Data Sovereign Cyber Defense For The AI Era

Modernizing Cyber Defense While Maintaining Digital Sovereignty

Connecting your world.

paloalto NETWORKS

TABLE OF CONTENTS

1. Executive Summary

Europe's digital landscape is undergoing a fundamental transformation. As enterprises accelerate cloud adoption, integrate artificial intelligence, and operate increasingly interconnected digital environments, cybersecurity is no longer only a technical function – it has become a strategic pillar of business resilience and geopolitical risk management.

Geopolitical tensions and state-sponsored cyber activity are reshaping the threat landscape. Attacks increasingly target critical infrastructure, supply chains, and industrial ecosystems. In parallel, growing reliance on globally operated technology platforms introduces new risks related to jurisdiction, control, and dependency.

Regulatory developments – including NIS2, DORA, the Cyber Resilience Act, and the EU AI Act – are reinforcing this shift. These frameworks go beyond compliance, requiring organizations to demonstrate control, transparency, and resilience across their digital operations and third-party ecosystems.

Together, these forces are elevating digital sovereignty into a core priority for CISOs.

Digital sovereignty, however, extends beyond data residency. It encompasses an organization's ability to maintain control, visibility, and resilience across data, operations, technology dependencies, and legal exposure – particularly in cloud-based environments.

This creates a central challenge for CISOs: How to leverage advanced, cloud-scale cybersecurity capabilities while ensuring sovereign control over critical systems and operations?

This whitepaper introduces sovereign security as a practical framework to address this challenge, connecting:

- Geopolitical risk shaping the threat landscape
- Regulatory pressure redefining governance expectations
- Operational realities of modern cyber defense

It outlines how sovereignty must evolve from a policy concept into an operational capability, embedded in security architecture, cloud strategy, and daily cyber defense operations.

Ultimately, sovereign security is not about limiting innovation. It is about enabling organizations to operate with trusted control, reduced dependency risk, and resilience under geopolitical pressure.

Enterprises that successfully integrate sovereignty into their cybersecurity strategy will be better positioned to navigate regulatory complexity, manage external dependencies, and sustain secure operations in an increasingly uncertain global environment.

2. Sovereignty in a Shifting Cyber Landscape

Europe's digital economy is becoming increasingly dependent on cloud infrastructure, interconnected ecosystems, AI-driven operations, and real-time digital services. While this transformation has accelerated innovation and operational efficiency, it has also significantly expanded Europe's exposure to geopolitical cyber risk.

Cyber operations are no longer limited to financially motivated attacks. They are used as instruments of strategic influence, economic pressure, and operational disruption.

Several trends are driving this shift:

- **Critical sectors** such as energy, transportation, telecommunications, healthcare, manufacturing, and logistics, have become primary cyber targets due to their importance to national resilience and economic stability.
- **State-sponsored threat actors** linked to Russia, China, North Korea, and Iran continue to target European infrastructure, industrial systems, and intellectual property through espionage, ransomware, supply chain compromise, and long-term persistence campaigns[1].
- **Hybrid warfare strategies** increasingly combine cyber operations with political, economic, and information-based tactics, amplifying disruption beyond the digital domain.

At the same time, Europe's growing reliance on globally operated technology ecosystems introduces new dimensions of sovereignty risk, as many of the leading cloud and cybersecurity platforms are developed, operated, or controlled outside Europe[4].

The challenge extends beyond data residency

Organizations must assess:

- Who operates and administers the infrastructure
- Who has access to sensitive systems and data
- Where telemetry and metadata are processed
- How encryption keys are managed
- Which jurisdictions exert legal authority over service providers

This is particularly critical for organizations in regulated industries and critical infrastructure sectors, where operational continuity, data governance, and strategic autonomy are directly linked to cyber resilience.

As geopolitical tensions reshape the global technology landscape, sovereign security is evolving from a compliance requirement into a strategic resilience priority – aimed at reducing external dependencies and strengthening trusted control over critical digital environments.

[1] CERT-EU: Threat Landscape Report 2025

[2] Eurostat 2026

[3] Eurostat 2025

[4] Fortune Business Insights 2026

According to Eurostat, approximately 53% of European enterprises used paid cloud computing services in 2025[2]. Adoption of AI is also accelerating across European organizations, further increasing dependence on externally operated platforms and cloud-based processing environments[3].

3. From Compliance to Control: Europe's Cyber Regulations

Europe's regulatory environment is undergoing a significant transformation. Cybersecurity, operational resilience, data governance, and digital accountability are no longer treated as isolated compliance domains. Instead, they are increasingly aligned to strengthen the protection of critical infrastructure, reduce systemic risk, and reinforce Europe's digital sovereignty.

Expanding EU Regulatory Obligations

A growing set of European regulations now directly influences how organizations design, operate, and secure their digital environments. For organizations operating in regulated sectors, this shift creates a new operational reality. Security decisions are now shaped not only by technical requirements, but also by considerations such as jurisdictional control, operational transparency, third-party dependency management, and resilience obligations.

NIS2 Directive

The NIS2 Directive expands cybersecurity obligations across essential and important sectors within the EU. It introduces stricter requirements for governance, executive accountability, incident reporting, supply chain risk management, and operational resilience. Organizations are expected to demonstrate increased visibility into third-party providers, infrastructure dependencies, and overall cyber risk exposure.

DORA (Digital Operational Resilience Act)

DORA establishes a unified operational resilience framework for the European financial sector. It emphasizes ICT risk management, resilience testing, incident response, third-party risk oversight, and operational continuity. A key focus is the concentration risk associated with external technology and cloud service providers, requiring financial institutions to maintain stronger control over critical dependencies.

GDPR (General Data Protection Regulation)

While primarily focused on personal data protection and privacy, GDPR continues to shape how organizations manage data residency, access controls, cross-border transfers, and accountability It reinforces the necessity of maintaining clear control over who accesses sensitive data and under which jurisdiction that access occurs.

CRA (Cyber Resilience Act)

The Cyber Resilience Act introduces lifecycle-based cybersecurity requirements for products with digital components. This includes secure development, vulnerability management, patching, and product accountability. The regulation reflects a broader effort to raise baseline security across interconnected ecosystems and supply chains.

EU AI Act

The EU AI Act introduces governance requirements for the development and deployment of AI systems, particularly for high-risk use cases. As AI capabilities become more embedded in enterprise environments and cloud platforms, organizations must ensure transparency, accountability, risk oversight, and strong data governance.

National-Level Regulatory Complexity

In addition to EU-wide legislation, individual countries continue to enforce national cybersecurity frameworks and sector-specific requirements. Organizations operating across multiple jurisdictions must account for expectations from national authorities and regulators.

This creates a layered compliance landscape, requiring organizations to navigate both harmonized EU regulations and localized obligations simultaneously.

4. Sovereignty Across Europe's Critical Infrastructure

Healthcare Ecosystems

Healthcare systems are becoming increasingly interconnected through telemedicine platforms, AI-driven diagnostics, digital patient records, and distributed care networks. At the same time, they must protect highly sensitive data and operate under strict regulatory and operational accountability requirements. Sovereign cloud security helps healthcare organizations modernize infrastructure while maintaining operational control and access governance.

The European Health Data Space initiative highlights the growing importance of secure and trusted data-sharing frameworks across Europe's healthcare ecosystem[5].

Financial Services

Financial institutions are under growing pressure to modernize digital services while strengthening resilience. Real-time payments, digital banking, open finance ecosystems, and AI-driven operations are accelerating dependency on cloud infrastructure and interconnected environments.

At the same time, regulatory frameworks such as the Digital Operational Resilience Act (DORA) are significantly raising expectations around operational resilience and third-party risk management.

As a result, operational sovereignty and external key management become strategic priorities for the financial sector, enabling organizations to strengthen control over critical assets, reduce dependency risks, and support evolving regulatory and security requirements.

Public Sector

Being responsible for safeguarding citizen data, national infrastructure, and essential public services, public institutions face some of the strongest sovereignty requirements in Europe. Therefore, sovereignty is increasingly evolving from a technical consideration into a core procurement and governance requirement.

ENISA Threat Landscape 2025 continues to identify public administration as one of the sectors most frequently targeted by cyber attacks.

[5] European Health Data Space Regulation
[6] ENISA Threat Landscape 2025

5. Sovereignty as a Foundation for Secure Innovation

Europe's sovereignty strategy does not aim to limit access to global technology innovation. Large enterprises continue to depend on advanced cybersecurity platforms, AI capabilities, and hyperscale cloud infrastructure. However, there is increasing recognition that these technologies must operate within governance models aligned with European legal, operational, and resilience expectations.

Strategic Autonomy Without Isolation

Europe's approach to digital sovereignty is not centered on restricting innovation or isolating technology ecosystems. Instead, it focuses on enabling trusted digital environments where cloud adoption, artificial intelligence, cybersecurity, and data-driven innovation can scale under clear governance and operational accountability.

As digital infrastructure becomes increasingly critical to economic stability, industrial operations, public services, and national resilience, Europe is promoting frameworks designed to strengthen control, interoperability, and trust across its digital ecosystem. This shift positions sovereignty not only as a security requirement, but also as a strategic enabler of innovation.

This drives demand for operating models that combine access to leading technologies with:

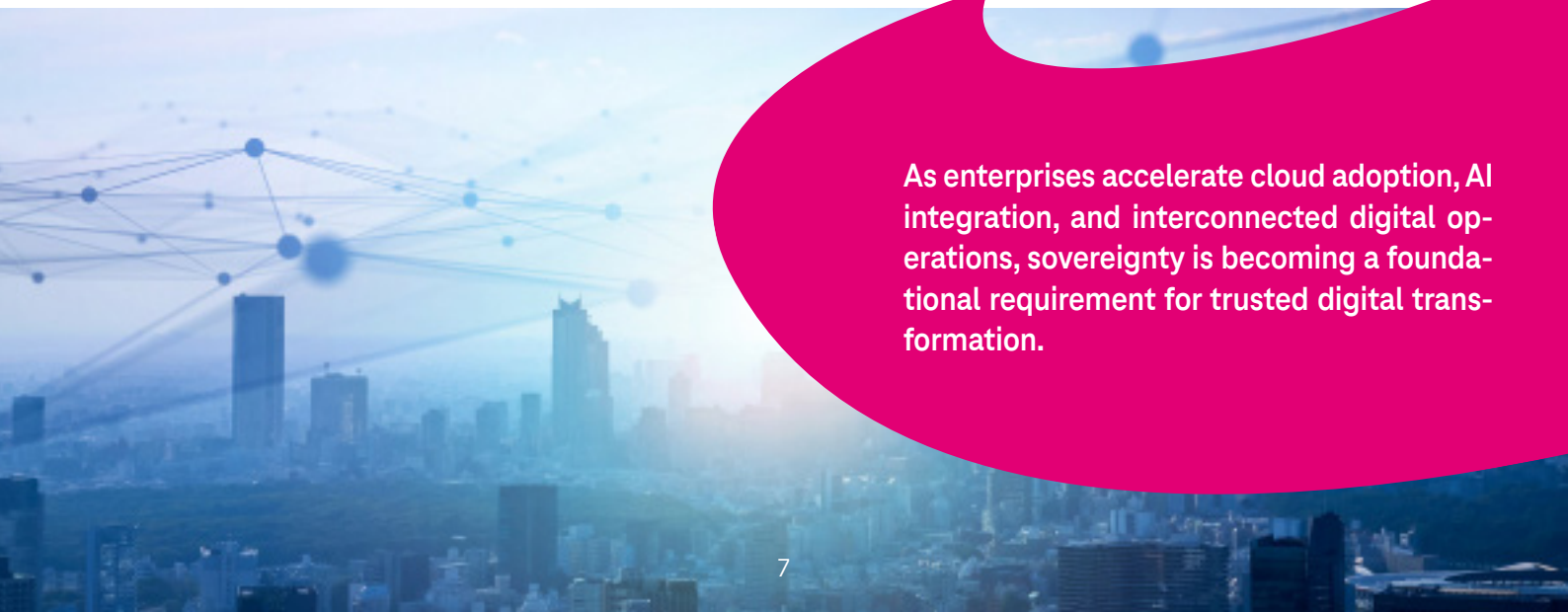
- Strong control over operational environments
- Clear jurisdictional alignment
- Transparency in service delivery and administration
- Accountability under European regulatory frameworks

In this context, sovereign security is emerging as a critical component of Europe's digital strategy, enabling organizations to strengthen resilience, maintain control, and meet regulatory expectations without limiting innovation.

Building Trusted European Digital Ecosystems

Sovereignty can not only be considered as a security requirement, but also as a strategic enabler of innovation. Several European initiatives illustrate this direction:

- **EUCS** aims to establish standardized security certification for cloud providers operating in Europe. It focuses on security assurance, transparency, and governance. Ongoing policy discussions indicate a strong emphasis on sovereignty-related criteria.
- **European Data Spaces** promotes sector-specific data-sharing ecosystems across industries such as healthcare, manufacturing, energy, mobility, and finance. It is designed to enable secure collaboration while preserving control over data ownership, access rights, and usage policies.
- **IPCEI-CIS** supports the development of European cloud and edge infrastructure capabilities. The initiative focuses on interoperability, resilience, and reducing strategic dependencies while enabling scalable innovation.
- **Schrems III** - The ongoing discussion reflects the evolution of international data transfer rules and reflects the importance of sovereign cloud and security architectures that maintain control over sensitive data and regulatory compliance.



As enterprises accelerate cloud adoption, AI integration, and interconnected digital operations, sovereignty is becoming a foundational requirement for trusted digital transformation.

6. Beyond Data Residency: The Pillars of Digital Sovereignty

Digital sovereignty has become a defining strategic priority shaping Europe's digital future. But for many organizations, sovereignty is still associated primarily with data residency. In reality, digital sovereignty extends far beyond where data is physically stored.

Digital Sovereignty in Practice

Digital sovereignty refers to an organization's ability to maintain meaningful control over its digital environment, including infrastructure, data, operations, and critical technology dependencies[7].

It encompasses operational control, governance transparency, infrastructure dependency, jurisdictional exposure, supply chain trust, and the ability to maintain resilience under changing geopolitical conditions.

Four key dimensions of digital sovereignty are:

- **Data Sovereignty**: Control over data access, usage, and governance, including who can access data and under which jurisdiction.
- **Operational Sovereignty**: Control over critical infrastructure and operational processes, ensuring continuity and resilience even under external disruption.
- **Technological Sovereignty**: The ability to manage dependencies on key technologies, ensuring flexibility, interoperability, and reduced reliance on single providers or external ecosystems.
- **Legal Sovereignty**: The ability to ensure systems and data are governed by predictable jurisdictional frameworks, minimizing exposure to conflicting or extraterritorial legal claims.

[7] Forbes 2026

Digital sovereignty is not about complete independence. Modern enterprises operate within global ecosystems of cloud providers, software vendors, and service partners. The objective is to ensure trusted control and transparency across these interconnected environments.

In practice, this requires visibility into:

- Who operates and administers the environment
- Which jurisdictions influence operational control
- How privileged access is governed
- Where data and telemetry are processed
- How encryption and identity are managed
- Which external dependencies are critical to operations

Balancing Sovereignty and Innovation

Digital sovereignty is often perceived as a trade-off between control and innovation. In practice, organizations can balance both objectives through operating models that combine advanced cyber defense capabilities with strong governance, transparency, and accountability.

The required level of sovereignty depends on factors such as:

- Regulatory obligations
- Critical infrastructure exposure
- Risk profile and threat landscape
- Data sensitivity
- Third-party dependencies

6. Beyond Data Residency: The Pillars of Digital Sovereignty

Data Sovereignty: Access, Location & Control

Data sovereignty is frequently reduced to data residency, but the two are not interchangeable. While data residency defines where data is stored, data sovereignty defines who can access that data, under which jurisdiction, and with what level of control.

This distinction is critical in distributed cloud environments, where data may be stored in Europe while administrative access, support operations, or key management are governed externally.

Key considerations include:

- Privileged access control
- Jurisdiction governing access requests
- Legal exposure to external authorities
- Location of telemetry and metadata processing
- Control over encryption and key management

Encryption as a Sovereignty Control

Encryption is a key mechanism for strengthening sovereignty. Models such as customer-managed or external key management allow organizations to retain independent control over data access. For regulated sectors, encryption governance is not only a security requirement but also a key sovereignty safeguard.

Data Classification and Tiering

Not all data requires the same level of control. Organizations are adopting classification models that align sovereignty requirements with:

- Sensitivity and business criticality
- Regulatory exposure
- Operational impact

This enables a balanced approach, maintaining innovation and scalability while applying stricter controls where necessary.

Data Sovereignty: The ability to exercise complete control over one's own data. Without it, you lose the power to decide who can access your data and how it can be used.

Operational Sovereignty: Control & Resilience

As digital operations become more interconnected, organizations must assess not only which technologies they use, but also who operates them and where dependencies exist.

Modern security operations often rely on globally distributed cloud ecosystems for detection, response, and analytics. While these models enable scale and advanced capabilities, they can introduce dependencies tied to external jurisdictions and operating models.

These aspects should be evaluated:

- Who operates security environments
- Where telemetry is processed
- Who has operational access
- How incident response authority is defined
- Whether operations can continue during provider outages or geopolitical disruption

Operating Models for Sovereign Security Operations

Organizations adopt different models depending on risk and regulatory requirements:

- In-house SOCs for maximum control and visibility
- European MSSPs for regional governance and operational alignment
- Hyperscale-integrated models for scalability, requiring careful management of dependency and jurisdictional risk

Operational Sovereignty: The ability to independently control and maintain critical infrastructure and operations. Without it, you risk losing control of key business processes and become vulnerable to external disruptions.

6. Beyond Data Residency: The Pillars of Digital Sovereignty

Technological Sovereignty: Managing Dependency Risk

Enterprise environments are increasingly dependent on a small number of global technology providers. While these platforms deliver scale and advanced capabilities, they can introduce concentration risk and reduced flexibility.

Key challenges include:
- Vendor lock-in
- Limited interoperability
- Dependency on proprietary ecosystems
- Exposure to external governance

Multi-Cloud and Hybrid Strategies

Many organizations adopt multi-cloud and hybrid architectures to improve flexibility and reduce dependency.

These approaches support:
- Workload portability
- Improved interoperability
- Flexible governance models
- Segmentation based on risk and sensitivity
- Reduced concentration risk

Complete independence is not realistic. Technological sovereignty is therefore best understood as a resilience strategy, focused on reducing unmanaged dependencies and increasing adaptability.

Technological sovereignty: The ability to develop, produce and control key technologies independently. Without it, there is a strong dependence on other countries or companies for critical technological solutions, which limits one's own ability to act and competitiveness.

Legal Sovereignty: Understanding Jurisdictional Exposure

Legal sovereignty addresses which jurisdictions govern digital environments and who can exert legal authority over systems and data.

This includes assessing:
- Provider jurisdiction and ownership structure
- Exposure to extraterritorial legislation
- Legal mechanisms for data access requests
- Transparency and enforceability of governance models

Data Location Alone Is Not Sufficient

Storing data in European data centers does not eliminate legal exposure.

Risks can still arise from:
- Foreign ownership of service providers
- Cross-border operations and support models
- International legal cooperation mechanisms
- Extraterritorial legal obligations

Organizations must therefore assess both infrastructure location and the legal frameworks governing service providers. The objective is to reduce uncertainty, strengthen accountability, and align operations with European legal and regulatory expectations.

Legal sovereignty: The ability to ensure that your data, systems, and operations are exclusively subject to the laws and jurisdictions you choose.

7. Operationalizing Sovereign Cyber Defense in Practice

Many existing sovereignty approaches were designed for traditional IT environments – focused on data residency and localized infrastructure – rather than for modern, AI-enabled cyber defense operating at cloud scale. As a result, organizations often perceive a trade-off between advanced security capabilities and maintaining sovereign control.

The next phase of sovereign cyber defense

Organizations across Europe face increasing pressure to modernize cyber defense capabilities while strengthening operational governance and sovereignty controls. This is particularly evident in regulated sectors and critical infrastructure environments.

Organizations require advanced threat detection, automated response, large-scale telemetry analysis, and real-time visibility, while simultaneously ensuring accountability within European governance and jurisdictional frameworks.

The next phase of sovereign cyber defense therefore extends beyond infrastructure location. It requires operating models that embed enforceable sovereignty controls directly into security operations – without limiting capability, scalability, or resilience.

Embedding Enforceable Sovereignty into Security Operations

Sovereignty cannot rely solely on policy, contractual assurances, or data location. It must be technically and operationally enforced across the environments where cyber defense activities take place.

Key capabilities include:

- Controlled and auditable operational access
- Transparent governance and accountability frameworks
- Clearly defined operational responsibilities
- Independent or customer-controlled encryption models
- End-to-end auditability across security workflows
- Operational execution aligned with trusted jurisdictional frameworks

In practice, organizations increasingly require assurance that these controls are consistently applied across daily activities, including:

- Threat monitoring and detection
- Incident response and escalation
- Platform administration
- Security operations management (internal or outsourced)

This is particularly critical in AI-assisted cyber defense environments. Large-scale telemetry processing, automated analytics, and distributed response models introduce additional layers of complexity around governance, access control, and operational transparency.

Sustaining Operational Sovereignty

Sovereignty is not a one-time deployment. Regulations evolve continuously and threat environments change rapidly. Operational governance models therefore need continuous review and adaptation, making an ongoing audit readiness, governance validation, operational transparency, and threat intelligence alignment necessary.

8. Sovereign Cortex with T Security

Organizations pursuing sovereign cyber defense are not simply selecting a security vendor. They are deciding how cyber defense will be governed, operated, and held accountable across complex regulated environments. This is where the partnership between Palo Alto Networks and Deutsche Telekom becomes critical, delivering a combined sovereign cyber defense operating model with the data sovereignty required to deliver it within auditable and enforceable frameworks.

Full-strength AI-driven cyber defense

Palo Alto Networks delivers AI-driven cyber defense across cloud, network, endpoint, and security operations. This is not a reduced-capability sovereign variant. It is the same platform that serves 70,000+ customers across more than 150 countries, analyzes 1.4 billion threat objects daily, and is recognized by Gartner and For-rester for leadership across multiple security domains. Unit 42 threat intelligence and Palo Alto Networks security operations capabilities provide continuous insight into the evolving threat landscape, while Deutsche Telekom delivers sovereign operatio-nal expertise and managed security execution within governed European environments. Within the sovereign operating model, organizations retain access to full-strength cyber defense capa-bility within clearly governed sovereign controls.

Operationally enforceable data sovereignty

Deutsche Telekom provides the sovereign operational layer that makes this model enforceable. This includes EU-only operational personnel access, Deutsche Telekom-controlled encryption key management, audit logging and operational transparency, and Frankfurt-based processing and storage. Sovereign operations are delivered through Deutsche Telekom, ensuring that data so-vereignty is operational, not just contractual. Sovereignty is enfor-ced across people, process, and technology, ensuring operational governance extends beyond infrastructure controls alone.

Built for governed execution, not just governed architecture.

- Operational controls that enforce data sovereignty in execution
- EU-only operational personnel.
- DT-controlled encryption.
- Audit logging and transparency.
- EU-based (Frankfurt-based) processing.
- 24x7 managed security operations.

Governable and accountable AI security operations

As AI becomes embedded in cyber defense operations, governance becomes a strategic requirement. The partnership addresses this directly, ensuring that AI-driven operations remain accountable, explainable, and governed within sovereign controls. This is a strategic space that neither infrastructure-led sovereignty providers nor capability-led cyber defense vendors credibly occupy on their own.

A sovereign cyber defense operating model

This is not a technology deployment layered with compliance controls. It is a purpose-built operating model where cyber defense, sovereignty, AI governance, and operational accountability are integrated from the outset. Organizations get the operating model, not just the tools, including defined operational controls, escalation models, shared responsibility frameworks, and 24x7 managed security operations. Organizations benefit from a single accountable operating model spanning cyber defense capability, sovereign governance, managed operations, and AI-driven security outcomes.

Sovereignty where it matters, across environments

Deutsche Telekom enables organizations to operate cyber defense through a consistent sovereign framework designed to support regulatory requirements across European environments. This includes maintaining control over data residency, operational access, and regulatory compliance. Through its sovereign operational capabilities, organizations can maintain clear control over where data is processed, who can access it, and how operations are governed, ensuring sovereignty is enforceable across jurisdictions without defaulting to maximum control at maximum cost.

9. The Way Forward

In a rapidly changing global landscape, organizations that can combine advanced cybersecurity capabilities with trusted control over their digital environments will be best positioned to operate securely, compliantly, and resiliently. Organizations should treat sovereignty as a core design principle, not an afterthought, prioritize operational enforcement over policy definition and balance innovation and sovereignty through governance models that maintain both capability and control.

About Palo Alto Networks

Palo Alto Networks (NASDAQ: PANW), the global AI cybersecurity leader, protects our digital way of life with a comprehensive portfolio of cybersecurity solutions and platforms across Network, Cloud, Security Operations, AI and Identity. Trusted by 70,000+ customers and powered by Unit 42 threat intelligence. www.paloaltonetworks.com

About Deutsche Telekom

Deutsche Telekom is Europe's leading digital telco company, serving around 220 million customers across mobile, fixed-network and IT services. Through its subsidiaries Deutsche Telekom Security and T-Systems, the Group is also one of Europe's largest providers of cybersecurity and managed security services. With Security Operations Centers across Europe, an end-to-end European network and IT infrastructure, and decades of experience serving regulated industries and public-sector customers, Deutsche Telekom provides the European trust anchor for sovereign digital services. www.telekom.com/companyprofile

Get in touch with us today!

Publisher
Deutsche Telekom AG
Friedrich-Ebert-Allee 140
53113 Bonn
www.telekom.de

Connecting your world.

paloalto NETWORKS