

Innovating for the Future

Cisco's 3-Year Strategy

John Dominguez
Territory Business Manager
Andean Region

Customer Priorities

Reimagine Applications

Power Hybrid Work

Transform Infrastructure

Secure Enterprise



Our Strategy

Help customers connect,
secure and automate to
accelerate their digital agility
in a cloud-first world

Cisco's Strategic Pillars

Secure, Agile Networks

Optimized Application Experiences

Future of Work

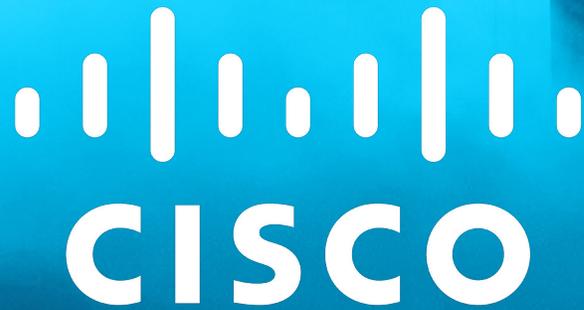
Internet for the Future

End-to-End Security

Capabilities at the Edge

Our Commitment

To drive the most trusted customer experience in the industry, through our innovation, choice and extraordinary people



Arquitectura de Seguridad Empresarial

Miguel Torrez Zamora

Systems Architect

Andean Region

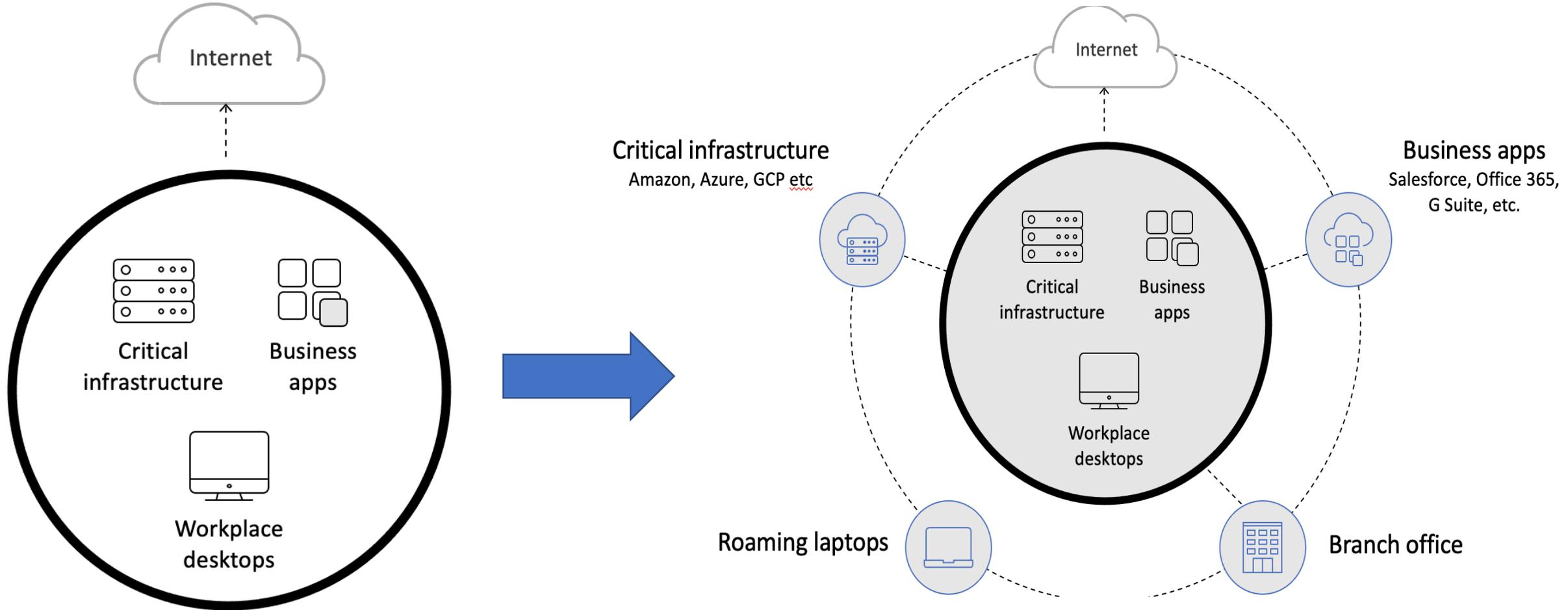
Entorno empresarial actual



- Explosión de dispositivos
- Fuerza de trabajo distribuida
- Uso de múltiples nubes

- Poca visibilidad
- Pocos expertos
- Poca integración

Entorno empresarial actual



Desafíos



TRANSFORMACION DIGITAL

*Aprovechar los beneficios
de la nube, la movilidad y
el IoT.*



CANTIDAD DE AMENAZAS CRECIENTE

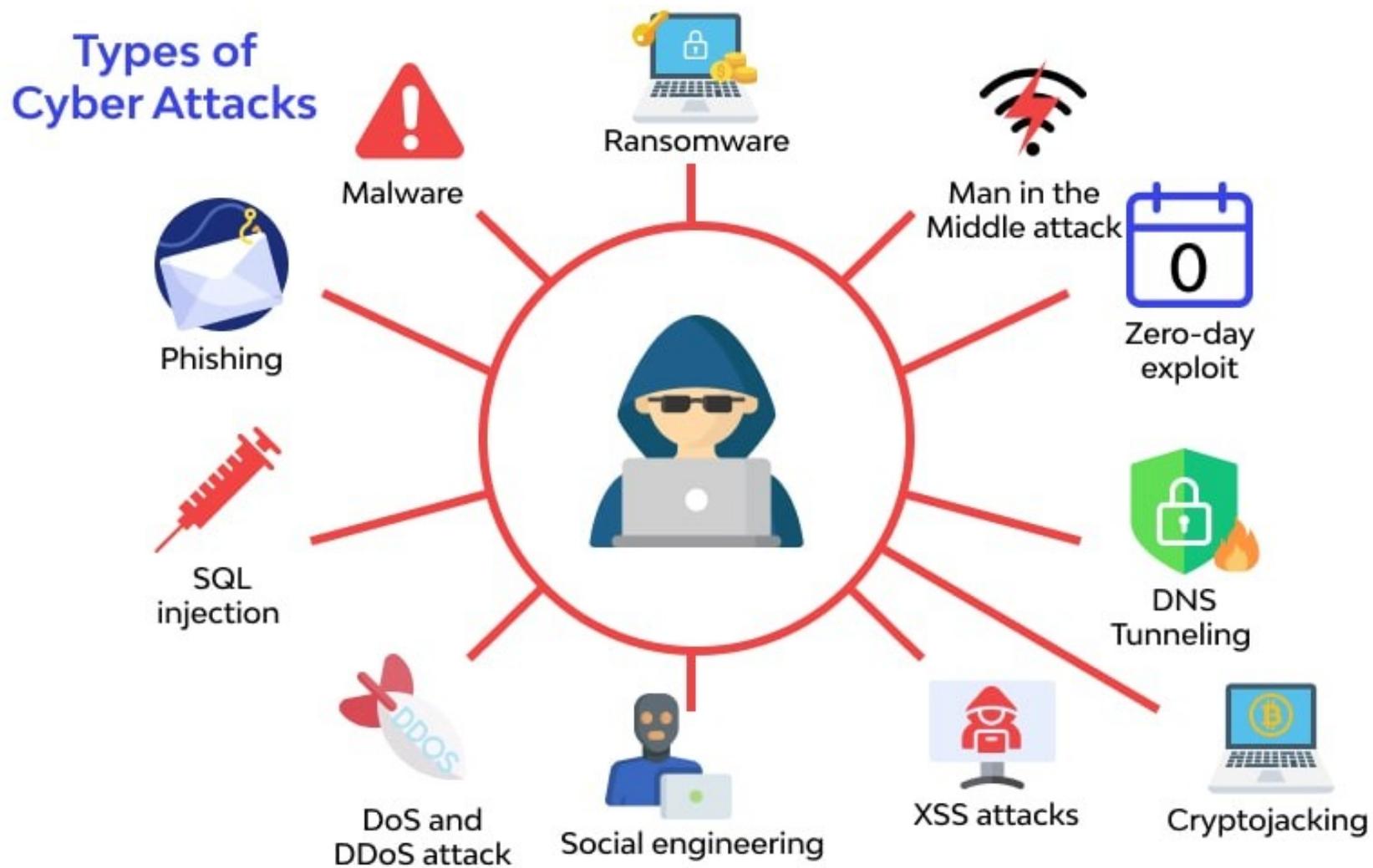
*Proteger contra mas y
nuevos vectores*



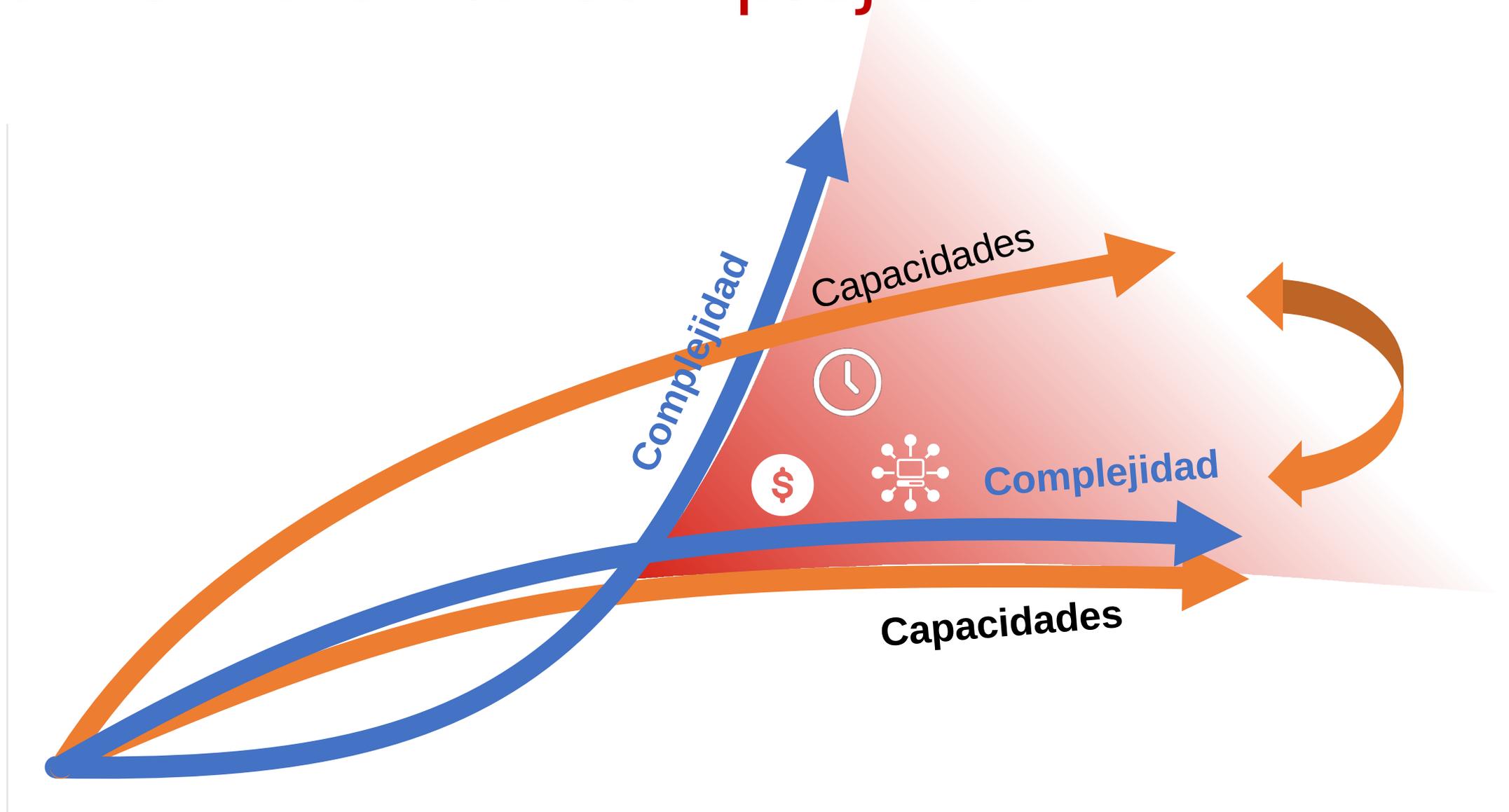
AUMENTO EN LA COMPLEJIDAD

*Simplificar operaciones y
reducir costos*

Cantidad creciente de amenazas



Aumento en la complejidad

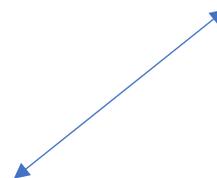


Transformación digital



En los últimos años:

¿Tiene un problema?



¿Que tan efectiva es nuestra política de seguridad?

¿Donde empezamos?



Detener las
amenazas en el
borde



Controlar quien
ingresa a la red



Encontrar y
contener los
problemas



Proteger a los
usuarios



Aplicar
segmentación
de red

Se necesita una arquitectura de seguridad

Visibilidad

No puedo proteger lo que no puedo ver

Segmentación

Reducir el alcance del ataque



Basada en la intención

Analíticos



Automatización

Inteligencia de amenazas

Protección

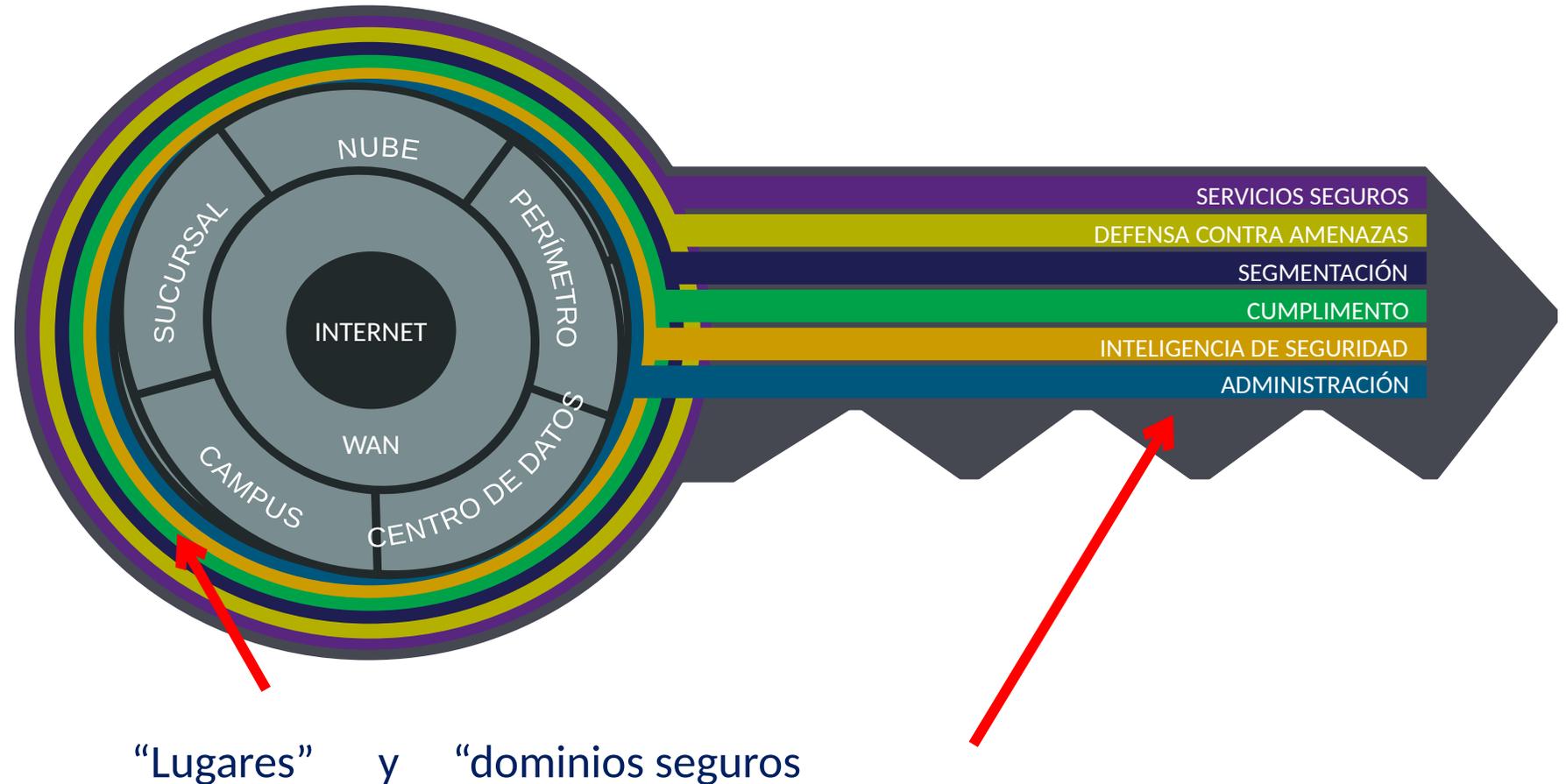
Detener los ataques



Metodología

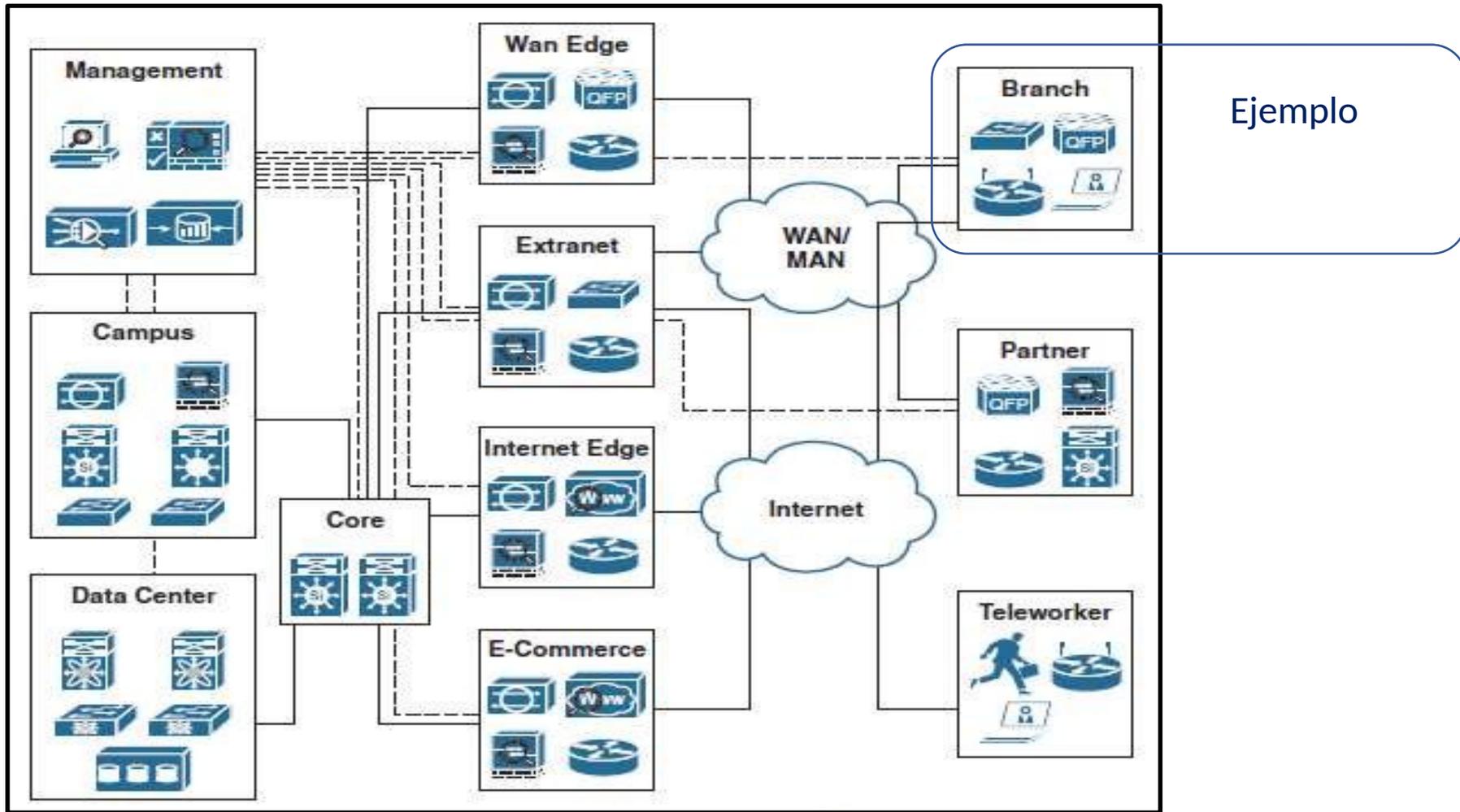
1. Dividir la infraestructura – PIN
2. Categorizar los riesgos y amenazas.
3. Construir la solución de seguridad:
 1. Funciones
 2. Arquitectura
 3. Bajo nivel

Enfoque de arquitectura no de producto



Dividir la infraestructura

La estrategia de seguridad extremo a extremo



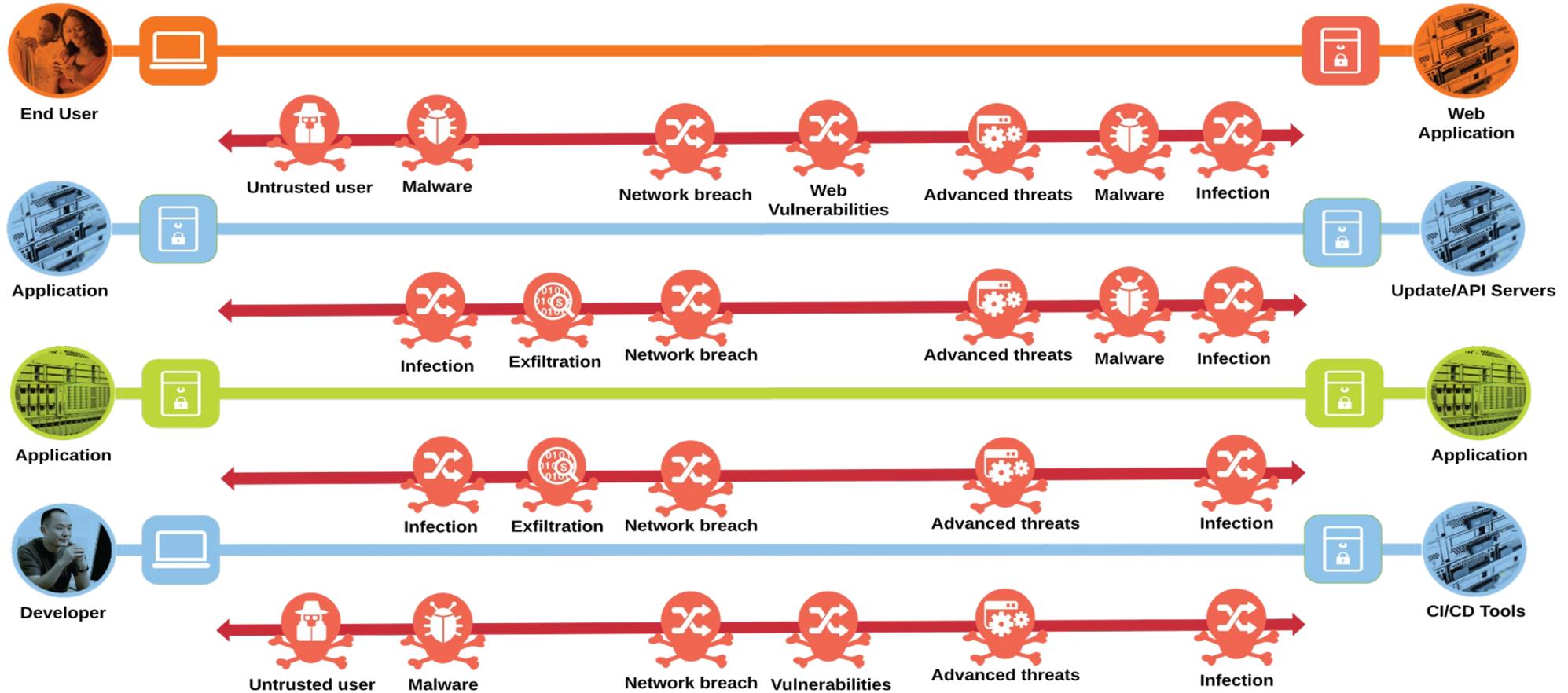
Categorizar los riesgos

Identificar los flujos



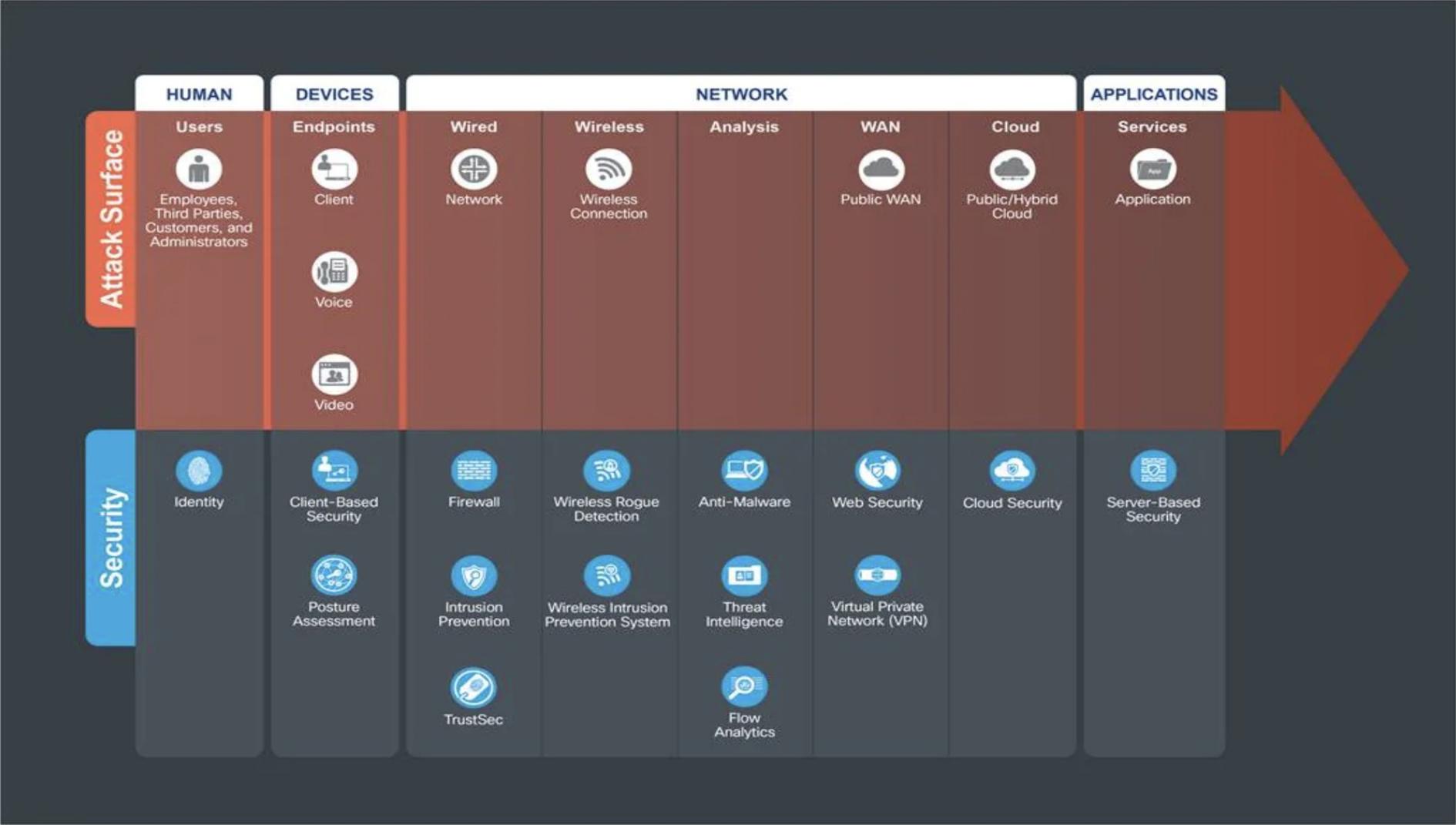
Categorizar los riesgos

Identificar las amenazas



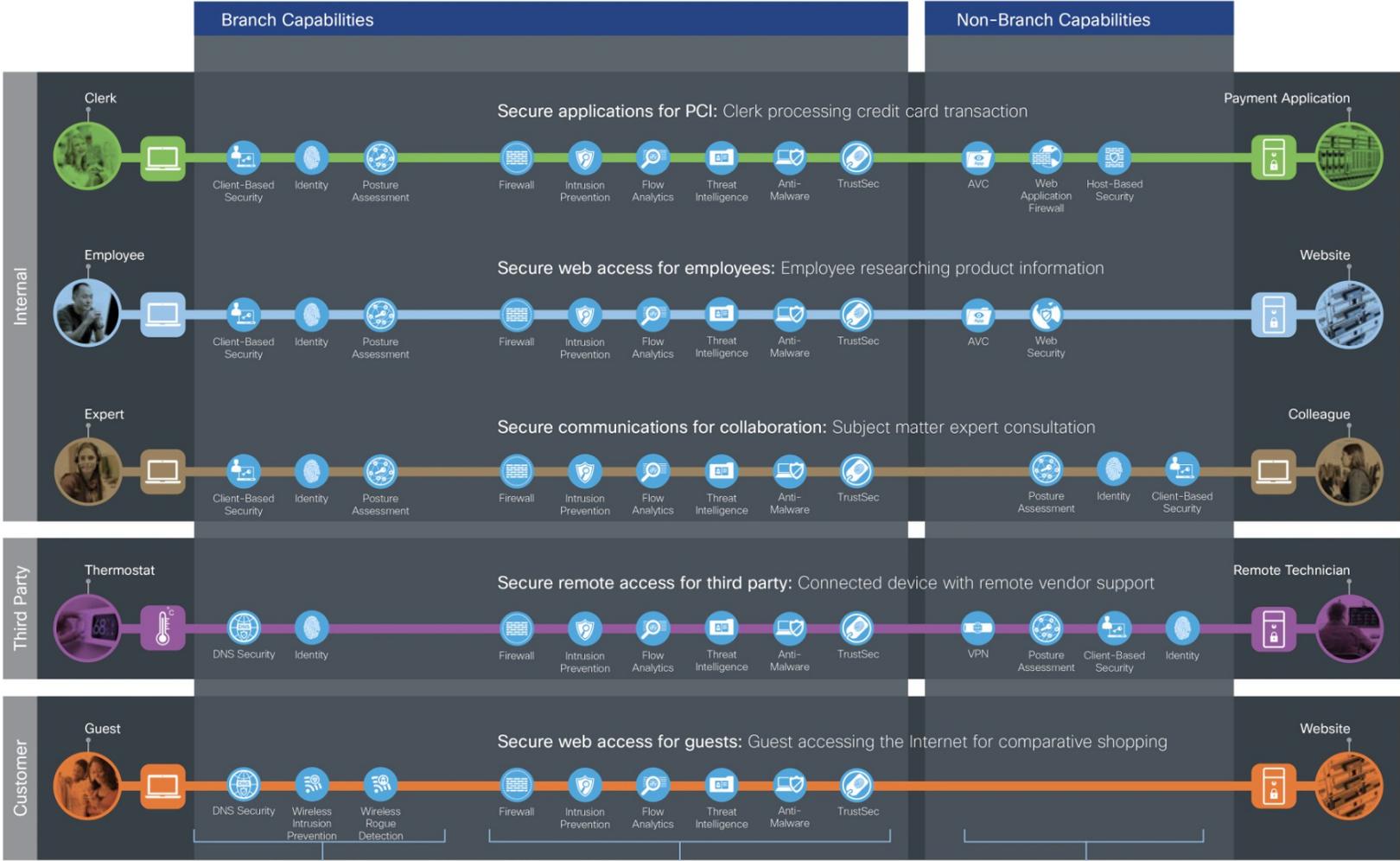
Categorizar los riesgos

Identificar el impacto



Categorizar los riesgos

Mapear con las capacidades requeridas



Categorizar los riesgos

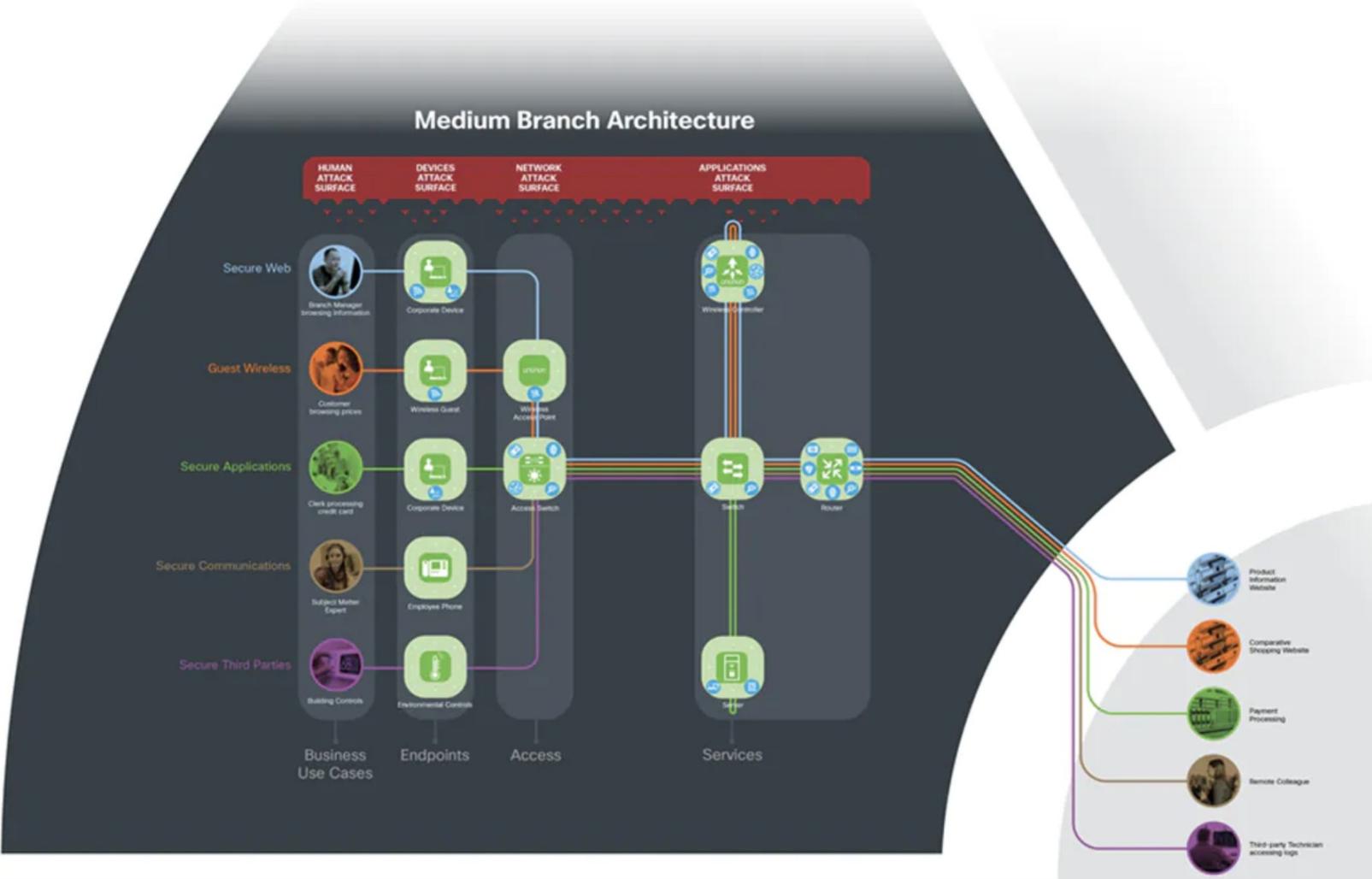
Mapear con las capacidades requeridas

AMENAZA		CAPACIDAD	
	Atacantes accediendo a información restringida		Acceso basado en la identidad
	Ataques de red desde usuarios externos		Segmentación
	Ataques usando virus, gusanos, etc		Prevención de intrusiones
	Distribución de malware entre cargas de trabajo		Anti-malware
	Exfiltración de datos, amenazas encubiertas		Analítica de flujos
	Redirección de sesiones a dominios maliciosos		Seguridad DNS
	Explotar vulnerabilidades no parchadas		Evaluación de vulnerabilidades e inventario de cargas
			Evaluación de postura de seguridad

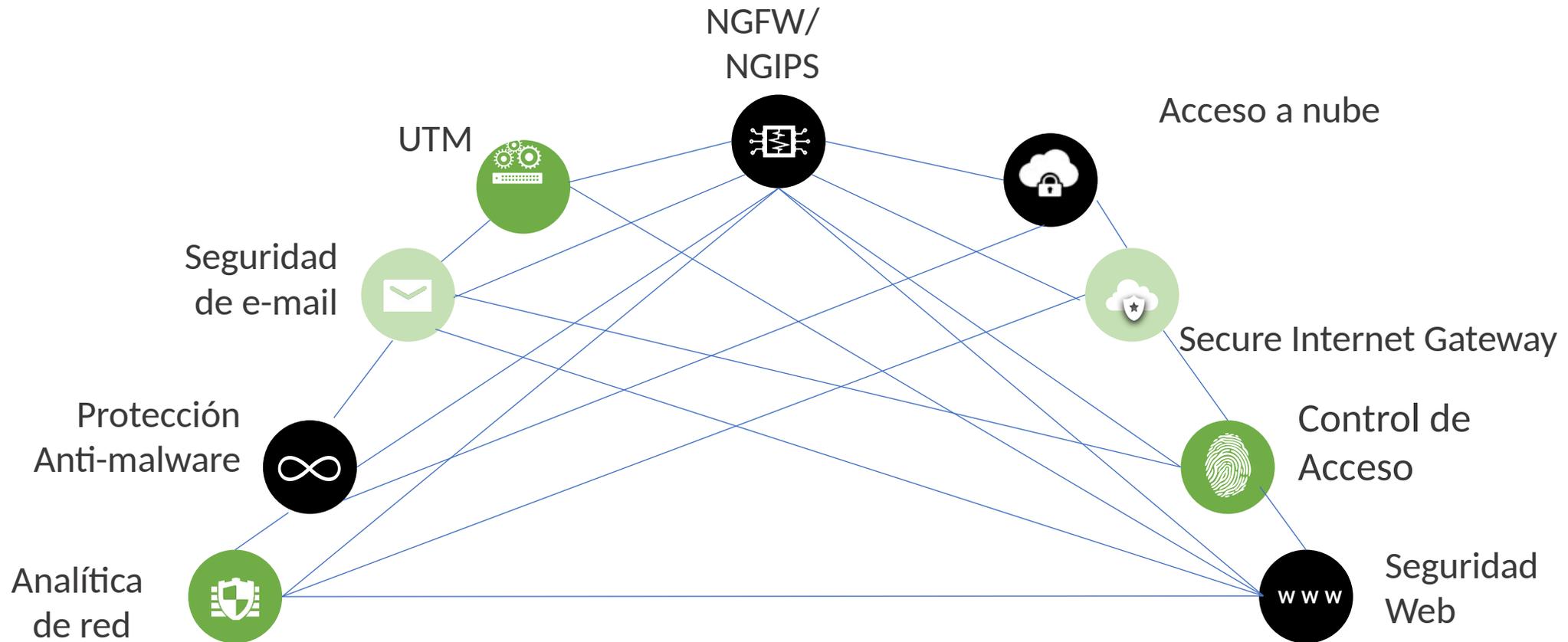


Construir la solución de seguridad

Diseño alto nivel



Arquitectura



Seguridad E2E Portafolio

TALOS

Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

SECURE X (XDR)

Managed Detection and Response Services

Security, Orchestration, Automation and Response

Incident Response and Remediation Services

Threat Visibility & Hunting

Device Insights

Kenna Vuln Mgmt

Secure Cloud Insights

3rd Party Integrations

User/Device Security

ZERO TRUST WORKFORCE

Adaptive MFA | Passwordless | Trust

Duo Secure Access | Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed



Cisco Secure Client

VPN

Posture

Telemetry

Threat

Query



ThousandEyes (Visibility)

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE)

Threat Protection | Secure Access Control | Managed Remote Access

Umbrella/Duo



PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible

SDWAN



On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security



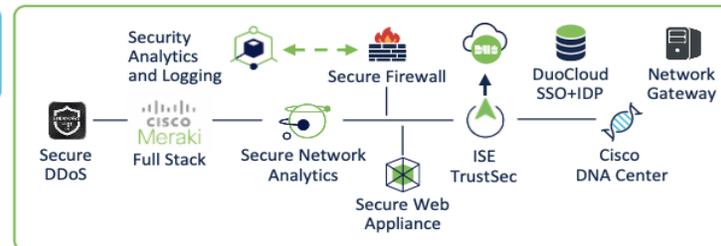
IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT



ZERO TRUST WORKPLACE

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility



Application Security

ZERO TRUST WORKLOAD

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack



App Visibility | Detection | Response



Gracias!