SUSESEC

NOVIEMBRE 2022

El valor de las certificaciones en la estrategia de seguridad

Juan Herrera Utande - SUSE

SUSExchange
Innovation for decision makers

Agenda

- SUSE hoy
- Nuestra apuesta por la seguridad
- El valor de las certifications
- El valor para tu proyecto
- Herramientas y mejores prácticas
- Resumen

SUSE Hoy

Nuestra presencia en las principales verticales

Ayudamos a las empresas a innovar y transformarse digitalmente desde el núcleo de TI, a la nube, el Edge, … y !más allá!

9 / 10
Largest retailers

13 / 15
Largest pharma firms

14 / 15
Largest aerospace firms

10 / 10
Largest auto OEMs

5 / 5
Largest technology firms

13 / 15
Largest manufacturers

4 / 5
Largest healthcare firms

13 / 15
Largest finance firms

Source: Company information.
Note: Largest firms by revenue

Trabajamos con los líderes en tecnología y con las principals comunidades de código abierto

Partners

SUSE

Innovate everywhere

Comunidades

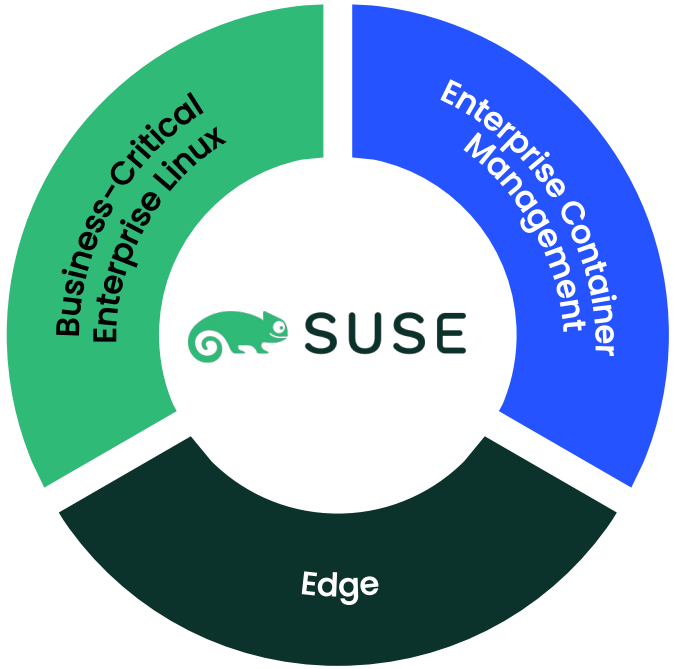
SUSE: un socio estratégico en todos los sectores

Finance	Information technology	Media and entertainment	Healthcare	Government / defense	Retail	Telecom	Manufacturing & automotive	Technology and other industries
AVIVA	Cisco	AMC	Cerner	BAE SYSTEMS	Carrefour	Bell	AIRBUS	Schneider Electric
Baillie Gifford	intel	Charter Communications	CVSHealth	Lockheed Martin	Office Depot OfficeMax	AT&T	DAIMLER	SIEMENS
Deutsche Bank	NVIDIA	CNN	Genentech	AIRBUS	The Home Depot	COX	BMW	Schlumberger
Fidelity Investments	Qualcomm	NBC	illumina	DB BAHN	Shoppers Drug Mart	DXC Technology	Audi	Honeywell
HSBC	SAMSUNG	nielsen	imagia		Kroger	Ericsson	TOYOTA	RioTinto
MIZUHO	SAP	SONY	invisalign	Ministry of Children, Community & Social Services	M&S EST. 1884	OPTUS	Elektrobit	tyco
Raymond James	servicenow	UBISOFT	Johnson & Johnson	Raytheon Technologies	Walgreens Boots Alliance	orange	Continental	BURTON
TD Bank	SOPHOS	ZIFF DAVIS	MERCK		Walmart	Telstra	BOSCH	BASF We create chemistry
usbank	teradata.		Pfizer		Woolworths	T-Mobile	SAIC	DUPONT
	Zillow				Hasbro	verizon	VW	UiPath

Principales áreas de negocio

Simplify and optimize existing environments

- Complexity of managing hybrid cloud infrastructure and apps
- Run workloads anywhere, containers, VMs, on-premises and across clouds
- Secure operation of all mission-critical workloads
- Need to eliminate downtime



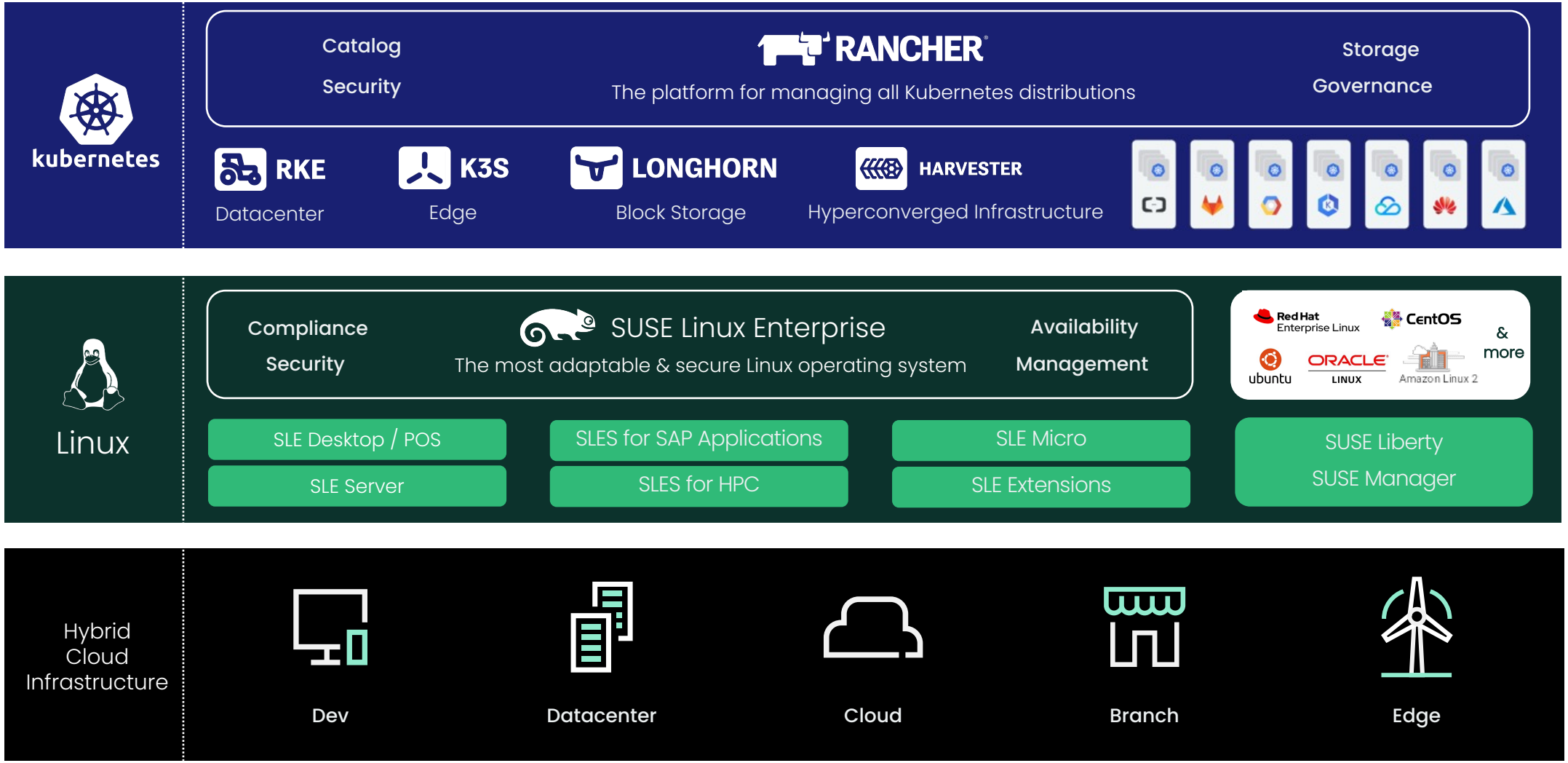
Bring apps and infrastructure into modern cloud computing

- Container and Kubernetes complexity
- Modernizing legacy apps and accelerating time to market
- Reduce cost and risk
- Secure Cloud Native apps

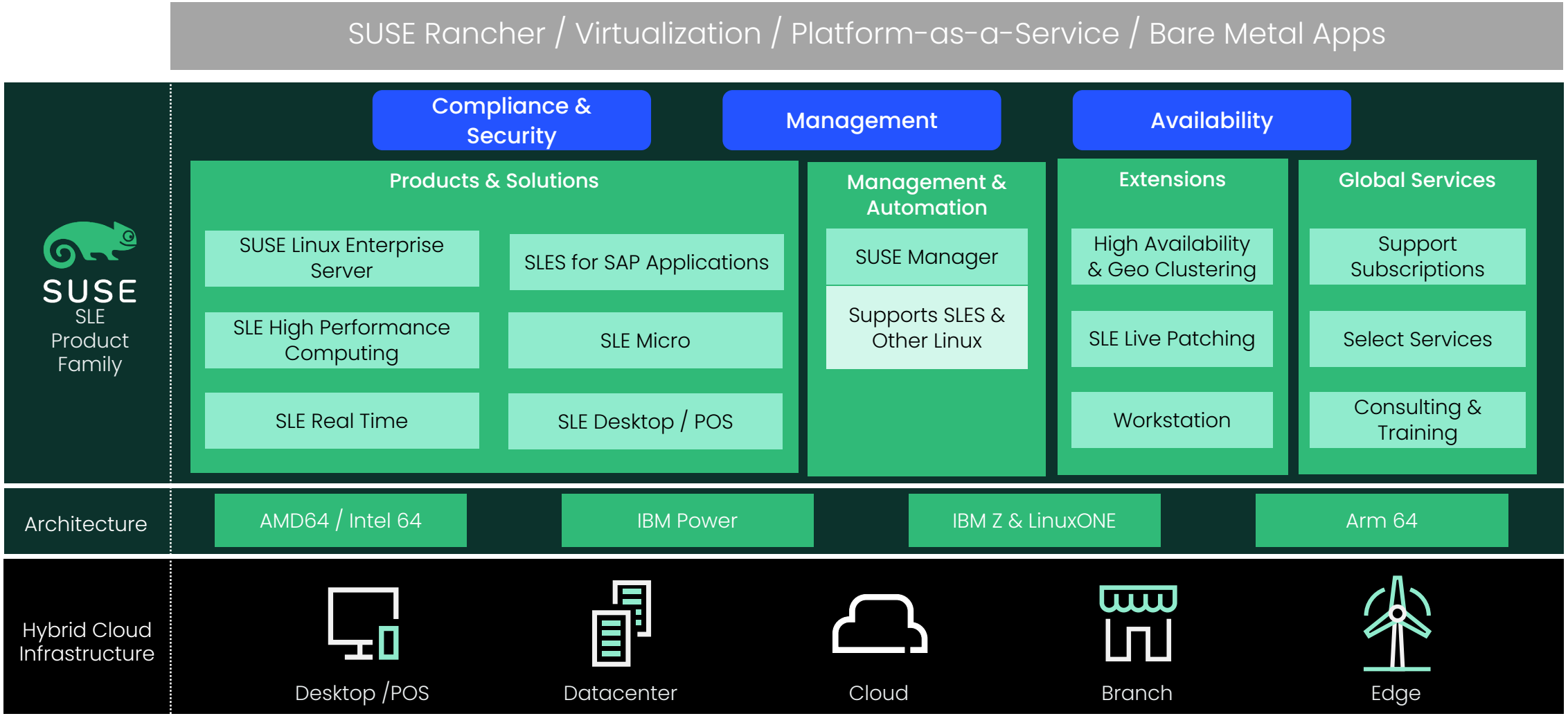
Accelerate business innovation

- Lack of a consistent platform from core, to cloud, to edge
- Concerns about security, privacy, compliance
- Breadth and complexity of edge use-cases

El portfolio de soluciones de SUSE



Linux para entornos críticos



Nuestra apuesta por la seguridad

El porqué de nuestra apuesta por la seguridad

Linux está adoptado masivamente pero no todos los Linux son iguales → diferenciadores

Los entornos en los que somos líderes tienen en común:
altamente regulados y necesitan de **certificaciones** y **validaciones específicas**.

- 85% de todos los entornos **SAP** usan SUSE: Los procesos de certificación de SAP son de los más exhaustivos de la industria de IT.
- Líderes en los sectores de **Defensa**, **Industria** y **Administración Pública** en Europa. Todos altamente regulados, requisitos estrictos de contratación, …
- Líderes en **HPC**. Gran parte vinculado a entornos sensibles. Capacidades de encryptación y aislamiento de procesos

→

Sectores de nicho

Esfuerzo en certificaciones

Calidad y robustez

Solución de Linux robusta con características únicas

Trasladar el valor de los entornos críticos a entornos Linux generalistas.
Generar confianza a través de soluciones validadas por terceros.

Mapa actual de certificaciones

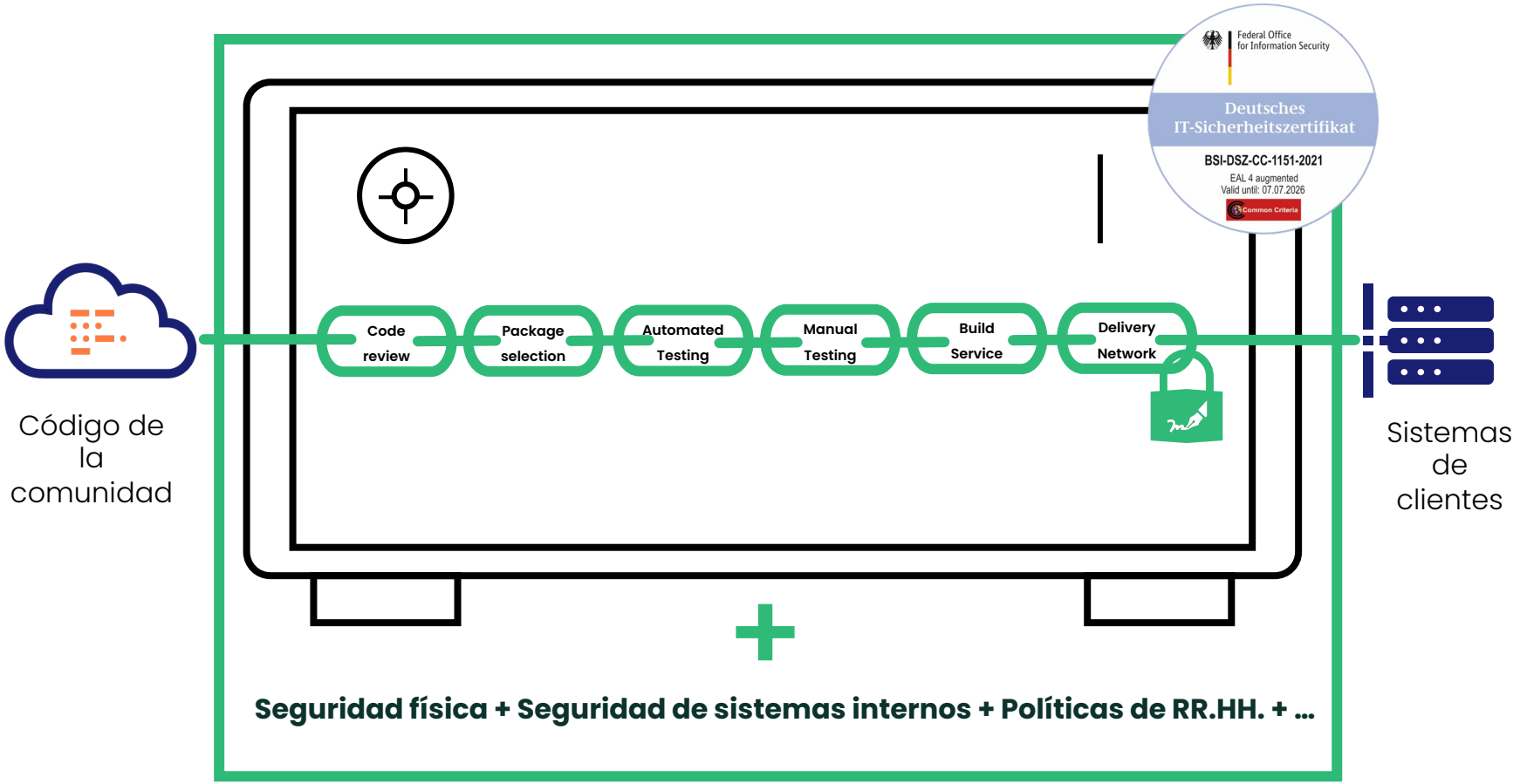
Un proceso que nunca termina … ¡y una apuesta sólida a futuro!

Projects / Certification	SLES	SLE Micro	SUSE Manager	SLE Real Time	SLES for SAP	SLE Automotive	Rancher Manager	Rancher RKE2	NeuVector	SUSE Org
BSI Common Criteria EAL4+	✓	En curso								
CCN (Spain)	✓	En curso								
ANSSI (France)	✓	En curso								
Common Criteria NIAP OSPP	✓	En curso	En curso							
FIPS 140-2/3	✓ / 4T23	Hereda	En curso	En curso	Hereda	Hereda		✓ / 4T23	En curso	
DISA STIG	✓	✓			Pendiente		✓	✓		
SCAP	✓	1T23	✓		Pendiente	Pendiente				
SLSA Level 4	✓							Pendiente		
NIST USGv6	✓									
CIS	✓						✓	✓		
ISO 27001/27701										1T23

https://www.suse.com/es-es/support/security/certifications/

Certificación Common Criteria EAL 4+

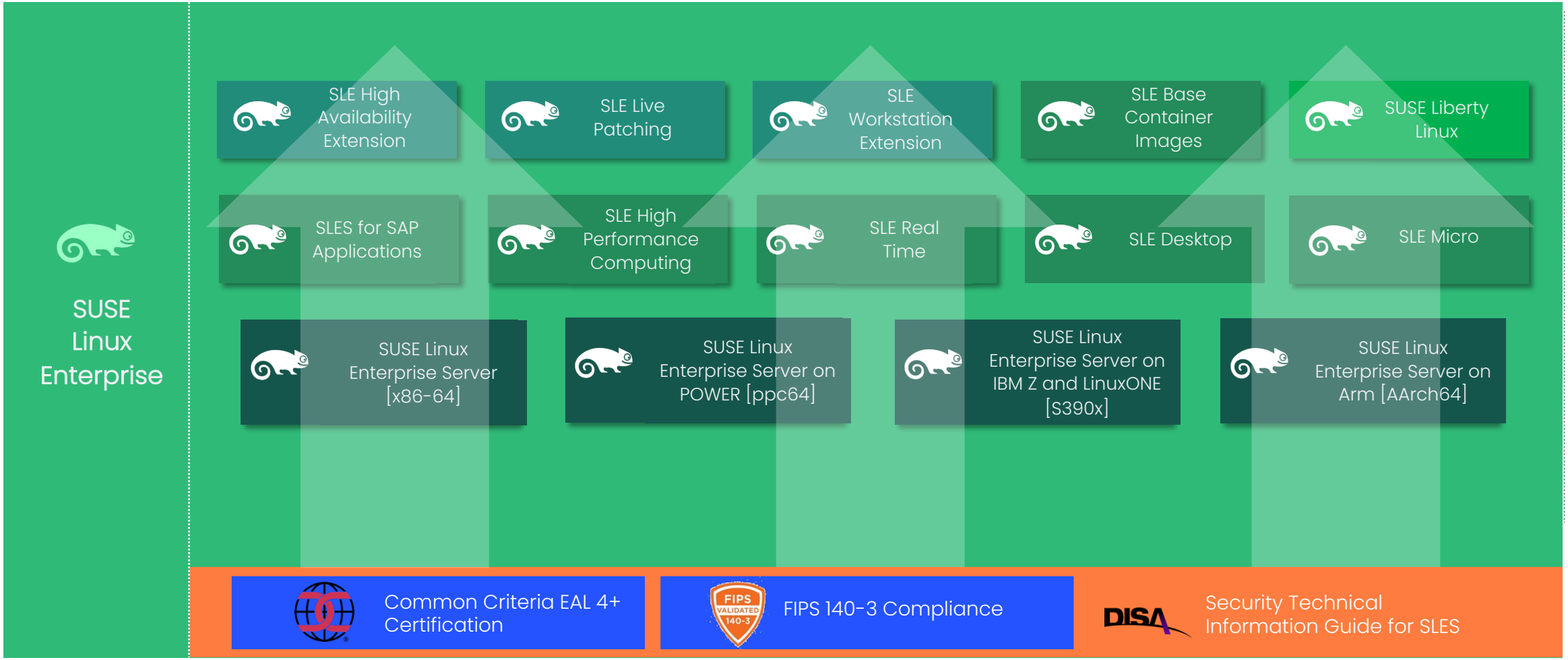
Confianza en la cadena de creación de software, procesos y herramientas



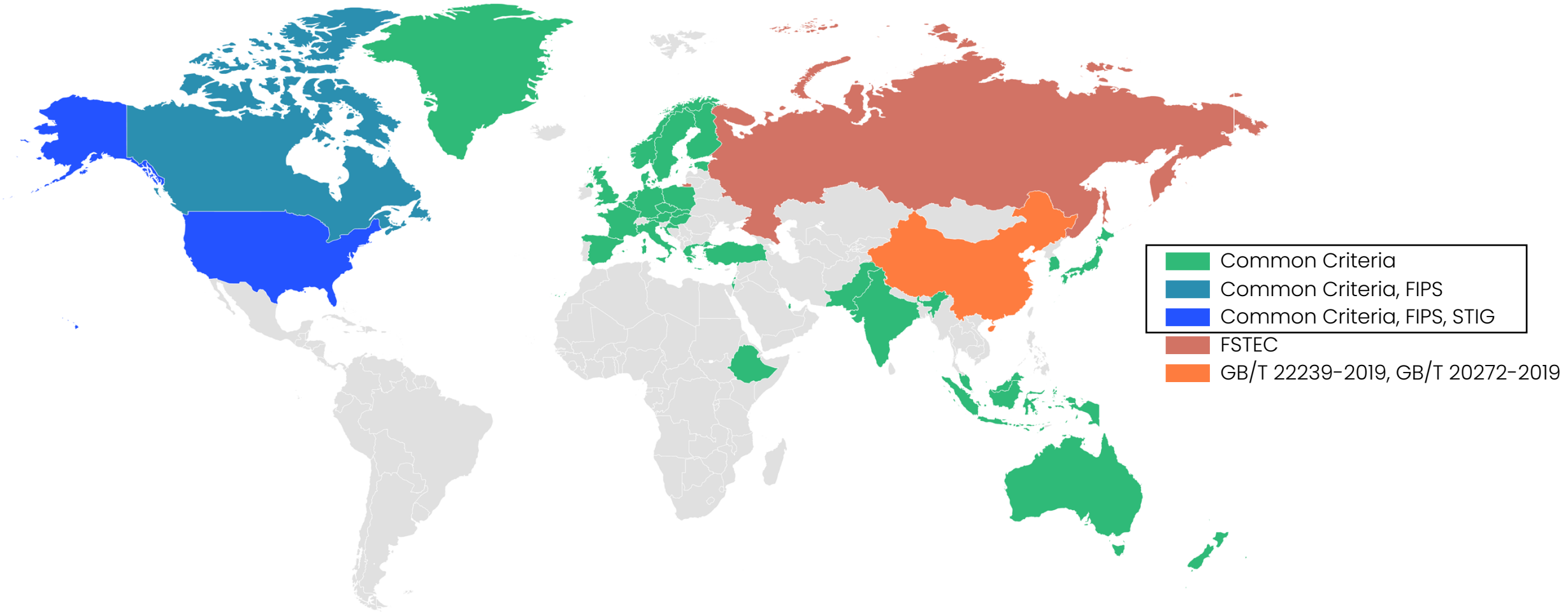
EAL 4+ Certified Secure Software Supply Chain

- ✓ Confianza para clientes y partners
- ✓ Beneficia a todo el portfolio
- ✓ Transversal: valida procesos internos, seguridad física, ...
- ✓ Clave para la obtención de ISO 27001/27701
- ✓ Reconocida mundialmente
- ✓ Único sistema operativo de propósito general certificado
- ✓ Prueba de calidad y seguridad en la construcción de software

Valor añadido para todo el portfolio de Linux



Aplicabilidad geográfica de certificaciones



Coverage by End-Customer location

Source: Gartner data; BCG analysis etc.

El valor de las certificaciones

Que aporta cada tipo de certificación

Program	What does it mean?	SUSE	Body
Common Criteria	"How can I be sure to get the security I need?"	• Whole system, including installation • SUSE processes • SUSE IT environment • SUSE physical environment	BSI NIAP
FIPS 140-3	"Are my crypto algorithms conforming to the standard?"	• Crypto Libraries • Random number generators	NIST
STIG	"I need a document formalizing a hardening guide!"	• Needs to look at the whole system following the questions / guidelines of the DISA	DISA
PCI DSS	"I need to manage financial data (e.g., credit cards)!"	• Affects more than the OS or software: hardware, datacenter, ...	SSC

CCN-STIC implementación segura para **SLES 15 – Nivel Alto**

Las series **CCN-STIC** son **normas, instrucciones, guías y recomendaciones** desarrolladas por el **Centro Criptológico Nacional** con el fin de mejorar el grado de ciberseguridad de las organizaciones.

Dirigidas al personal de las **Administraciones Públicas** y empresas y organizaciones de **interés estratégico**.

Sin ser imperativas*, describen las recomendaciones para que un sistema sea compatible con los requisites del **Esquema Nacional de Seguridad** (ENS)

* No son imperativas para el conjunto de las AA.PP. pero si lo son para ciertas entidades y entornos de interés estratégico

El valor para tu proyecto

¿Qué valor me puede aportar?

Usar soluciones de SUSE certificadas no tiene costes adicionales y aportan valor en múltiples escenarios

Clientes finales …

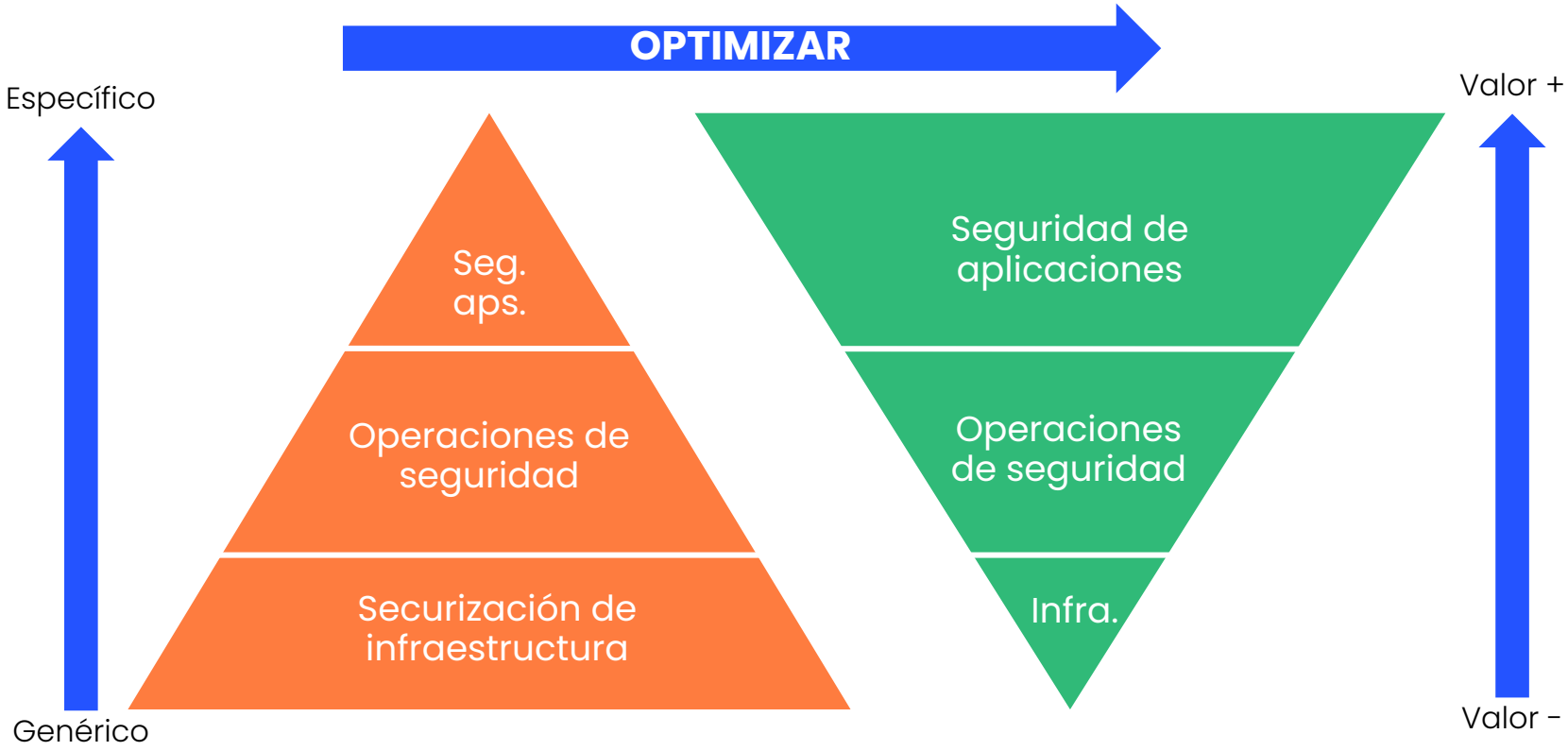
- La certificación de la cadena de suministro me libera de auditar ciertas capas de mi “stack” de TI.
- Las certificaciones STIG, CCN-STIC, me ofrecen guías probadas para la securización de mi sistema operativo. Reutilizar y adaptar.
- La automatización de las auditorías y los parcheos de seguridad (en caliente) me permite abordarlos con más frecuencia y liberar recursos.

Consultoras, ISV, desarrollos internos: usar una plataforma base certificada …

- Simplifica la certificación de los desarrollos propios (me centro en la capa que añado)
- Acceso a la documentación de cumplimiento de la certificación de cara a RFP/RFI/procesos de evaluación de software
- Desarrollo de estrategias conjuntas y certificación de productos
- Herramientas de valor añadido para crear mis soluciones

Fijar foco dónde hay más valor para mi negocio

Reducir tiempo y esfuerzo de la capa de infraestructura para dedicarlo a las capas que dan valor al negocio



Herramientas y mejores prácticas

Las soluciones de seguridad de SUSE

Developer Services

- Epinio pre-configured secure app runtimes
- Rancher Desktop with an integrated container security scanner
- SLE Base Container Images (BCI) inherits SLE security, ship containerized apps securely

security

- NeuVector: Zero-trust, full lifecycle container security platform that maintains the highest level of security and compliance + providing speed and agility for DevOps teams need.
- KUBEWARDEN: Admission control and K8s policy auditing & enforcement

RANCHER RGS (SUSE Rancher Government Solutions)

- RKE: Rancher Kubernetes Engine uses enhanced authentication & RBAC
- K3S: Enables FIPS compliance and regularly scans components for CVEs
- LONGHORN: Protects of sensitive data including PII, & financial data, & enterprise assets

HCI / VMs

- HARVESTER: Isolate VMs for an additional level of security, especially for edge use cases
- KVM: KVM uses SELinux and secure virtualization (sVirt) for enhanced VM security and isolation

SUSE Manager

- OpenSCAP: Open Security Content Automation Protocol
- CVE: Common Vulnerabilities and Exposures
- Prometheus: Keep track of security patches
- Grafana: Visualize impact of security updates

SUSE Linux Enterprise

- Security-Enhanced Linux (selinux)
- AppArmor
- eBPF: Extended Berkeley Packet Filter
- Common Criteria EAL 4+
- FIPS 140-3 Compliance
- DISA STIG guides: SLES/Rancher
- CCN-CERT Guía de implementación segura para SLES
- ...

SUSE Manager automatiza seguridad y cumplimiento

Automatización

- Simplifica la gestion de la segurida a escala mediante la aplicación automatizada de parches y configuraciones
- Integra los "frameworks" Ansible y Salt
- Escalabilidad
- Gestión de acceso securizado

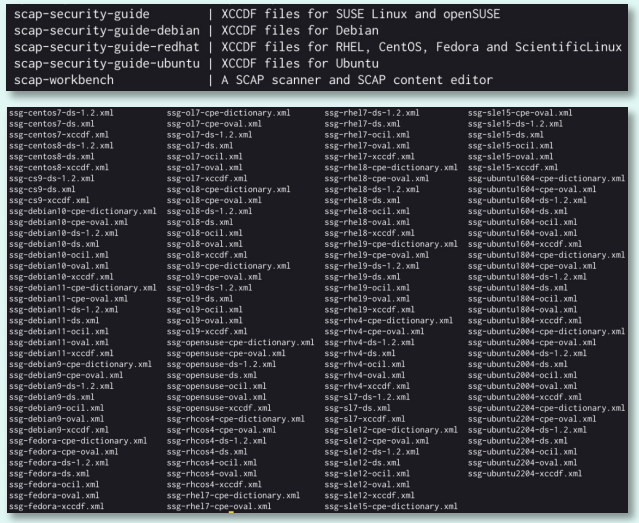
Reporte y validación

- Valida perfiles SCAP a través openSCAP
- Reportes de openSCAP
- Auditorías de CVE
- Prometheus "exporters" para métricas de seguridad
- Visualización de métricas de seguridad

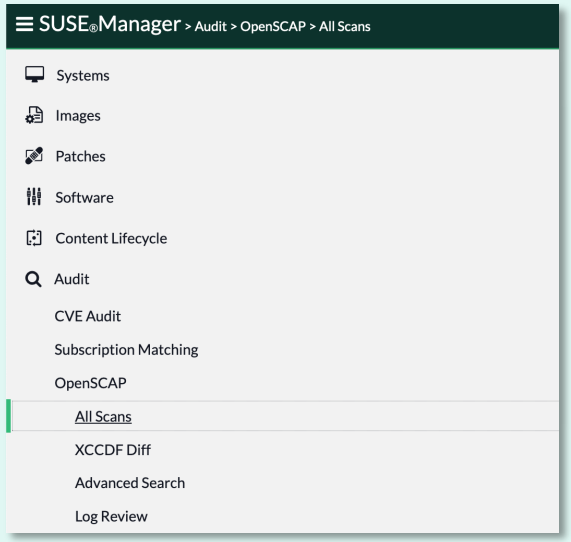
Parcheo estándar y "Live patching"

- Soporte de parcheo para todo tipo de entornos Linux
- Soporte para cadenas de actualización
- Programación y ventanas de mantenimiento
- "Live patching" para Kernel y librerías de usuario

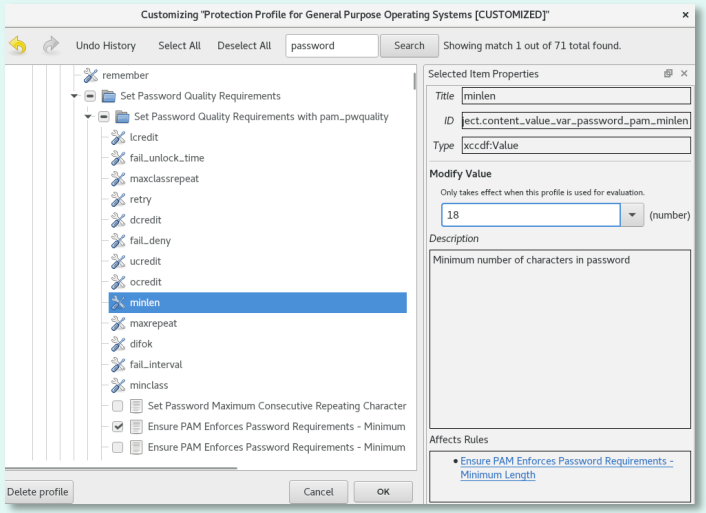
Aplicación, gestión y auditoría de perfiles SCAP



SUSE provee todos los perfiles relevantes (STIG, CIS, OVAL, ...)



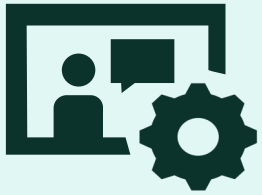
SUSE Manager: ejecuta escaneos periodicos de perfiles SCAP y automatizada las remediaciones



openSCAP Workbench permite adaptar perfiles existentes o crear nuevos

Live Patching: seguridad aplicada en el momento

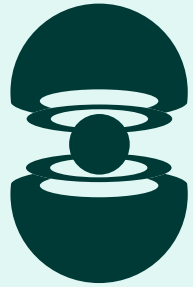
NUEVO



Actualiza tus aplicaciones sin interrupción (con SUSE toolkit)

NUEVO

Actualiza librerías clave (glibc, openSSL,...) sin perdida de servicio



Actualiza el kernel de Linux sin reinicios durante un año

Compatible con SUSE Manager

“Confidential Virtual Machines”: protección de datos

NUEVO

Data in use

Protect virtual memory & registers

Data in transit

Zero trust network encryption

Data at rest

Disk, volume & partition encryption

CONFIDENTIAL CLOUD

SUSE | AMD | Google Cloud

- Safely process sensitive data on cloud
- Protect against outside and inside attacks
- No change to workload or code

Securización de la base de Linux

SUSE Linux Enterprise

SELinux Linux Security Module

Security-Enhanced Linux (SELinux) is a security architecture for Linux that includes kernel modifications and user-space tools that allow administrators to have more granular control over who and what can access the system.

AppArmor Linux Security Module

AppArmor is an easy-to-use Linux application security solution designed to keep your Linux servers safe from malicious threats, allowing you to deploy security policy in hours, not days.

Extended Berkeley Packet Filter

Extended Berkley Packet Filter is a kernel technology that is used to safely and efficiently extend the capabilities of the kernel without requiring kernel changes.

Common Criteria EAL 4+ Certification

FIPS 140-3 Compliance

Security Technical Information Guide for SLES

Resumen

Recapitulación

SUSE ofrece una plataforma **sólida** y **probada** tanto para entornos seguros como de propósito general

Múltiples entidades independientes han **certificado** nuestros **productos** y **procesos**

Los **clientes** y **partners** pueden aprovechar ese **valor diferencial** para sus soluciones y su entorno IT

Podemos proveer **conocimiento** y **herramientas** que ayuden a implementar **entornos seguros**

SUSESEC

¡Gracias!

For more information, contact SUSE at:

+1 800 796 3700 (U.S./Canada)

+49 (0)911-740 53-0 (Worldwide)

Maxfeldstrasse 5

90409 Nuremberg

www.suse.com

SUSExchange
Innovation for decision makers