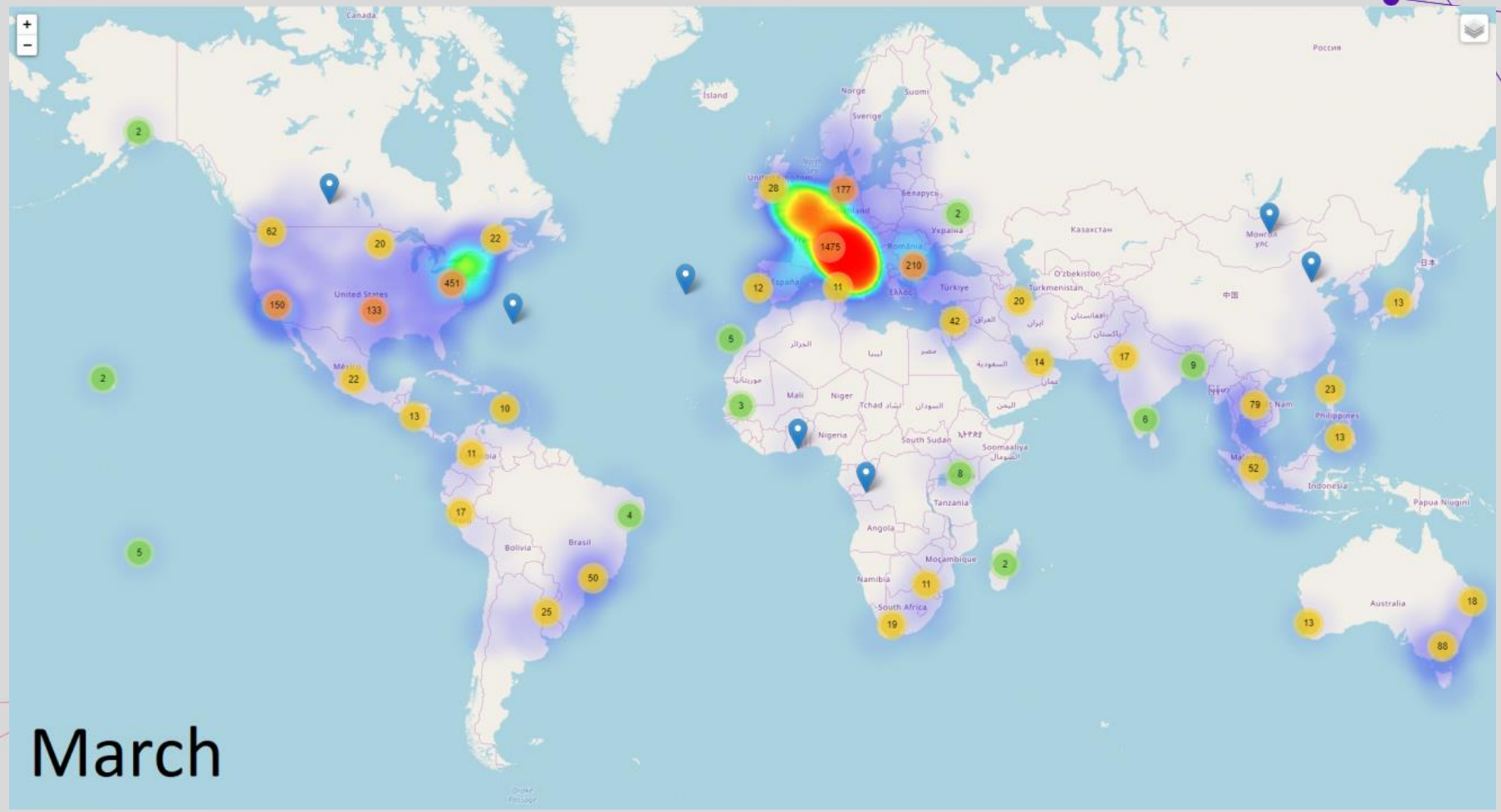
(Fonte: Bitdefender Labs)

Come cambiano gli attacchi informatici:
I nuovi (e vecchi) scenari di attacco



(Fonte: Bitdefender Labs)

Come cambiano gli attacchi informatici:
I nuovi (e vecchi) scenari di attacco



(Fonte: Bitdefender Labs)

Come cambiano gli attacchi informatici: I nuovi (e vecchi) scenari di attacco

(Fonte: Bitdefender Labs)

Economia dell’attacco:
Si diversificano i «vettori»

Come cambiano gli attacchi informatici: I nuovi (e vecchi) scenari di attacco

Si fa leva sull'incertezza e sui timori delle persone…

12.03.2020

CORONAVIRUS: NUOVA ONDATA DI #PHISHING E #MALWARE

Il Coronavirus non ferma i criminali del web, che non si fanno scrupoli ad approfittare del rischio di epidemia in corso per architettare nuove ed…

02.03.2020

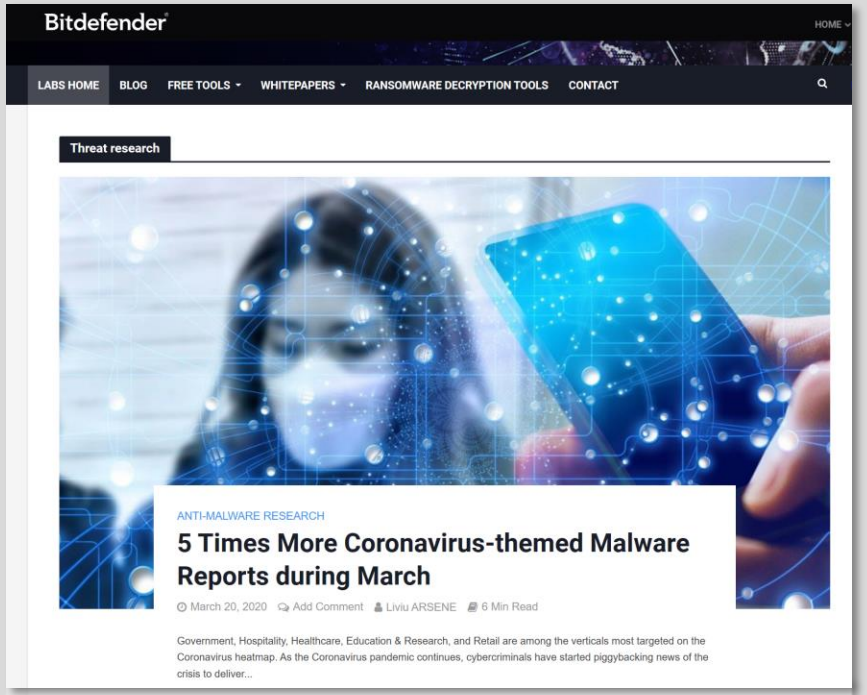
PALERMO: OPERAZIONE ANTI-PHISHING

La Polizia di Stato, Compartimento Polizia Postale – Palermo, coordinata da quella Procura, ha individuato e posto sotto sequestro una pagina web di…

12.03.2020

CORONAVIRUS: ATTENZIONE ALLE RICHIESTE DI DONAZIONE A FAVORE DI STRUTTURE SANITARIE

In questi giorni circolano molte richieste di donazione a favore di strutture sanitarie per finanziare l'acquisto di materiali per combattere la…



(Fonti: Polizia di Stato e Bitdefender Labs)

Come cambiano gli attacchi informatici: I nuovi (e vecchi) scenari di attacco

I CyberCriminali approfittano della maggiore "socialità" delle persone…

https://www.marionegri.it/magazine/coronavirus-e-fake

(Fonti: Istituto Mario Negri e Bitdefender Labs)

Vecchie e nuove tecniche

I TREND DI ATTACCCO «ATTUALI»

1. Business Email Compromise
2. Remote Desktop Protocol
3. Ransomware

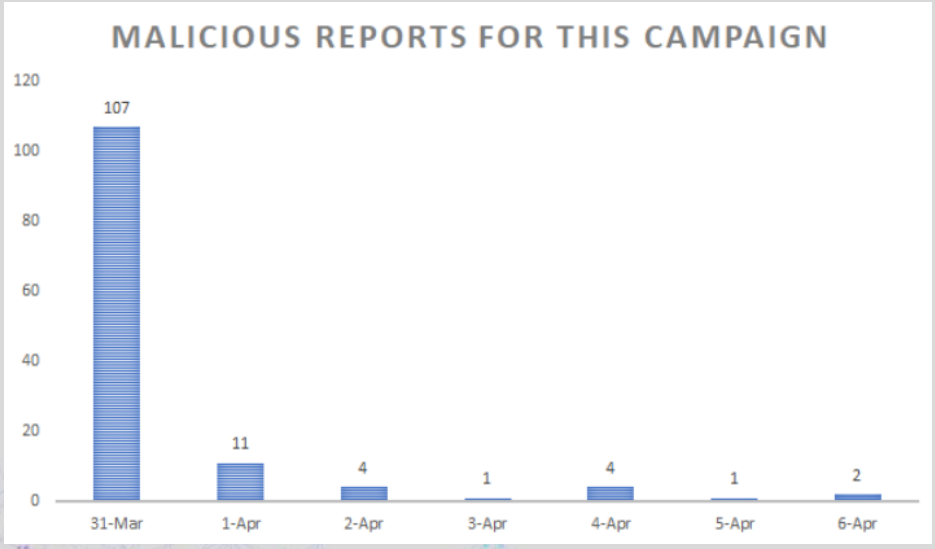
Business Email Compromise

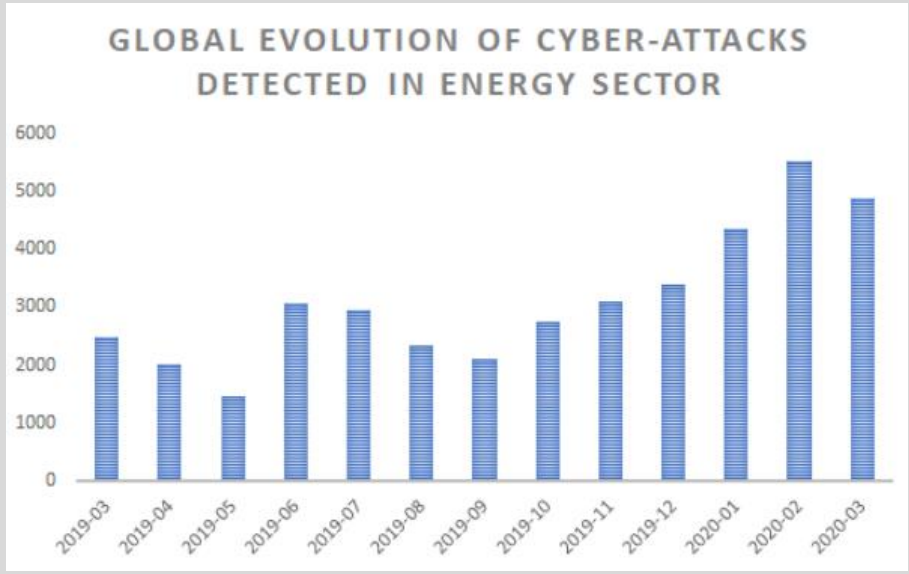
Mai obsoleto

$1.7 bn

Di perdite causate da attacchi di tipo BEC & EAC

Attacchi «Opportunitstici»





* FBI's Internet Crime Complaint Center (IC3) - 2019 Internet Crime Report

Remote Desktop Protocol

… il più subdolo

434 Million

Attacchi RDP prima del COVID

Features

- Accesso Remoto (interno, sicuro)
- Facile accesso (utenti)
- Gestione semplice

Drawbacks

- Accesso Remoto (Facilmente sfruttabile per attacchi)
- Facile accesso (anche per i criminali, se non sicuro)
- Gestione Semplice (Vulnerabile se senza patch o non configurato)

* Global Bitdefender telemetry reports

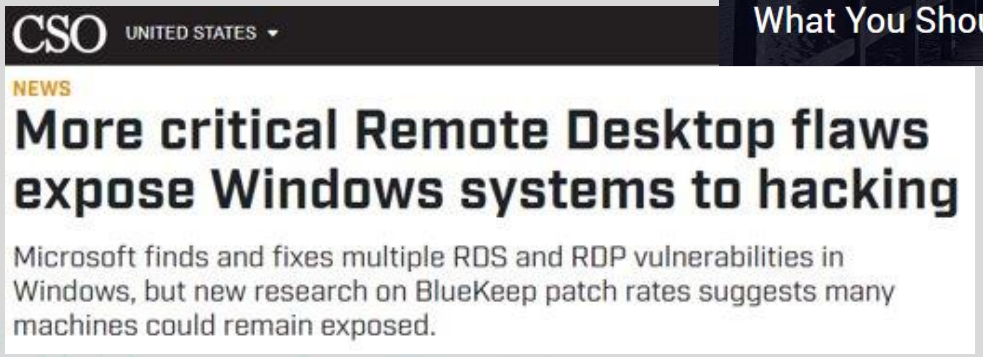
Detection	Count
Attack.Bruteforce.RDP	434,042,426
PrivacyThreat.PasswordStealer.HTTP.Internal	134,649,493
PrivacyThreat.PasswordStealer.HTTP	55,836,548
Exploit.SMB.ExeCriticalLocation	1,915,919
Exploit.HTTP.ShellShock	1,901,317
Exploit.HTTP.DirectoryTraversal	1,216,860
Exploit.SMB.CVE-2017-0144.EternalBlue	973,927
sav_malware	293,827
PrivacyThreat.PrivateDataLeakage.HTTP.Alert	179,485
Attack.PortScanning	129,909
Bot.DGA.filtered	91,694
Exploit.CommandInjection.Gen.8	83,647
Attack.Bruteforce.FTP	54,483
Exploit.HTTP.CVE-2017-5638	53,070
Exploit.CommandInjection.29	39,823
Attack.LocalFileInclusion.5	30,980
Exploit.LoginTooLong.SMB	29,242
Suspicious.TorActivity	28,518
Attack.LocalFileInclusion.36	14,972
Anomaly.IPv4	11,693

Remote Desktop Protocol

… il più subdolo

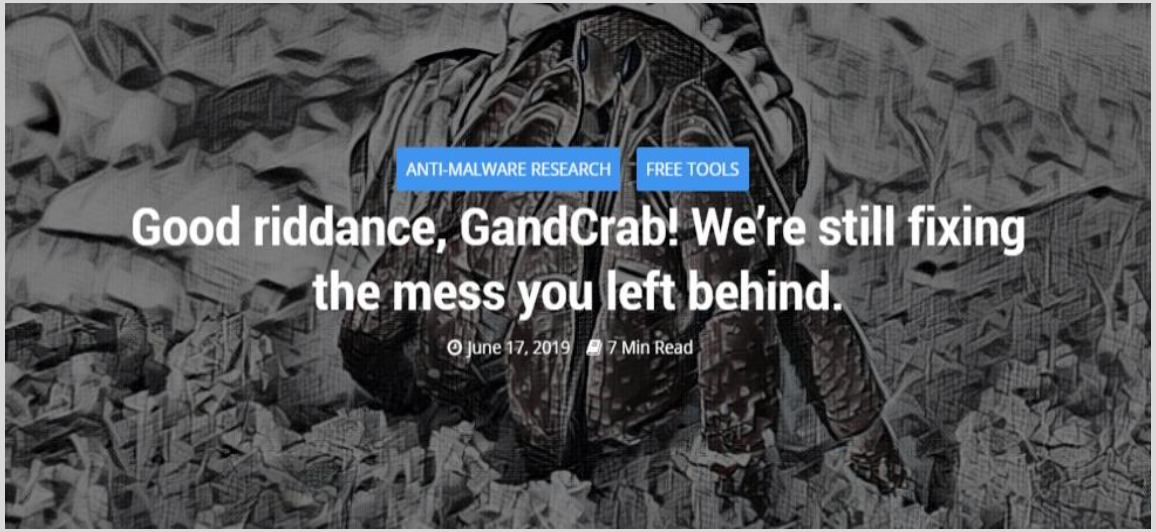
30%

Aumento attacchi relativi al Remote Desktop Protocol (RDP) durante Marzo



Ransomware

Un classico che si rinnova



Home Enterprise = «The New Normal»

Lavoro da casa, quali rischi corro?

Restare in Sicurezza tra Phishing,

Attacchi e Compromissioni

I rischi informatici connessi allo «Smart Working»

Le connessioni di rete domestiche non sono sempre sicure

Sicurezza Wi-Fi

Reti aperte

Device poco sicuri (BYOD – Routers)

Aumentano i rischi di compromissione dei dati

Utilizzo promiscuo dei sistemi

PC Personali

difficoltà nel controllo degli accessi

Il personale IT è a casa come tutti gli altri

(o è comunque a ranghi ridotti)

Aumento Superficie di attacco

VPN & VDI

Strong Authentication

Aumentano gli attacchi basati su phishing e su malware di varia natura

Mail & Web Phishing

Nuove metodologie di attacco

Risk Management assente e scarsa visibilità sorgente di attacco

Come possiamo proteggere gli «Smart-Worker»?

La prima linea di difesa: Security Awareness

Conoscere le minacce

Assumere i giusti Comportamenti

saper comunicare i problemi

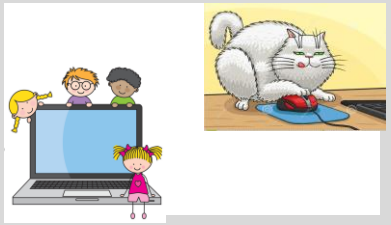
Rendere più sicure le connessioni di rete WiFi

Non utilizzare reti aperte

Usare password complesse

non utilizzare Default di Fabbrica

Minimizzare gli accessi indesiderati ai sistemi quando si lavora a casa



Leva sugli «Cyber Skills» in azienda

Riduzione Superficie di attacco

VPN & VDI

Strong Authentication

Risk Visibility

Identificazione sorgente di attacco (IOC)

SMARTWORKING significa:

Centralità del «PUNTO TERMINALE»

Policy e «Controlli di Nuova Generazione»

Il cambiamento «industriale» dell’endpoint security:

Il cambiamento «industriale» dell'endpoint security:

ENDPOINT SECURITY CONTROLS FORMULA

PREVENTIVE
+
DETECTIVE
+
CORRECTIVE
+
COMPENSATIVE
+
RECOVERY =

«NEW» ENDPOINT PROTECTION

Il cambiamento «industriale» dell’endpoint security

OLD

1) Conoscere il Problema
2) Dare istruzioni all’Endpoint per risolverlo

Il cambiamento «industriale» dell'endpoint security

OLD

1) Conoscere il Problema

2) Dare istruzioni all'Endpoint per risolverlo

NEW

1) Conoscere & mitigare il **comportamento** che genera il Problema, prima che accada

2) L'endpoint reagisce autonomamente

3) Dare Visibilità della Genesi del problema

4) Dare Istruzioni all'IT per ulteriori indagini e mitigazione future

Bitdefender Ultra PLUS

Protezione degli Endpoint e delle reti:

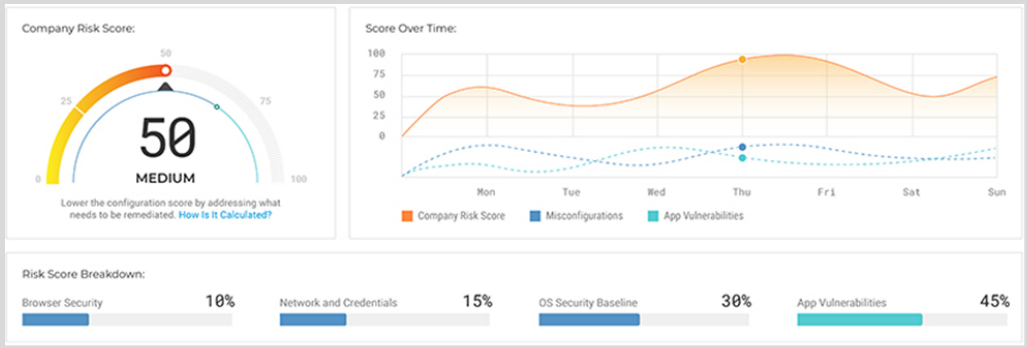
RISORSE: SKILLS + BUDGET ATTUALI

Approccio Bitdefender **GravityZone Ultra Plus:** protezione in tempo reale degli endpoint e visibilità sulle infrastrutture di rete in un'unica soluzione:

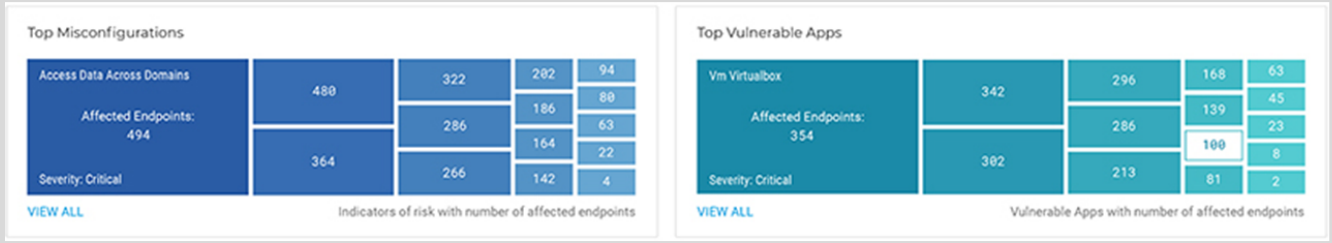
	Tecnologia	Necessità	Priorità
GravityZone **Ultra PLUS**	**EPP** Endpoint Protection	Rinnovare con tecnologie efficaci la protezione degl Endpoint	**Rispondere alle nuove tecniche di attacco**
	EDR Endpoint Detection and Response	Abilitare e correlare le informazioni derivanti dal rilevamento MultiLayer	**Abilitare i processi di «Early Warning»**
	ERA Endpoint Risk Analytics	Gestire costantemente il Rischio	**Assegnare la corretta priorità agli Interventi**
	Network Traffic **Security** Analytics **NTSA**	Abilitare l'analisi dei flussi di Rete	**Identificare i «movimenti» laterali**
	ESG (aggiuntivo)	Rinnovare con tecnologie efficaci la protezione Della Posta Elettronica	**Rispondere alle nuove tecniche di attacco**

Consapevolezza dei rischi e giusta priorità agli Interventi

GravityZone EndPoint Risk Analytics

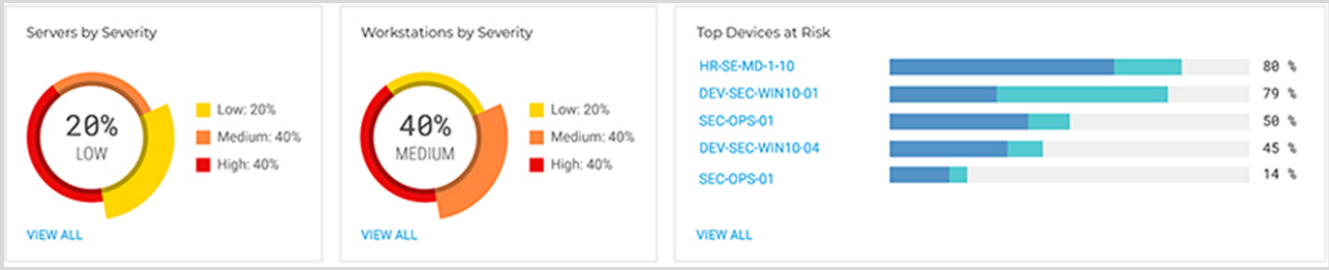


View your overall Company Risk Score and see how various misconfigurations and application vulnerabilities contribute to it



Assess prioritized misconfigurations and application vulnerabilities across your organization's endpoint estate

Get a risk snapshot for servers and end-user devices and review the endpoints exposed the most



THANK YOU!

GRAVITYZONE™
THE SECURITY PLATFORM FOR
end-to-end breach avoidance