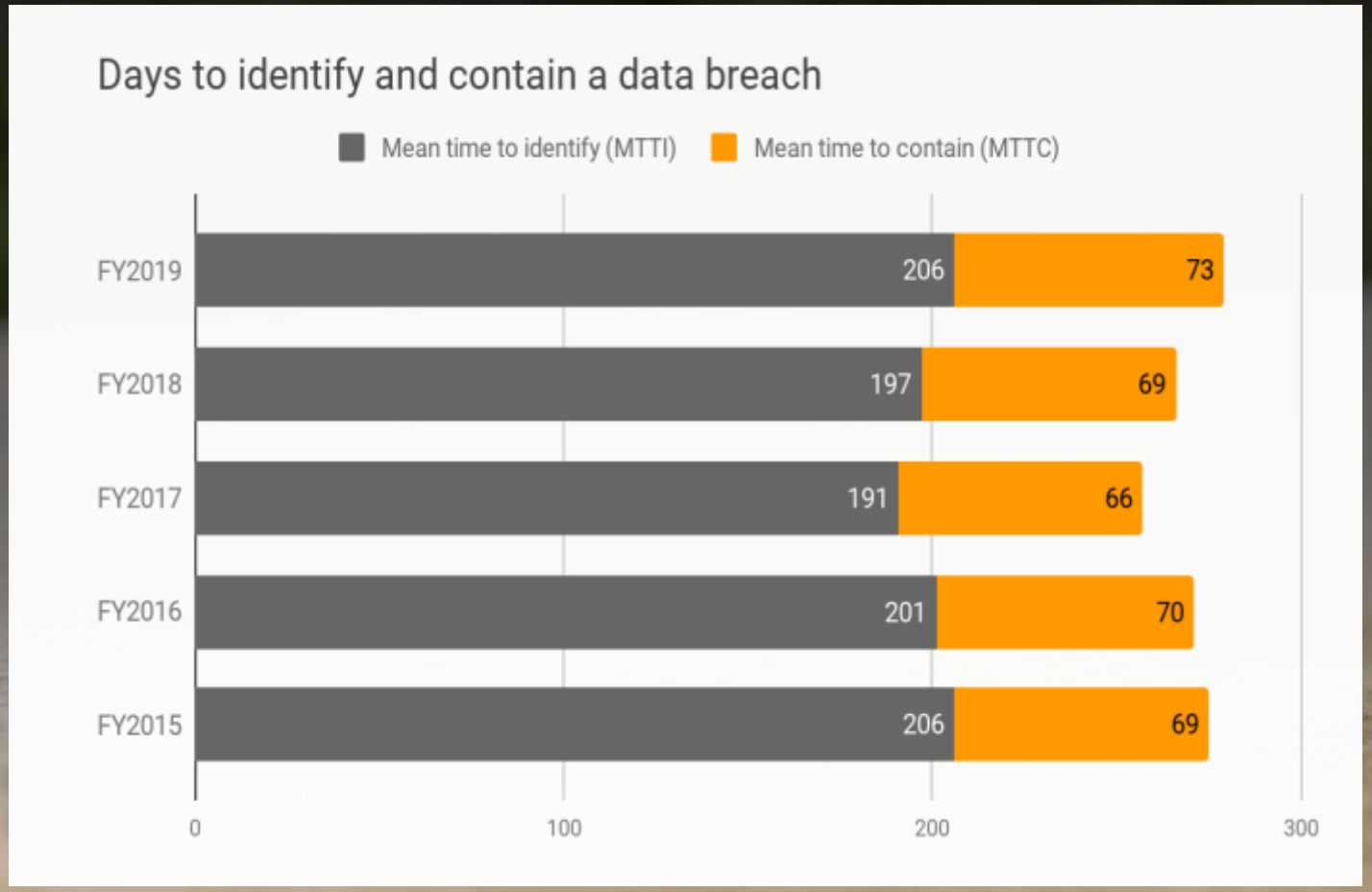
No podemos proteger
Aquello que NO VEMOS!

Ruben A. Bayud
BDM Southern Cone
Lumu Technologies
rbayud@lumu.io

Problema: SOMOS LENTOS PARA DETECTAR COMPROMISO

> El intervalo de tiempo es inaceptable, Cibercriminales tardan solo 15 horas para romper una red y las organizaciones 191 días para descubrirlo.

Problema: SOMOS LENTOS PARA DETECTAR COMPROMISO



CITRIX®
10 YEARS

yahoo!
SEVERAL BREACHES
MONTHS

EQUIFAX
6 MONTHS

Marriott®
INTERNATIONAL
4 YEARS

Ejemplos recientes

infochannel.info

Microsoft admite que sufrió una brecha de seguridad

Jue, 23/01/2020 - 09:48

Ventana Global

Autor: Melissa Pérez Alcántara

México

La tecnológica dijo que su base de datos de servicio a clientes fue vulnerada entre el 5 y el 31 de diciembre

Cuentas expuestas

Fortinet removes SSH and database backdoo...
www.zdnet.com

Fortinet removes SSH and database backdoors from its SIEM product

Exclusive: Details of 10.6 million MGM hotel g...
www.zdnet.com

MAGAZINE
By ROOT VIEW

El error crítico de OpenSN_

Fallas de Microsoft Azure podrían haber permitido que los hackers se apoderen de los servidores de la nube

• 13 hours ago 0 45 2 minutes read

Investigadores de ciberseguridad en Check Point revelaron hoy detalles de dos vulnerabilidades potencialmente peligrosas recientemente parcheadas en los servicios de Microsoft Azure que, de ser explotadas, podrían haber permitido a los hackers dirigirse a varias empresas que ejecutan sus aplicaciones web y móviles en Azure.

Azure App Service es un servicio integrado totalmente


An avalanche of security vendors
Security Management and Compliance
infrastructure security
Cyber Security
Endpoint Security
Application Security
Cloud Security
Mobile Security
Identity and access management
Security Partners
Security Organizations
Security Conferences
Analyst Houses
RSA
solarwinds
customer success
DELL
IBM
SANS
HUAWEI
FORTINET
STONESOFT
AhnLab
FORRESTER
quocirca
hp
NTT
ALIEN VAULT
CenturyLink
Symantec
aruba
a Hewlett Packard Enterprise company
JUNIPER
Barracuda
verizon
tenable
:RESOLVER
zscaler
CELAES 2019
splunk>
LogRhythm
The Security Intelligence Company
PHISHME
Check Point
IBM
websense
Gartner
Raytheon
RAPID7
portnox
boundlessly smart
riverbed
Trustwave
AT&T
Cyveillance
black hat
IDG
WatchGuard
CISCO
RSA Conference
SOPHOS
IBM
Gartner
FireEye
FOX IT
info security
THREATSTREAM
Symantec
CYLANCE
OWASP
eset
US-CERT
proofpoint.
ziften
EUROPOL
CISCO
BeyondTrust
SOPHOS
ISACA
nexthink
change your perspective
Microsoft
WatchGuard
NIST
(ISC)²
Barracuda
Bromium
kaspersky
cloud security alliance
radware
NEXUM
Qualys.
TREND MICRO
VERACODE
Atos
UNISYS
Akamai
CITRIX
IBM
f5
SafeNet
websense
SOPHOS
ORACLE
skyhigh
appthority
Bit9
FUJITSU
Entrust Datacard
ca
BlueCoat
dimension data
Symantec
Microsoft
Trustwave
Microsoft
HID
Symantec
Arellia
TeleSign
SOPHOS
DELL
KASPERSKY
McAfee
Trustwave
Ping Identity
DUO
gemalto
TREND MICRO
SECUREAUTH
zscaler
intel
CITRIX
TREND MICRO
CISCO
RSA
onelogin
SAP
Barracuda

EL RESULTADO ES UN FALSO SENTIDO DE SEGURIDAD

LUMU

Acerca de Lumu

Lumu Technologies es una compañía de Ciberseguridad que ilumina a empresas de todo el mundo con una **nueva forma de visualizar, en tiempo real, amenazas, atacantes y enemigos que ya están comprometiendo su organización.**

Atrévete a pensar diferente!!!

Si supieras que ya estas comprometido,
gestionarías la seguridad de otra forma?

Premios y Reconocimientos

12 Hottest New **Cybersecurity Startups**

FEATURED BY

CSO FROM IDG

Lumu to **Emerge from Stealth**

FEATURED BY

DARK Reading

13 Hot Endpoint And **Network Security Tools**

FEATURED BY

CRN

Hottest New **Cybersecurity Products**

FEATURED BY

CSO FROM IDG

LUMU

Los ataques siguen un mismo ciclo

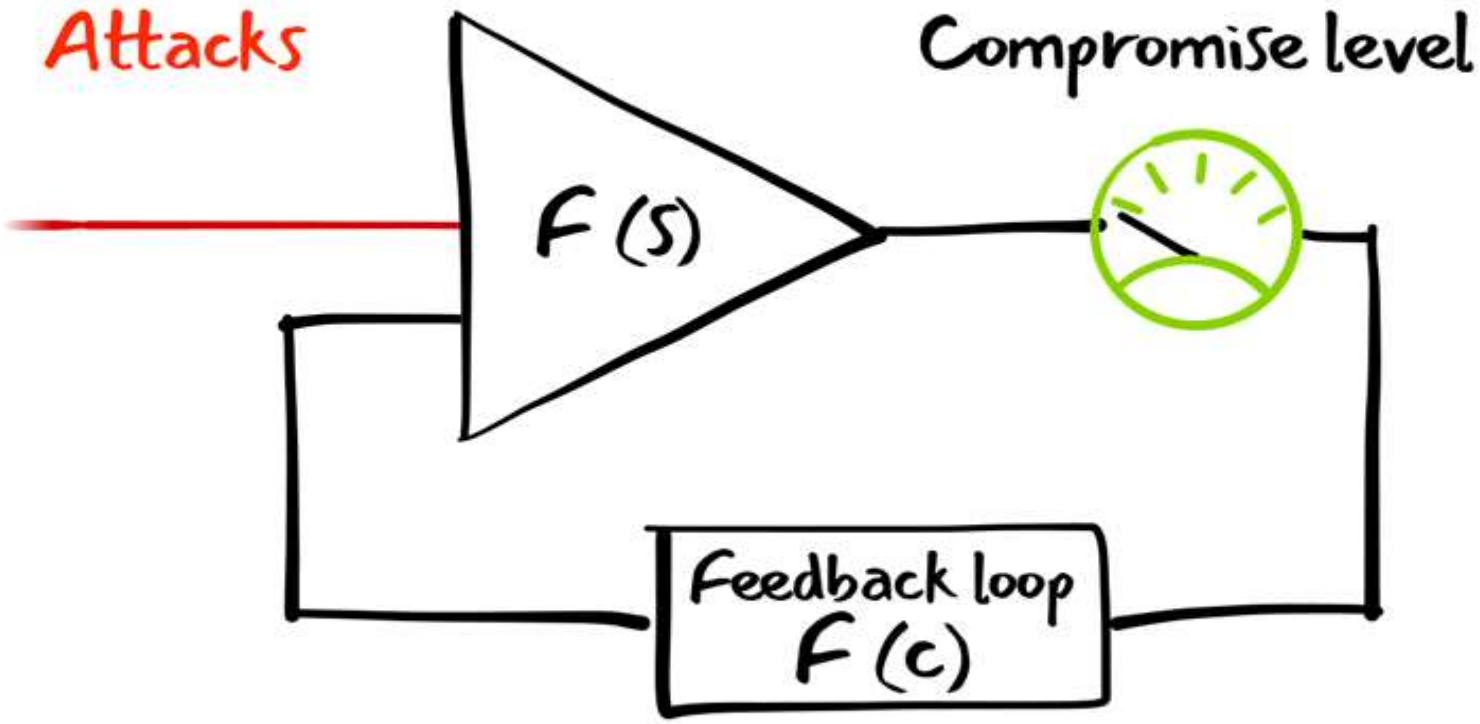
Los adversarios también usan la red.

Illuminar es: La Evaluacion Continua de Recursos Informáticos que ya estén Comprometidos

- Recopila información de la empresa
- Estandariza datos y alimenta a la plataforma
- Encuentra amenazas y anomalias dentro de tu plataforma
- Visualiza y hace que los resultados sean un punto de acción

LUMU

El Avance de la Cybersecuridad



F (S): Security architecture

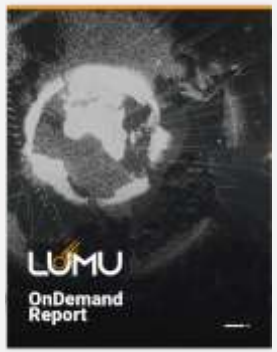
F (c): Compromise level

Sabores de Iluminación

Lumu Free
Una Chispa de Luz

- Visibilidad de Compromisos Confirmados
- Lumu Portal
- Toma de Metadatos: DNS en tiempo real
- Hasta 10 gateways
- 45 Días de Compromisos.

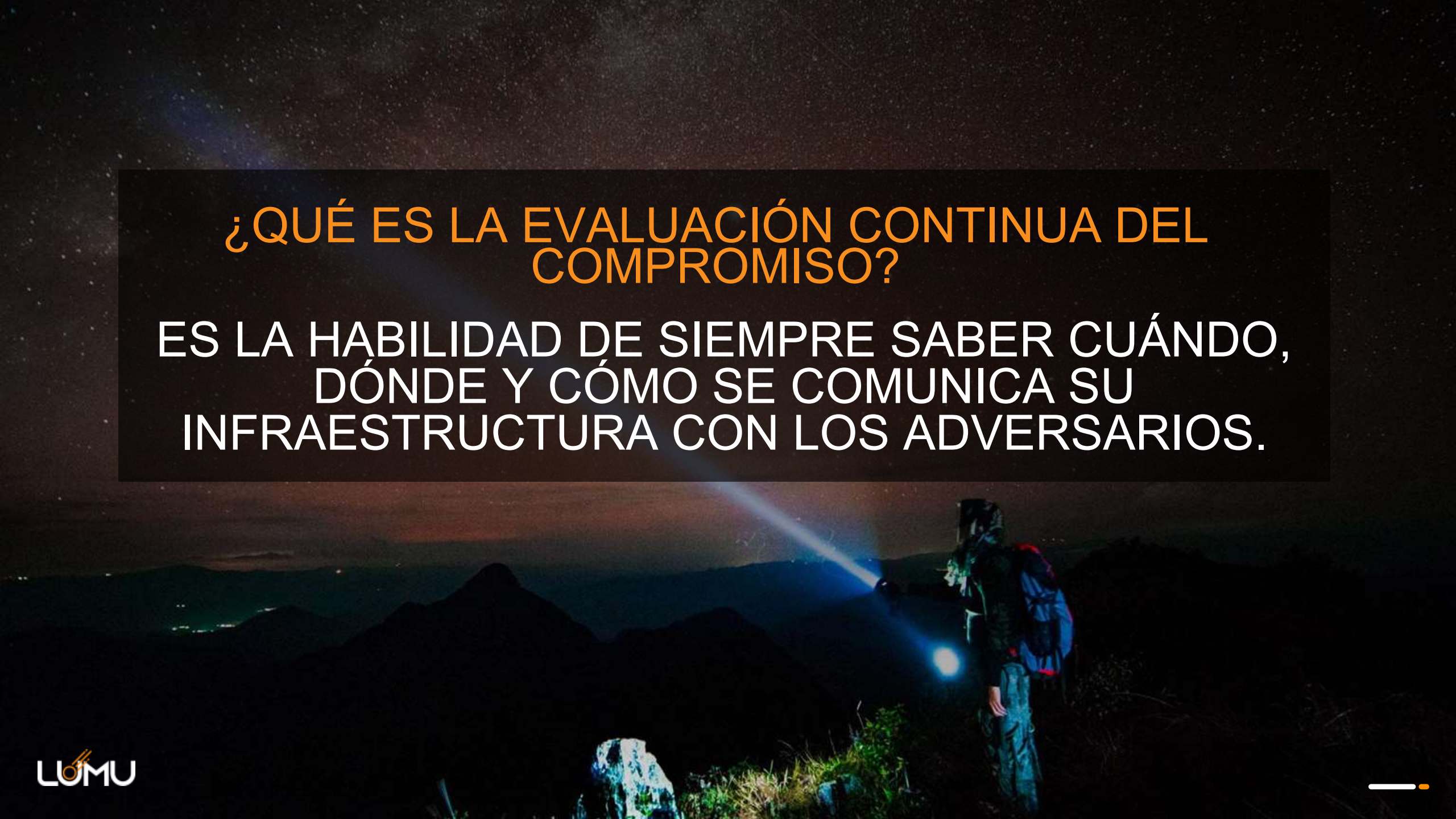
Lumu OnDemand™
Un Destello de Luz



- Evaluación de compromiso ad-hoc
- Ingestión completa de datos
- Confirmación de activos comprometidos
- Informe de Accionable

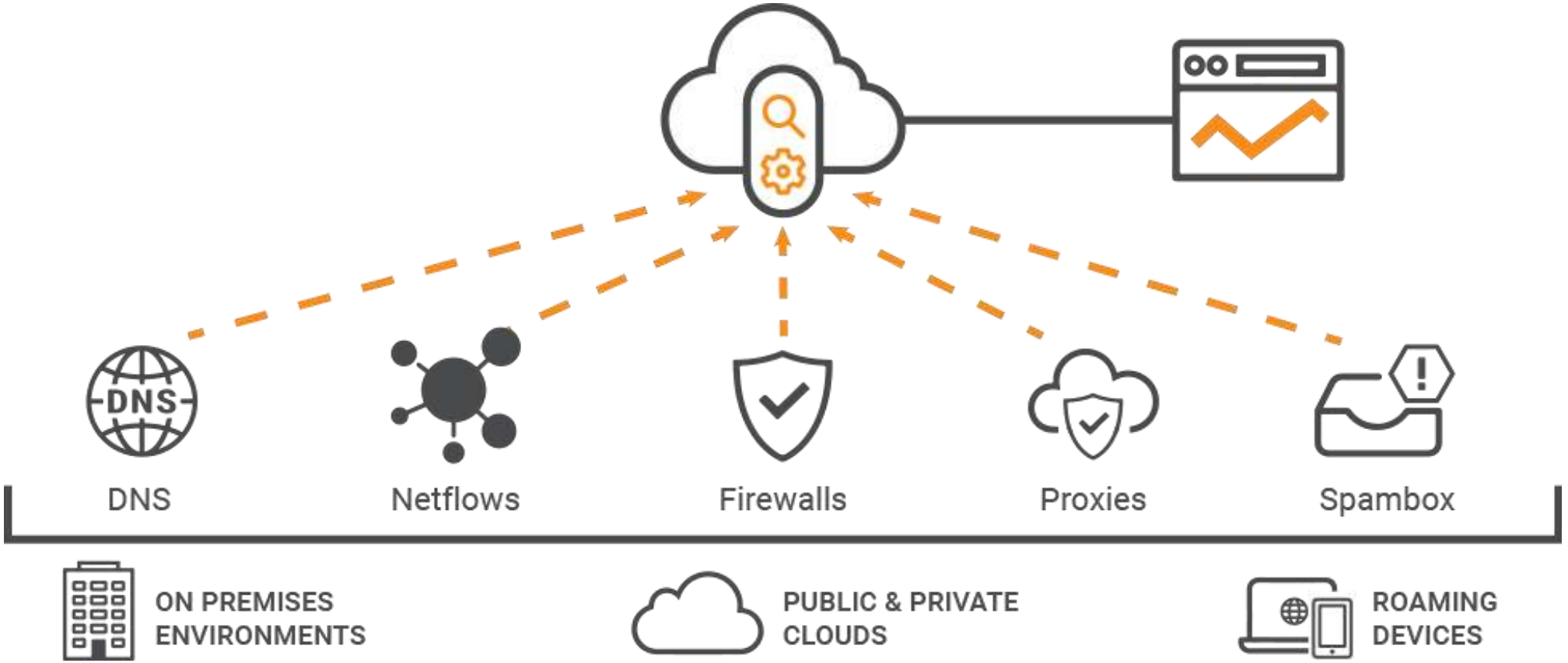
Lumu Insights™
Una Explosión de Luz

- Visibilidad detallada de IoCs confirmdos.
- Network metadata clustering
- Toma de datos en tiempo real, Multiples colectores.
- Virtual appliance data-collector Ilimitado
- No necesita agentes
- 2 Años de compromisos guardados.

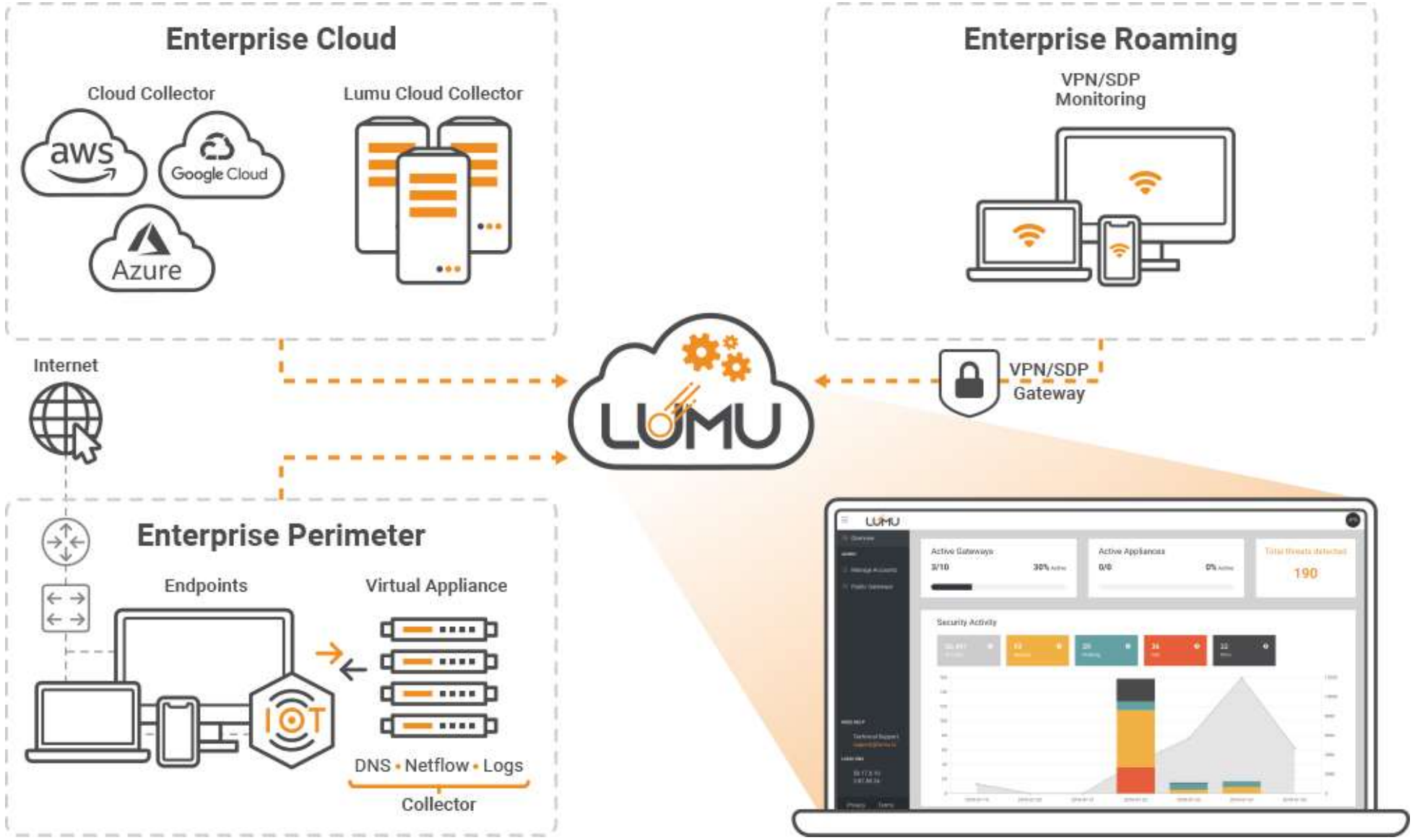

¿QUÉ ES LA EVALUACIÓN CONTINUA DEL COMPROMISO?
ES LA HABILIDAD DE SIEMPRE SABER CUÁNDO, DÓNDE Y CÓMO SE COMUNICA SU INFRAESTRUCTURA CON LOS ADVERSARIOS.
LUMU

Lumu Insights Data Collection

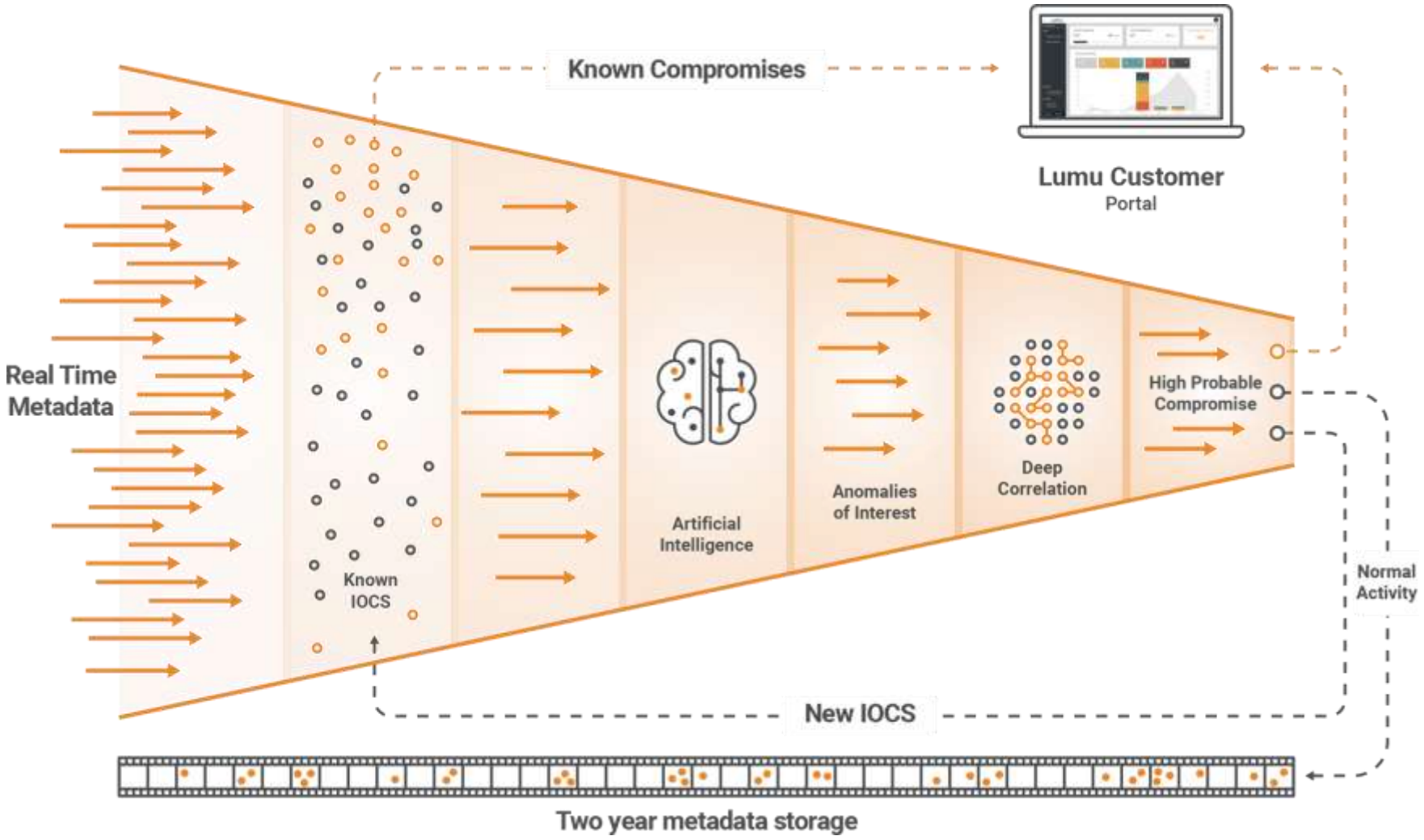
✓ *Video*



Arquitectura de Implementación



Proceso de Iluminación



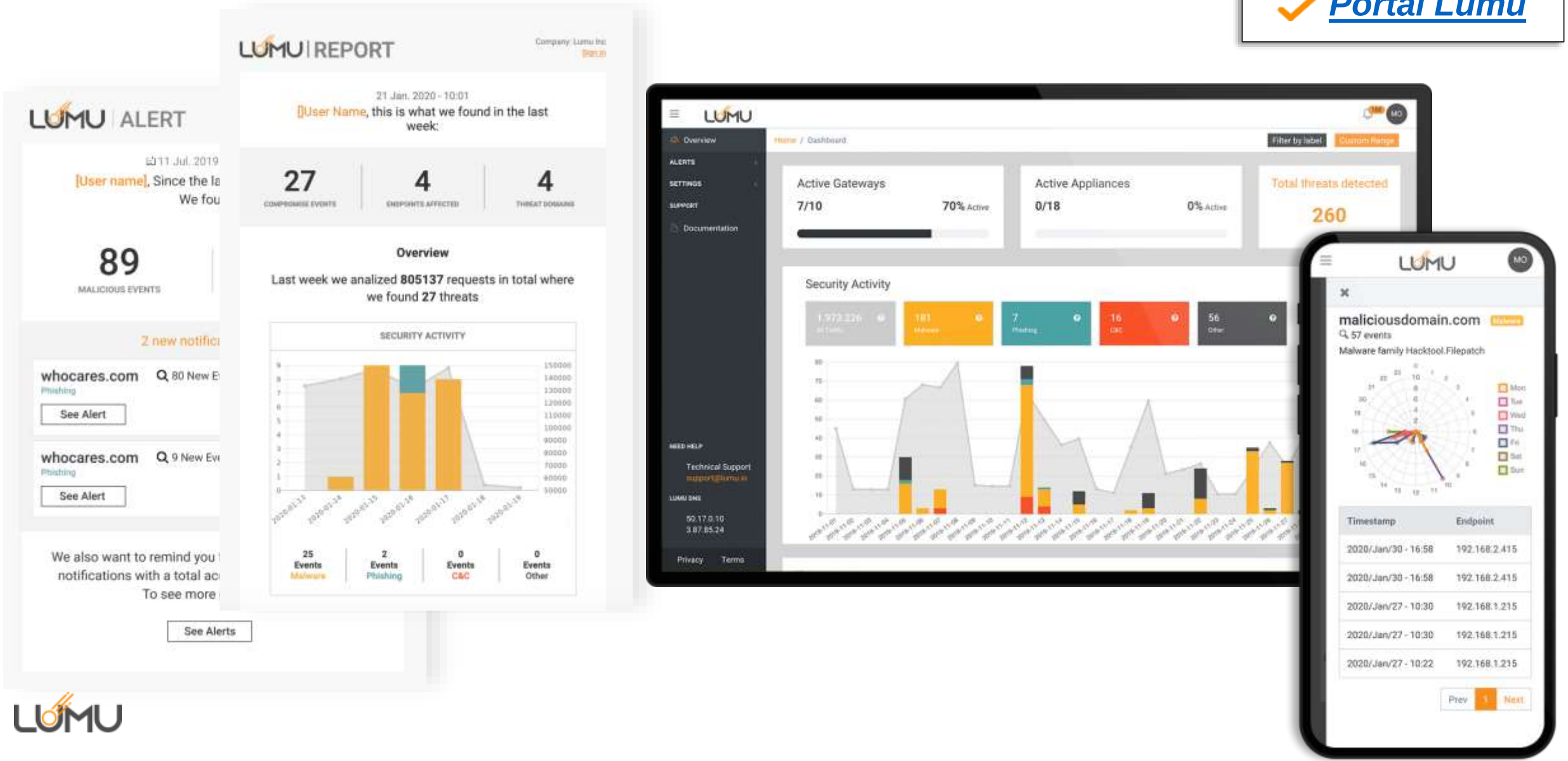
Extensive Cyber Intelligence

- Malware Patrol
- AbuseIPDB
- Alexa Top 1 Million sites
- Apility.io
- APT Groups and Operations
- AutoShun
- Binary Defense IP Banlist
- BGP Ranking
- BOTVRIJ.EU
- BruteForceBlocker
- C&C Tracker
- CertStream
- CCSS Forum Malware Certificates
- CI Army List
- Bambenek Malware
- Cisco Umbrella
- Critical Stack Intel
- C1fApp
- Cyber Cure free intelligence feeds
- DataPlane.org
- DigitalSide Threat-Intel
- Disposable Email Domains
- DNSTrails
- Emerging Threats Firewall Rules
- Emerging Threats IDS Rules
- ExoneraTor
- Exploitalert
- FastIntercept
- JoeWein
- DNS DH
- Immortal Malware Domains
- ZeuS Tracker
- FireHOL IP Lists
- FraudGuard
- Grey Noise
- Hail a TAXII
- HoneyDB
- Icewater
- Infosec - CERT-PA
- I-Blocklist
- IPsum
- Majestic Million
- Malc0de DNS Sinkhole
- Maldatabase
- MalShare.com
- Maltiverse
- Bambenek DGA
- Malware Corpus Tracker
- Malware Domain List
- MalwareDomains.com
- MetaDefender Cloud
- Netlab OpenData Project
- NoThink!
- NormShield Services
- OpenPhish Feeds
- PhishTank
- Ransomware Tracker
- REScure Threat Intel Feed
- Rutgers Blacklisted IPs
- SANS ICS Suspicious Domains
- Signature-base
- The Spamhaus project
- SSL Blacklist
- Ransomwaretracker
- Monero Miner Check
- Statvoo Top 1 Million Sites
- Strongarm, by Percipient Networks
- Talos Aspis
- threatfeeds.io
- Technical Blogs and Reports, by ThreatConnect
- Threatglass
- ThreatMiner
- WSTNPHX Malware Email Addresses
- UnderAttack.today
- URLhaus
- VirusShare
- Yara-Rules
- 1st Dual Stack Threat Feed by MrLooquer
- Malware Domains

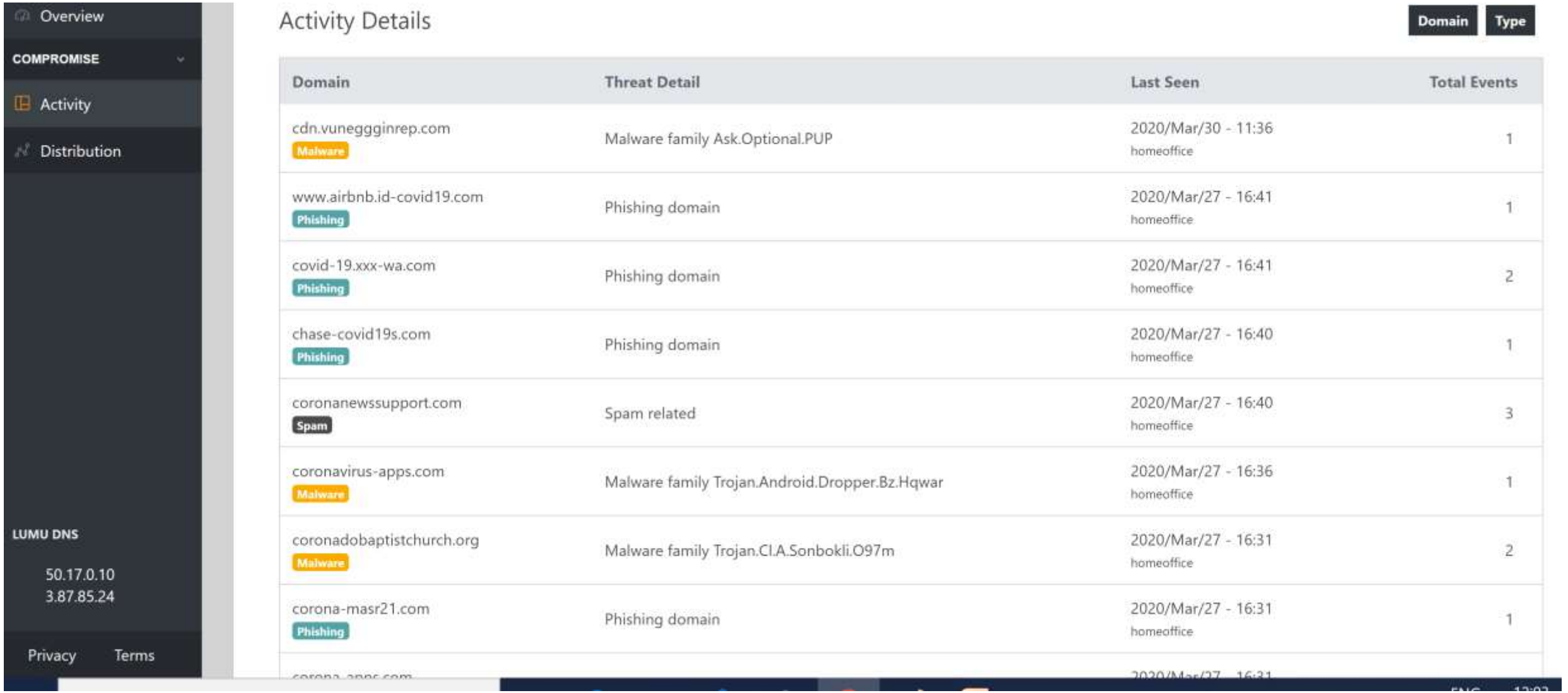
LUMU

No podemos proteger Aquello que no vemos

✓ Portal Lumu

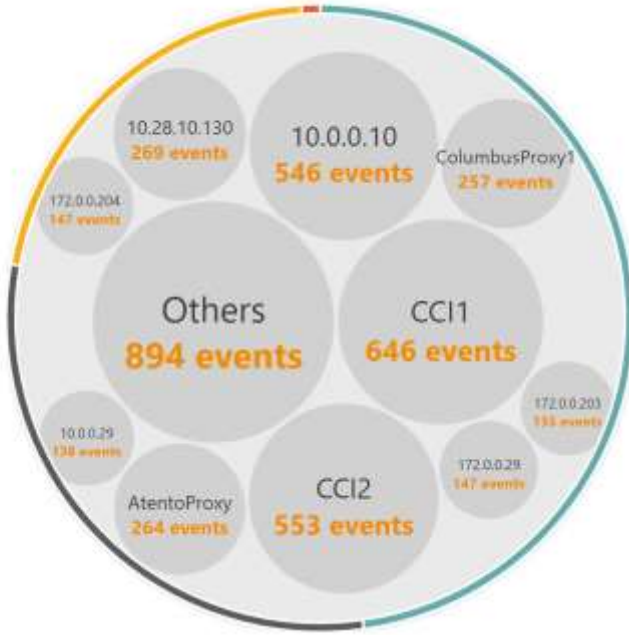


No podemos proteger Aquello que no vemos



No podemos proteger Aquello que no vemos

Distribution



Unlabeled Activity
2.35B Queries in total

Malware	21.3% (891 events)	Phishing	47.8% (2K events)
C&C	1% (40 events)	Other	30% (1.25K events)

✓ [Portal Lumu]

Distribution Details

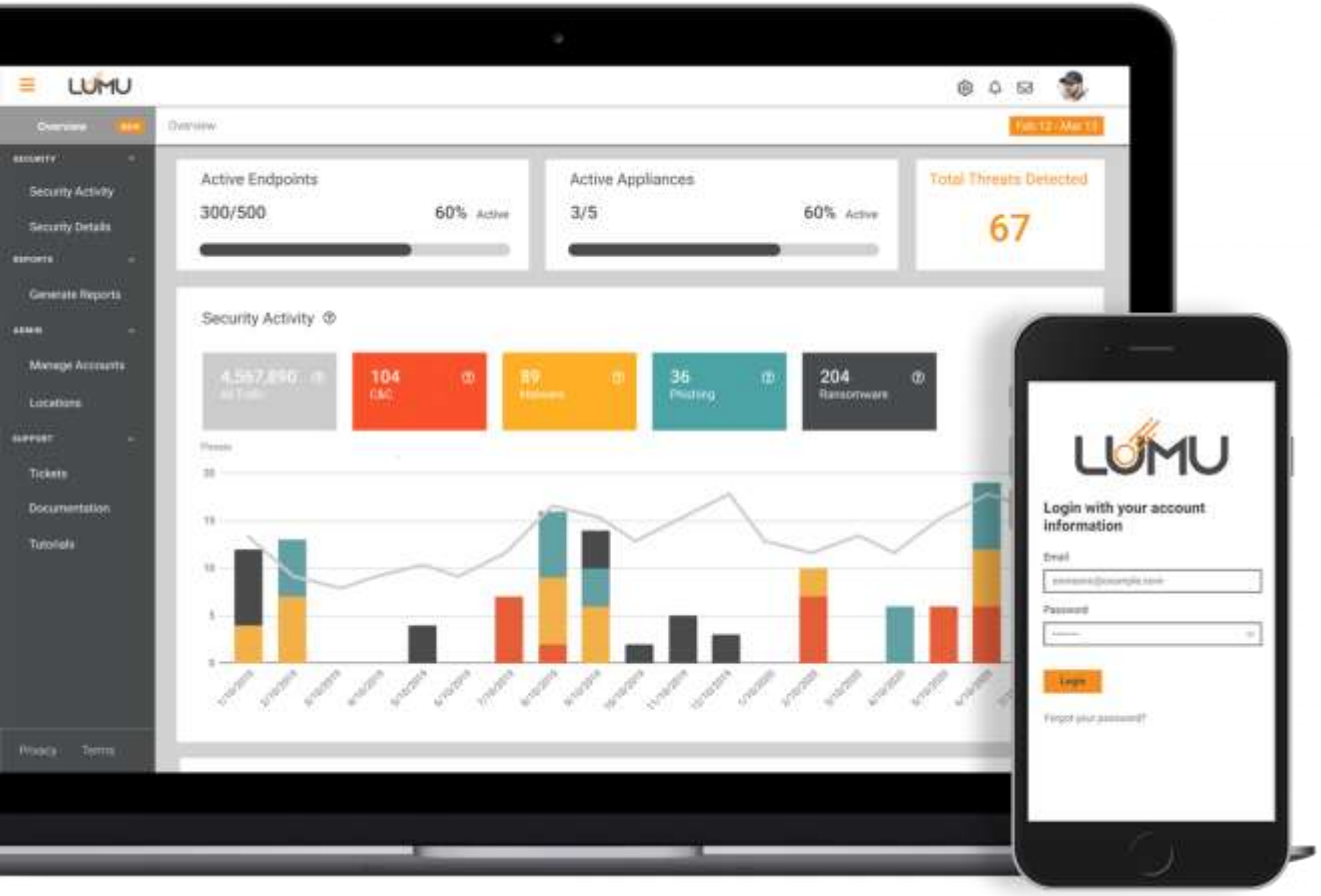
Endpoint | Type

Endpoint	Source	Threats	Trend	Label
Javier	Gateway	12		Unlabeled Activity
Bogota Office	Gateway	455		Bogota
Test1	Gateway	8		Unlabeled Activity
192.168.1.99	Custom Collector	12		Unlabeled Activity
192.168.1.7	Custom Collector	1		Unlabeled Activity
cdeiro.local	Virtual Appliance	34		Unlabeled Activity
192.168.0.7	Virtual Appliance	18		Unlabeled Activity
192.168.1.128	Custom Collector	6		Unlabeled Activity
192.168.1.5	Custom Collector	11		Unlabeled Activity
192.168.1.115	Virtual Appliance	181		Unlabeled Activity

Rows per page: 10 ▾ Prev 1 Next

LUMU

Caracteristicas Clave:



Identifica IOCs

Aumenta tu Defensa

Implementación Transparente

Illumina los Puntos Ciegos

LUMU

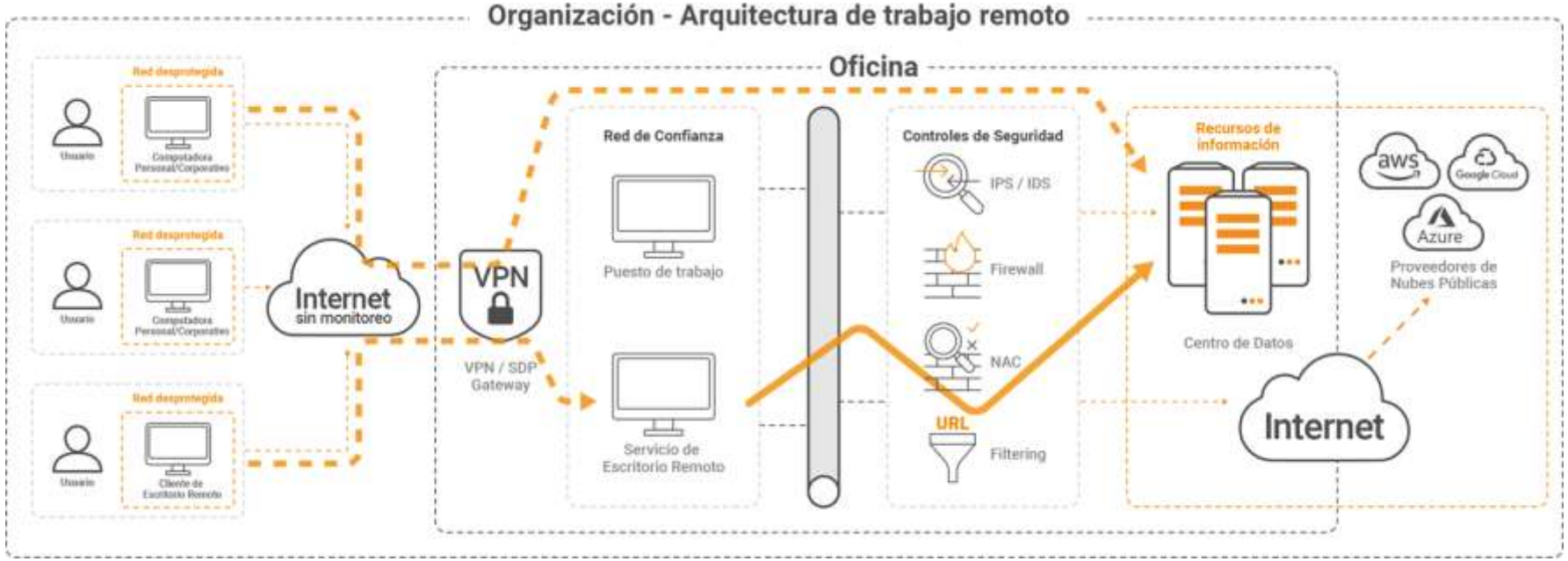
El Surgimiento del Trabajo Remoto Aumenta Importancia en la Visibilidad de Compromisos

Rubén A. Bayud
BDM Southern Cone
rbayud@lumu.io

Impacto en la Red

Antes

Ahora



La Necesidad Imperativa de una Visibilidad Mejorada

Interrupción repentina del lugar de trabajo

Algunos controles de seguridad se anularon

Equipos de seguridad adaptándose aún al trabajo remoto

Organizaciones no preparadas para BYOD

Protección en manos de los usuarios finales

Cibercriminales motivados

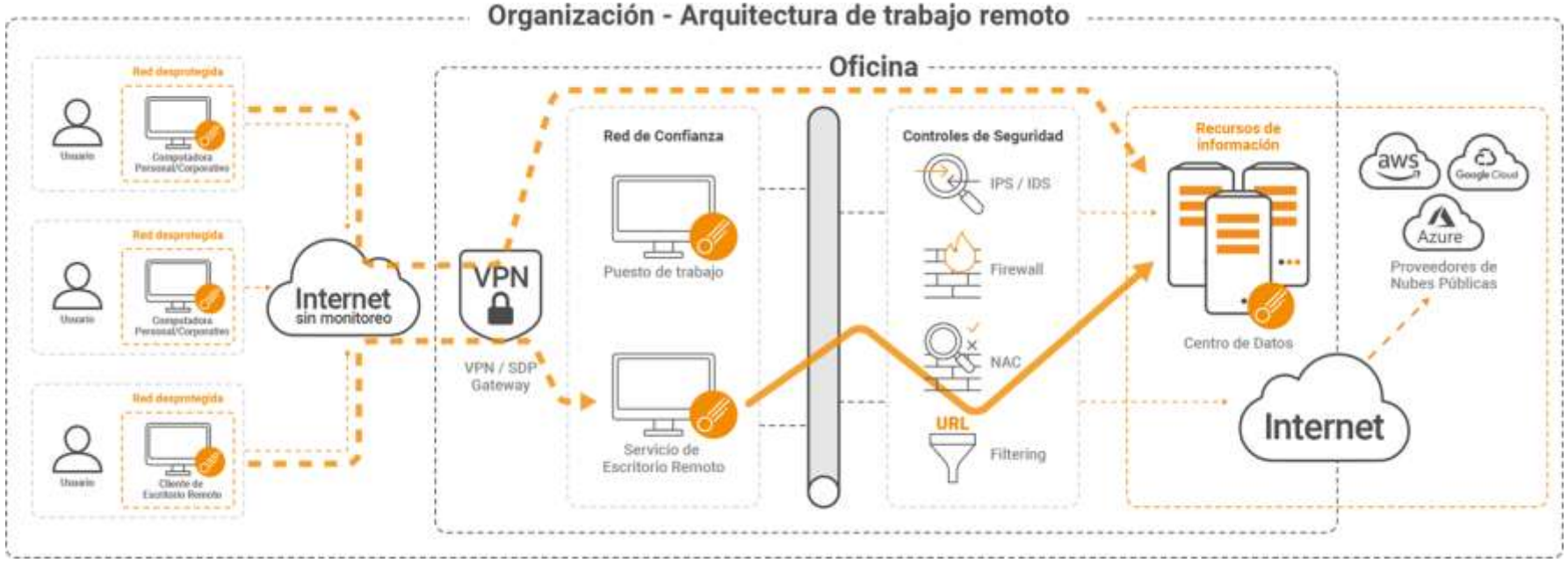
LUMU

Cómo ayuda Lumu

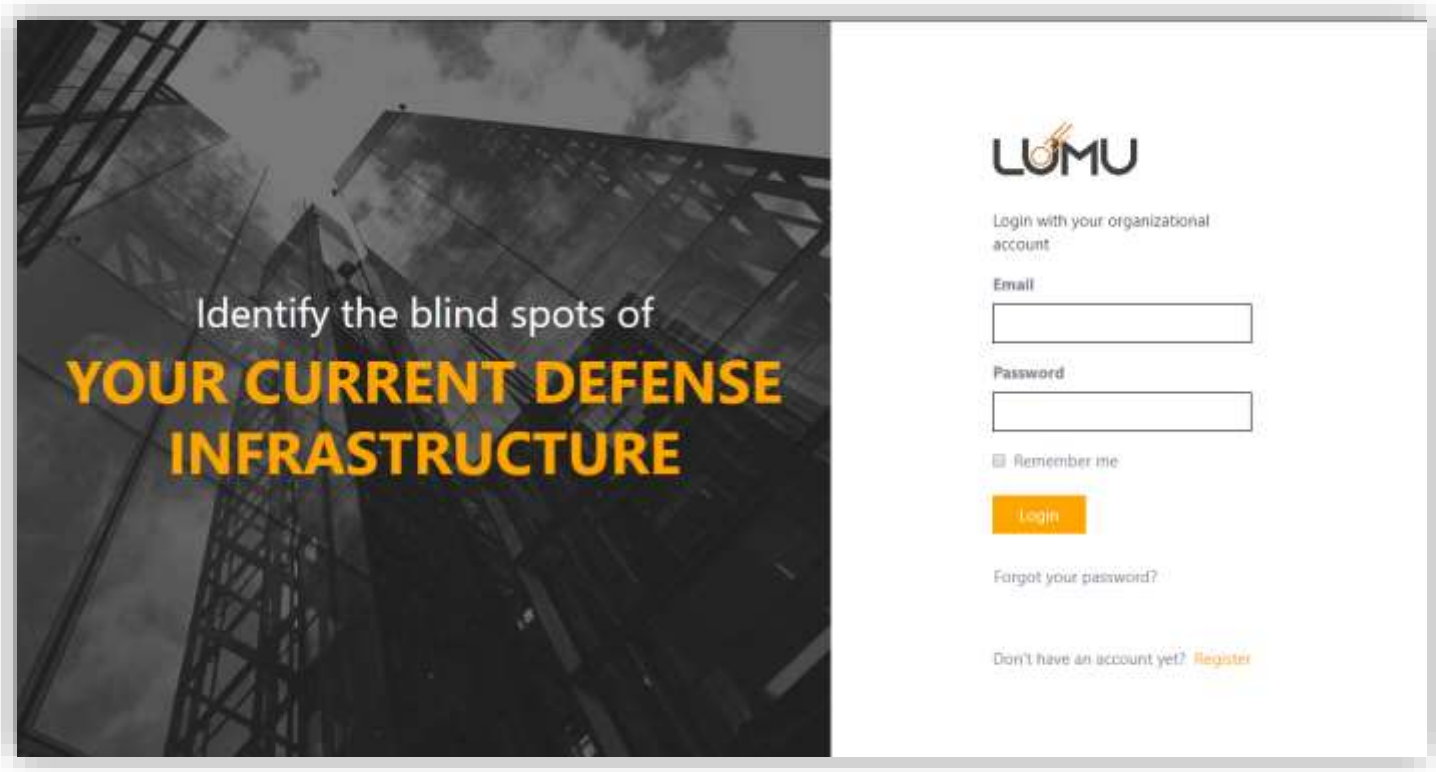
Antes

&

Ahora

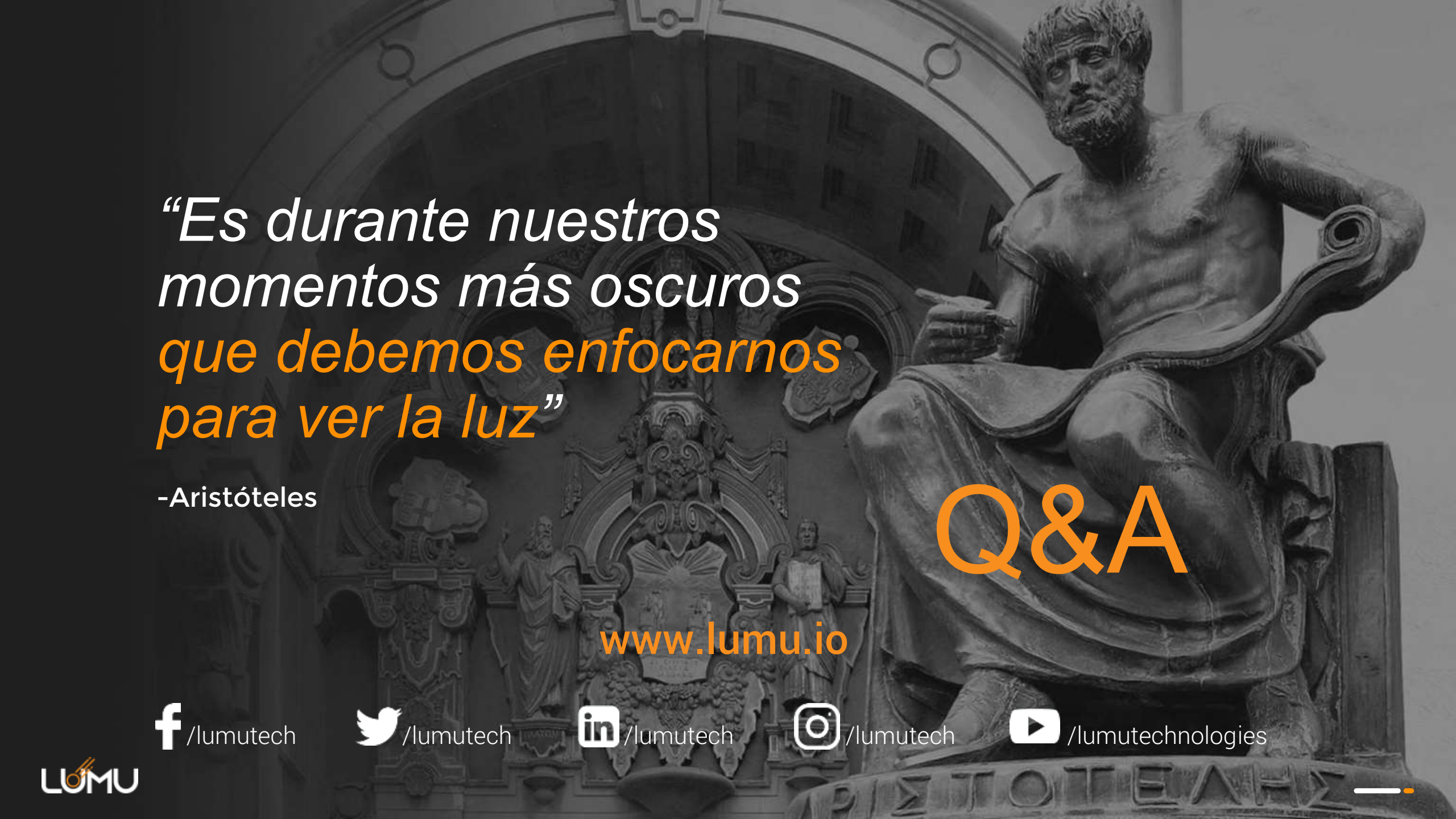


Implementación Transparente = ROI Instantaneo



- **Step 1:** Apunta tus DNS a Lumu
- **Step 2:** Conectate a https://portal.lumu.io e identificá ataques que afectan a tu empresa.
- Disfruta aumentando la seguridad con Lumu

✓ GUIA


“Es durante nuestros momentos más oscuros que debemos enfocarnos para ver la luz”
-Aristóteles
Q&A
www.lumu.io
/lumutech
/lumutech
/lumutech
/lumutech
/lumutechnologies
LUMU