Security
at the Speed of Trust –

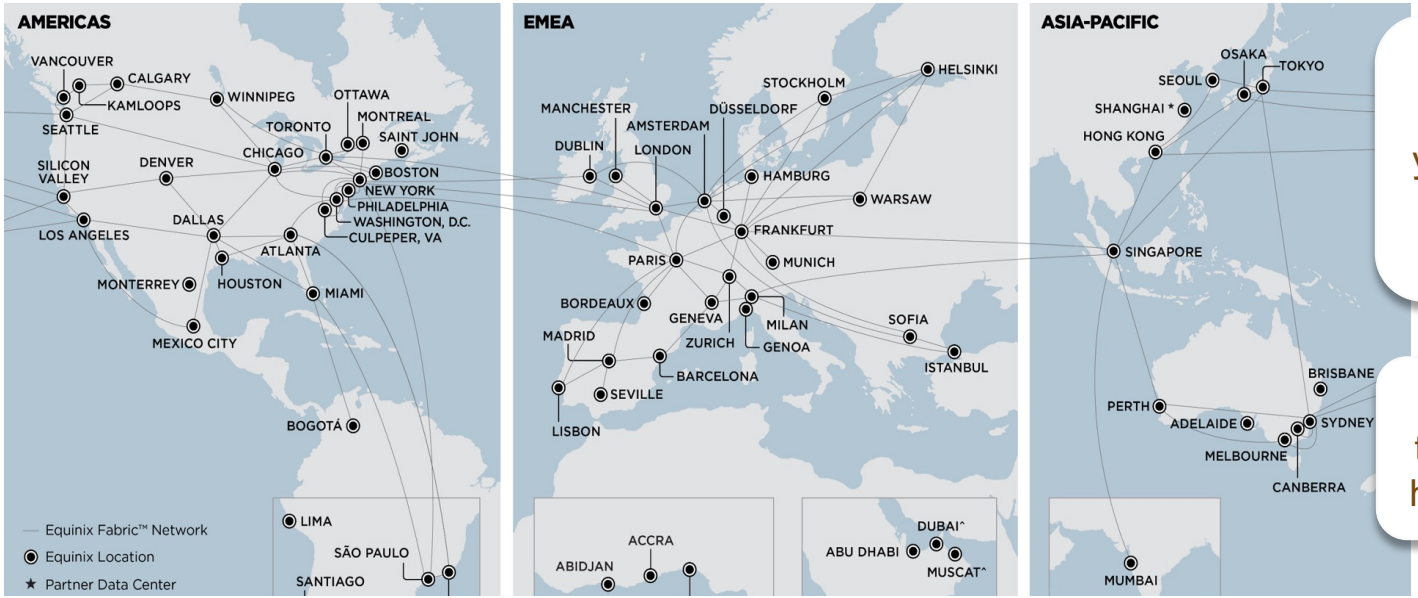
CREATING A SECURITY-AS-CODE MODEL

Equinix Infosec Team

CSO50 | EQUINIX

PRODUCED BY CSO

The Equinix Evolution



Equinix was established over 25 years ago as a *hub* for network traffic and digital commerce.

This was before the term "*digital business*" had even been coined.

Equinix operates **240+** data centers in **71** major metros as a **neutral venue** that brings together over **1,800** networks worldwide to collaborate and exchange.

Security-as-Code: Getting Started

In July 2020, Equinix began a project to modernize its security approach, focusing on **automating security controls**. The project started with an **assumed breach posture**.

To establish a strong foundation, we constructed a **security data lake** for **centralization** of data and information.

Then, we shifted our approach to problem-solving and adopted a **Security-as-Code Model**, allowing us to automate our controls and operations.

Goals / Business Value

Minimize alert fatigue

Standardize workflows by provisioning immutable infrastructure

Approach security with principles of intelligence-led, zero-trust, and automation

Prioritize the most crucial aspects to develop countermeasures quickly

Continually enforce policy to maintain visibility at scale

Reduce operational risks

Security-as-Code: Primary Drivers

Industry Challenges

Security teams often face several challenges:

- Policy implementation
- Technical debt
- Risk misalignment

Meanwhile, threat actors operate in a dynamic environment that incentivizes the development of new capabilities at a comparatively low cost.

Digital Transformation

Equinix has grown significantly for over 25 years, primarily due to global digital transformation. Our clients are adopting new business models, innovations, and digital leadership expectations; in support, we are constantly expanding our technology portfolio and enhancing our security measures to counteract emerging cyber threats.

Security as a Key to Digital Transformation

Five key areas of focus for our investments across the enterprise:

Enable governance, risk, and compliance	by deploying automated and continuous compliance focused on common controls
Advance product and data center security	by putting product security controls in place throughout the development lifecycle with 24×7 continuous security monitoring
Enhance threat and vulnerability management	by expanding the visibility of vulnerabilities across source code, code development, network assets, and operations technology
Leverage security intelligence and machine learning	within security tooling to enable continuous automation of protection, detection, and response capabilities
Accelerate global incident response and threat hunting	by proactively hunting for attack indicators and readying a formal response team to remediate any material breach

Security-as-Code: How We Built It

Our Mission

Create a cohesive and comprehensive security platform that **integrates** all aspects of our current and emerging business model and **delivers** frictionless and seamless experiences for our employees and customers via a single security platform that provides end-to-end automation.

Data-as-Code

We created a scalable data lake powered by Google Chronicle and data management scaled via Cribl. This enables us to ingest logs from all security systems and infrastructure platforms into one unified data model.

GRC-as-Code

We built a singular GRC platform that provides Automated Regulatory Compliance, advanced workflow automation, enhanced reporting, and dashboard functionality – all within the ServiceNow Integrated Risk Management (IRM) platform supported by FAIR-based risk quantification.

Infrastructure-as-Code

We continue to expand on the Security-as-Code model by importing our security stack into HashiCorp Terraform to provide an immutable infrastructure that runs on code, reducing complexity and user misconfigurations while enabling teams to do more with less.

Results

50% cost savings by Automated Regulatory Compliance

Repurposed **six** analysts for threat hunting activities

Ticket Reduction : **20k** to **7.5k**/quarter

15 min avg ticket closure

Enriched **90%** of detections through Threat Intelligence

Provided self-service curated statements

Built **180** authority documents, **11,874** citations, and **276** integrated requirements

Automated prevention of – **70%** of events before they become incidents

3k manhours saved/quarter

45-60% reduced time on assessments

Equinix Security Trust and Transparency (ESTT): Supported **3,000+** audits and fielded **100,000+** questions

Key Takeaways

Connect all your security capabilities and deliverables "as code" by:

- Approaching security with principles of automation and application of security intelligence
- Using data-driven decisions to assist in identifying and mitigating risks
- Empower your teams with a common platform: Risk Management, Policy & Standards, Engineering, and Security Operations & Support operating within a unified security data lake
- Automating security scans and testing within code pipelines
- Establishing a continuous feedback loop that provides security findings to developers
- Embedding security controls as gates within the Software Development Lifecycle (SDLC)
- Implementing a continuous monitoring strategy to automatically highlight issues

Team Recognition