ANALYST CONNECTION

Sponsored by: Cisco

Air-gapped sovereign critical infrastructure isolates systems operationally and physically for resilience against geopolitical threats. Implementation requires trusted supply chains, disconnected-capable hardware, minimal critical workloads, and long-term vendor road maps that support offline evolution.

Approaching Air-Gapped Environments for Sovereign Critical Infrastructure in EMEA

July 2026

Questions posed by: Cisco

Answers by: Andrew Buss, Senior Research Director; Luis Fernandes, Senior Research Manager

---

Q. What are air-gapped environments for sovereign infrastructure, and why is this topic particularly important for EMEA customers?

A. Air-gapped sovereign infrastructure refers to an architectural approach for building and running IT systems that are completely self-contained and physically and operationally isolated from external networks and outside control. An air-gapped sovereign architecture puts the IT system and data under the operational control of a single sovereign entity with no outside dependencies. It also means that the management and operations of the infrastructure do not depend on connecting to any external control plane functionality to continue functioning as expected.

In practice, this means that any hardware, once purchased and set up within such environment, will not depend on product activation validated externally to function.

This allows the infrastructure to be operationally resilient in the face of a major incident including withdrawal of vendor support or nation-state attacks, all of which can impact operations and resilience. An air-gapped architecture, by being self-contained, is significantly more isolated and operationally resilient.

Organizations looking to implement air-gapped sovereign architectures are organizations with strict regulatory, compliance, or critical national infrastructure requirements. Typically, these would be governments, defense, healthcare, utilities, and financial services.

Q. How can air-gapped sovereign critical infrastructure solutions protect critical systems and data as well as intellectual property from external parties?

A. The cyberthreat landscape is rapidly evolving and very sophisticated. It often has significant funding and nation-state support that enables research and development into new attack vectors. Recent GenAI solutions have expanded and accelerated the range of attacks. Many established organizations across EMEA have fallen victim to attacks including automotive and retail organizations.

Air-gapped systems by their very nature are isolated from external networks or third-party control. Data transfers between an air-gapped infrastructure and other systems are typically through physical data media, which are offline and can be scanned independently before being accepted onto the air-gapped systems. This greatly reduces the opportunity for threat actors to gain access to systems and data on the air-gapped infrastructure.

In addition, if any threats are inadvertently introduced to the air-gapped systems, there is no easy route to exfiltrate any data that could compromise confidential information or intellectual property.

The air-gapped sovereign infrastructure is also operationally inaccessible by foreign vendors, providing protection against the compelled disclosure of data by vendors pursuant to third-country legal process. It also means the operation of critical systems is entirely within the control of the organization, even if it is no longer possible to engage in business dealings with the vendor.

Q. Many companies in EMEA have a hybrid approach to IT infrastructure. How can air-gapped architectures for critical infrastructure be implemented within hybrid approaches?

A. IDC's EMEA digital infrastructure research shows that four in five organizations, including government, make use of public cloud alongside private IT infrastructure for many reasons, including scale, cost, performance, and convenience.

IDC's 2025 *Worldwide Digital Sovereignty Survey* shows that most companies consider sovereignty a part of their multicloud and hybrid cloud strategy. About 37% of them use on-premises infrastructure, and sovereign cloud is the only type of cloud they will use.

When talking about highly or medium-sensitive data, 29% of the surveyed organizations said they will only use a local provider as their public cloud vendor, whereas 14% said they prefer on-premises. These customers are most likely to consider air-gapped sovereign critical infrastructure solutions.

In EMEA, particularly in the European Union (EU), there is a strong culture of data privacy and security. The EU has led the way in codifying this with the General Data Protection Regulations (GDPR) and Data Act. As a result, many organizations, even if using public cloud, are looking to introduce more control over their application and data deployments. Interest in digital sovereignty, including sovereign cloud solutions, has also grown strongly.

Digital sovereignty is not a one-size-fits-all approach. It depends on the overall context, including the sensitivity of the data and systems, technological solutions, and overall cost. For most workloads, even within organizations that have some of the strictest requirements and regulations, deploying them to an air-gapped sovereign infrastructure would be cost- and operationally prohibitive. Therefore, these workloads would typically be deployed to standard private IT infrastructure or public cloud with suitable security, operational, or sovereignty controls in place dependent on their level of sensitivity.

The subset of truly critical systems and data would be deployed to an air-gapped sovereign critical infrastructure, but because of the costs and operational complexity, this should be kept to the relevant set of workloads. It is important to recognize that being air-gapped means there is no direct interconnect between air-gapped and non-air-gapped systems.

Q. What is the best way to think about specifying requirements for air-gapped sovereign critical infrastructure and implementing the solution?

A. As mentioned earlier, there no one-size-fits-all approach; it depends on the context of the systems and data and the applicable requirements and regulations. Applying IDC's Digital Sovereignty framework, air-gapped sovereign critical infrastructure largely fits within the hardware, infrastructure operations, and data management spheres, with a high requirement on security and privacy, standards and interoperability, and risk management.

Air-gapped sovereign critical infrastructure should therefore be the right venue for the right workload. Organizations mentioned that the top 5 workloads they have or expect to migrate to sovereign environments are data management, backup/recovery, back-end business apps, storage, and app development.

There are several challenges with designing and implementing an air-gapped sovereign critical infrastructure solution. One is that for many years, infrastructure hardware and software have been designed to be constantly cloud-connected and -enabled, even for routine ongoing operations. Disconnecting from these cloud control planes disrupts the functionality of the systems. Vendors wishing to move some workloads to an air-gapped environment have to adjust the capabilities to function fully while completely disconnected from outside networks. This should include a commercial construct for subscription-based licensing operating in a trust-based manner.

Last, but not least, physical IT infrastructure hardware is often manufactured in locations that are in geopolitically sensitive regions. There is a possibility that equipment that contains rogue code or functionalities that could disrupt operations over time could be installed within the air-gapped sovereign critical infrastructure. For this reason, it is important to consider vendors with strict trusted supply chain controls that are effectively monitored and enforced.

Infrastructure is also composed of multiple components from a variety of vendors across compute, storage, networking and security. Therefore, it is vital to consider their full-stack ecosystem, capabilities, certifications, and road maps to ensure they meet the needs of the solution.

Q. How can air-gapped sovereign critical infrastructure solutions evolve to match changes in future operating models?

A. Ideally, for ease of evolution and modernization over time, the overall hardware and software offerings used in air-gapped sovereign critical infrastructure solutions should be the same as, or very close to, those used in connected infrastructure but with the capability of being deployed in an air-gapped manner. This could take the form of derivative versions of common products rather than being very bespoke hardware and software. This would leverage economies of scale and allow the evolution of the capabilities on offer. A key element, however, is the enhanced longevity of products in the market, strict compliance, and certification processes will limit the models that would be allowed to be used to maintain, expand, or transform the infrastructure.

In operation, once fully functioning and stable, air-gapped sovereign critical infrastructure should not require regular patches or updates over the short to medium term. Only if a severe reliability issue or a new functional requirement emerged would significant updates be required to be deployed. These should be made available from the trusted suppliers in a secure offline manner that can be tested and validated and then deployed using offline media.

For the longer-term evolution of air-gapped architectures, manufacturers need to develop and present to customers, under a nondisclosure agreement (NDA) if necessary, their long-term multigeneration road maps for equipment designed expressly for secure, air-gapped infrastructure deployments.

Additionally, manufacturers should provide the expertise to support users in their deployment of air-gapped sovereign critical infrastructure environments given their higher complexity, higher costs, potential integration issues, and typically lack of internal know-how and skills.

About the Analysts

Andrew Buss, *Senior Research Director*

Andrew Buss is senior research director within IDC's enterprise infrastructure global research domain. He covers datacenter infrastructure and facilities services as part of the digital and datacenter infrastructure strategies subdomain. His research focuses on datacenter facilities owned and operated by SPs, hyperscalers, and enterprises.

Luis Fernandes, *Senior Research Manager*

Luis Fernandes is a senior research manager within IDC's enterprise infrastructure global research domain. He covers datacenter infrastructure services as part of the digital and datacenter infrastructure strategies subdomain. Luis develops research that spans from edge to core to cloud, looking at trends and strategy shifts on how companies buy, build, and run their digital infrastructure.

MESSAGE FROM THE SPONSOR

From Customer Needs to Delivery

Cisco customers in EMEA want control over their digital infrastructure and data while enjoying the freedom to choose the right deployment models for their operations, security postures, and strategic goals. As such, one customer's sovereign architecture might look completely different from the next. What is important is to give organizations a greater choice about how they control their data. The arrival of AI makes the combination of choice and control even more essential, making sure digital sovereignty does not become the brake on EMEA's AI innovation.

To gain a deeper insight on how Cisco is building sovereignty around customer choice, read "Cisco Sovereign Critical Infrastructure: From Customer Needs to Delivery."

IDC Custom Solutions

IDC Research, Inc.
One Beacon Street
Suite 33100
Boston, MA 02108, USA
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com