IoTIntelligence™ REPORTS

Powered by: Valuer

IoT Community

Cloud-Native Applications

Areas of Innovation Included:

Distributed Computing

API Security

Cloud Infrastructure

Secure Access Service Edge (SASE)

Data Security Management

Table of Contents:

Distributed Computing

Distributed computing refers to a distributed computer system that comprises software components located on multiple computers connected by a local or wide area network. Run as a single system, despite being spread out, this model is crucial for improving the efficiency and performance of the whole distributed system, sharing data, and coordinating processing power more efficiently. Additionally, it offers advantages in terms of scalability, resilience, and cost-effectiveness.

Distributed systems can consist of a multitude of possible configurations, such as personal computers, mainframes, minicomputers, and workstations, among others. Essentially, this model aims to enable the network to function as a single computer.

From the Valuer platform:

Average year of founding of the Distributed Computing companies:

2014

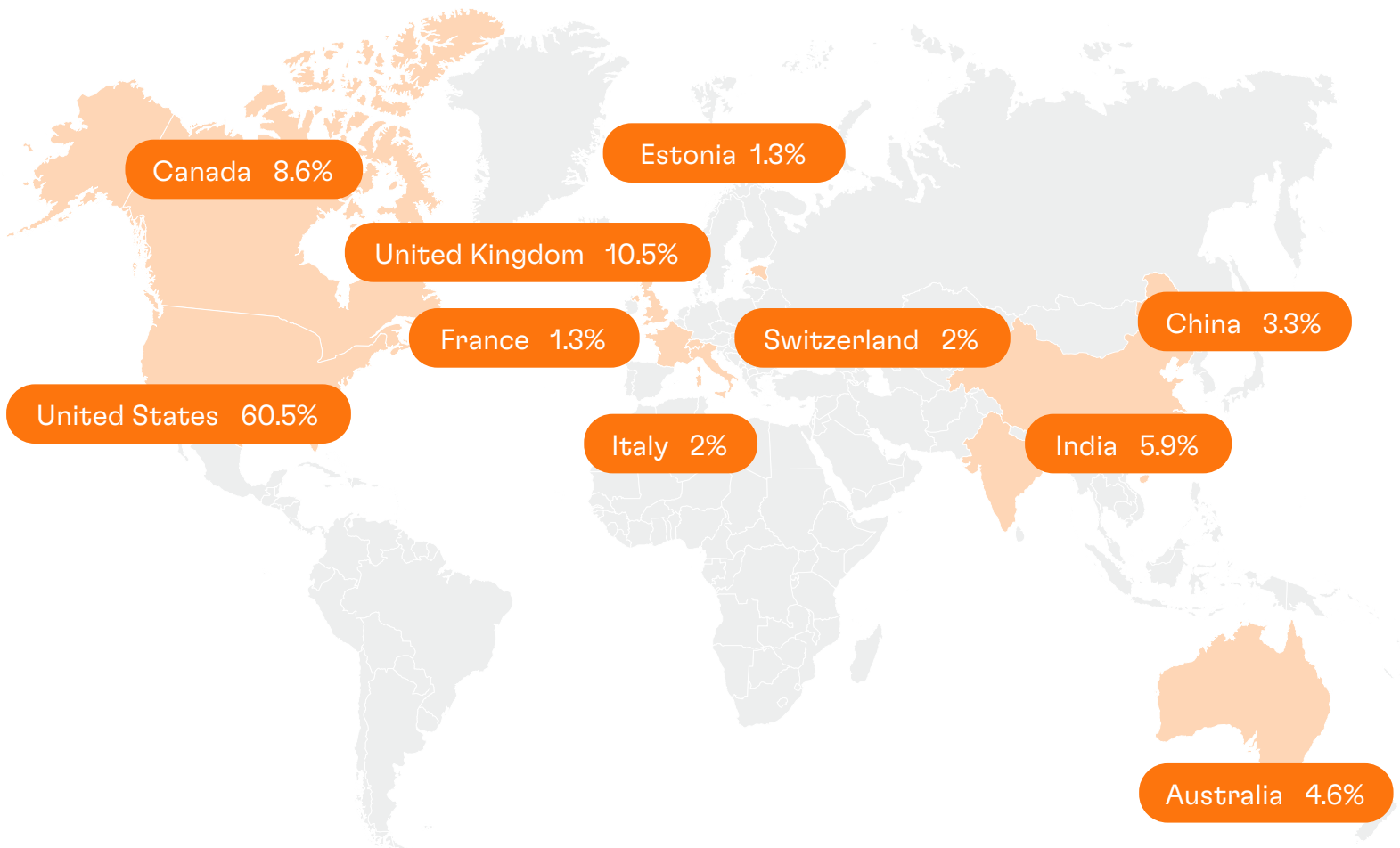
Average funding of the Distributed Computing companies:

$21,748,586

Maximum funding of the Distributed Computing companies:

$280,832,709

10 countries with the most Distributed Computing companies on the Valuer platform:



Company Highlight:

Synadia

Corporate Gold Member of the IoT Community

Year of inception:
2017

Location:
Los Angeles, CA, United States

Company stage:
Growth/Expansion

Funding:
16,100,000 USD

Team size:
25

Website:
synadia.com

Synadia provides a cloud messaging and data streaming platform aimed at enabling the next generation of connected digital experiences. The company is behind the open source project NATS.io, used by millions of developers globally. The technology serves as a connective fabric for modern distributed systems, allowing users to build edge applications with enhanced security, latency, and scalability.

The company was founded in 2017 by Derek Collison, an experienced entrepreneur and technologist with a vast experience in cloud computing and distributed systems. Synadia operates from its headquarters in Los Angeles (CA), with a team encompassing 25 members.

Customers:

Form3 Mastercard SUSE

Business Model

The company's business model is centered around the following characteristics:

- Synadia is a B2B company offering enterprises a modern connectivity platform that simplifies the development of distributed applications for true multi-cloud and edge deployments.
- The company works with large global Fortune 100 enterprises modernizing their digital infrastructure and small innovative startups building global data platforms. Its products cater to customers in financial services, retail, industrial/manufacturing, and energy sectors.
- Synadia offers customers an Enterprise NATS subscription for on-premise deployment, in their private cloud, or on a hybrid basis. It also manages a decentralized global SaaS utility for customers on a self-service basis.
- The company generates revenue on a monthly and annual subscription basis.

Value Proposition

The company communicates the following as its main value propositions:

- Synadia significantly simplifies the development and deployment of applications for the edge by leveraging a single platform technology that scales from a single server to cluster to global superclusters deployments.
- Operational cost reduction is another featured benefit, enabled by supporting multiple application design patterns, including microservices request-reply, key-value, and data streaming use-cases with zero-trust security and multi-tenancy built in.
- The offerings do not require cloud lock-in. Moreover, they enable transparent true multi-cloud deployments across any geography either on a self-managed basis or via NGS, a self-service global utility managed by Synadia.
- Synadia's work is supported by eminent VCs and strategic investors, including Accenture Ventures, True Ventures, and Bold Ventures.

Product Portfolio 1/2

Synadia's portfolio encompasses two main offerings - NGS and NATS Enterprise subscriptions.

NGS

NGS is a global multi-cloud, multi-geo, and extensible cloud service managed by Synadia, comprising a global communications utility for all digital systems, services, and devices. Built on NATS technology, the system is globally available under a single URL, secure by default, and enables secure and easy data sharing between communication domains.

The offering allows users to build and deploy distributed applications to a global customer base, empowered by security and encryption mechanisms.

NGS is currently deployed across all major public clouds and geographies to provide low latency response times globally that address the needs of real-time businesses. The solution does not require configuring firewalls, load balancers, or specific cloud infrastructure and can support data privacy and GDPR compliance via specialized features like tagging. Customers can easily extend NGS to 3rd party locations by adding a NATS LeafNode. NGS can also be extended to private datacenters, satellites, autos, plant floor locations, oil rigs, windmills, and medical mannequins.

NATS Enterprise Subscription

As a connective technology, NATS supports distributed systems' operation by managing the common patterns within them, such as message exchange, stream processing, and statement processing. The software can be deployed on a single server, clusters cloud, edge, and IoT devices, performing well with and without requiring third-party deployment frameworks. Common use-cases include cloud messaging, control and command, data streaming, and more.

NATS' main advantage is that it entails Adaptive Edge Architecture that allows users to combine edge, devices, cloud, and hybrid deployments, empowered by multi-tenancy that ensures faster time to value. The technology can process millions of messages a second per server, thus delivering cost efficiency and significantly reduced compute and network usage for streams, services, and eventing. Moreover, it can self-heal and scale up and down, alongside its ability to sustain topology changes with zero downtime.

Powered by NGS and NATS.io, Synadia's offering extends to:

1. Multicloud functionality with complete portability that allows users to switch workloads between clouds or load balance across clouds in milliseconds;
2. Intelligent edge for performing asynchronous and autonomous edge processing with observability from cloud to edge at a lower edge latency and network costs;

3. Stream processing tool conducting changes to client topologies, schemas, and APIs without rebooting processing stream and event data;
4. Microservices that accommodate cloud-native operations as an alternative to server-based applications, enabling enhanced throughput and performance with greater cost efficiency;
5. Access to intelligent data that automatically persist responses for common queries in a distributed key-value store;
6. Solutions that ensure high-security, multi-tenancy performance for internal SaaS applications that support deployments of zero trust infrastructure with minimal maintenance;
7. Automated deployment, scaling, and management of containerized applications enabled by Kubernetes.

Market Opportunities

The company is operating in the global event stream processing market.

- According to Markets and Markets, this market is poised to reach $1.83 billion by 2023, growing from an estimated $690 million in 2018.
- Registering a CAGR of 21.6% in the forecast period, the market is anticipated to remain lucrative on account of the rising demand for IoT and smart devices and the growing focus on analyzing large volumes of data from multiple sources to gain real-time insights.
- Notable market players include IBM, Microsoft, Google, Oracle, SAS, SAP, and TIBCO, among others.

Another target market for Synadia is the global edge computing market.

- As projected by Markets and Markets, this market is forecasted to rise from $36.5 billion in 2021 to $87.3 billion by 2026, registering a CAGR of 19% during the forecast period.
- Key market drivers include the growth in enterprise customers, large-scale investment, increased use of BYOD in modern business practices, and the surging demand for latency connectivity.
- Notable players include Cisco, HPE, Huawei, IBM, Dell Technologies, Nokia, Litmus Automation, and AWS, to name a few.

Achievements

To date, the company has achieved the following milestones:

- NATS.IO is a CNCF-sponsored project with over 200 million server downloads, 30,000 GitHub stars, and over 1,000 contributors.
- Synadia's customer base encompasses Fortune 500 enterprises in finance, retail, healthcare, industrials, and innovative businesses in FinTech, IIoT, AI, gaming, and transportation.
- To date, the company has secured over $16 million in investment capital.

Executive Team

Derek Collison

Founder & CEO

Experience:

- Board Member at Ronald Reagan UCLA Medical Center (current)
- Innovation Board Member at XPRIZE (current)
- Founder & CEO at Apcera
- Member of Board of Directors at Cloud Native Computing Foundation
- CTO, Chief Architect Cloud Application Platforms at VMware
- Technical Director at Google
- SVP and Chief Architect at TIBCO Software

Academic Background:

- BS in Computer Science from the University of Maryland Baltimore County

API Security

Application programming interface security, or API security, entails the practices and procedures required to prevent and mitigate unique attacks and vulnerabilities on APIs. API security is responsible for the safe transfer of data through APIs that are connected to the Internet.

Due to their nature of holding sensitive data and enabling software functions, API security is crucial for modern web application security, providing features that solve vulnerabilities such as broken authentication and authorization, lack of rate limiting, and code injection. Web APIs most commonly use TLS (Transport Layer Security) to protect the information sent by and received via the API.

From the Valuer platform:

Average year of founding of the API Security companies:

2014

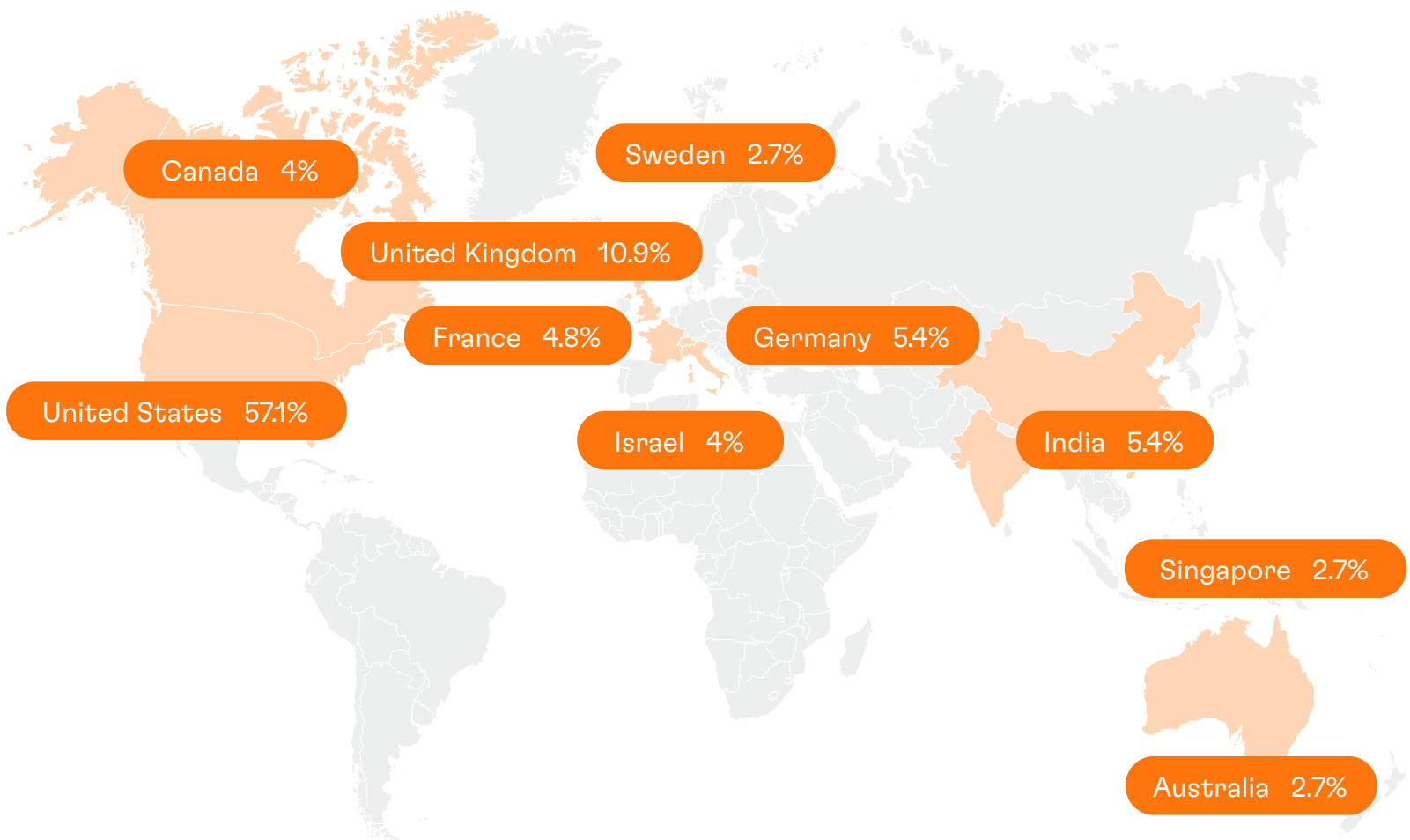
Average funding of the API Security companies:

$5,189,202

Maximum funding of the API Security companies:

$33,500,000

10 countries with the most API Security companies on the Valuer platform:



Company Highlight:

Traceable

Year of inception:
2019

Location:
San Francisco, CA, United States

Company stage:
Go-to-Market

Funding:
80,000,000 USD

Team size:
136

Website:
traceable.ai

Traceable is a California-based cybersecurity company that has developed a solution based on data and AI to protect applications and APIs. The company was founded in 2018 by Sanjay Nagaraj and Jyoti Bansal, senior software engineers that shared a common vision to develop an advanced web and API security mechanism that can deliver protection from emerging cyber threats.

Operating from the headquarters in San Francisco, the company's current team comprises over 130 members.

Customers:

FalconX

Houwzer

Business Model

The company's business model is centered around the following characteristics:

- Traceable operates on a B2B model, catering to companies that seek cloud-native application protection, API discovery, risk management, data privacy, and compliance.
- The company's main target users comprise DevOps teams, cybersecurity executives, compliance teams, and security operation teams to help them strengthen the API security of their entities.
- Traceable offers its solution on a SaaS model via a three-tier subscription model: (1) **Free,** for individuals and small business owners with a 15-day trial, (2) **Team,** for product and DevOps team at $10 per API endpoint per month (billed annually), and (3) **Enterprise,** for larger InfoSec and DevOps teams at a custom fee.

Value Proposition

The company communicates the following as its main value propositions:

- The Traceable AI platform aims to empower security and DevOps teams with a solution that protects, monitors, and investigates the traffic across web applications and APIs. It enables clients to detect threats that arise from application logic abuse by monitoring API call sequences within and across user sessions.
- The platform learns continuously from app and user behavior. Namely, it analyzes data to detect emerging threats based on application logic, thus providing security against OWASP Top10 and OWASP API Top 10 threats.
- Additionally, with its API Catalog, the company benefits security, DevOps, and compliance teams with risk assessment of possible attacks and proactive resolution of potential issues.

Product Portfolio 1/2

Traceable AI platform protects cloud-native and API-based applications from cyberattacks. It combines end-to-end distributed tracing, cloud-native integrations, and advanced context-based behavioral analytics to shield against the evolving threats that result from the increasing adoption of APIs and microservices.

To provide complete cybersecurity API protection, the platform relies on the following principles:

1. Visibility - provides insights into the real-time security condition of the applications and APIs.

- API Discovery creates API and application inventory, including the shadow and orphaned APIs. Clients can gain insights regarding API changes, app topologies, and data flows, including connectivity between edge APIs, internal services, and data stores.
- API DNA automatically extracts specifications on protocol, method, parameter details, data types, data sensitivity, value boundaries, and character distribution for every API endpoint.
- API Insights provides an overview of runtime details like sensitive data flows, call maps, usage behavior, user details, and event and threat details.
- API Risk Monitoring analyzes over 70 criteria and continuously updates the risk scores based on projections of possible attacks.
- User Attributed Activity Tracking helps clients to visualize security events and witness the threat possibility across all applications.

2. Protection - detects and stops API and web attacks, including OWASP (web) Top 10 and OWASP API Top 10 attacks.

- API & Web Application Protection stops the attacks and protects the applications with a WAF powered by ML anomaly detection for low false positives.
- Sensitive Data Tracking prevents sensitive data exposure by identifying API endpoints that handle sensitive data.
- ATO and Brute-force Attack Protection defends against such attacks through rate limiting and IP range blocking rules.
- API Vulnerability Detection identifies the exposed points before any attack can occur.
- Multi-session Threat Detection presents insights from API call sequences within and across user sessions.
- Drop-in Security Enhancement allows integration within the API gateway to automatically block threats and adapt to real-time changes.

3. Analytics - provides insights into transaction data for investigating operations and accelerating the resolution of potential issues.

- Trace Explorer enables extracting critical security information from captured transaction data and exploring vulnerabilities via an interactive dashboard.
- Threat Hunting simplifies transaction data sifting and detecting potential threats.
- Forensics allows investigating potential issues and improving troubleshooting.
- Audit and Compliance are simplified through regular API inventory updates.
- API Performace Metrics presents the number of API calls, error distribution, latency distribution, call frequency, etc.

API Catalog

The API Catalog provides automatic and continuous API discovery and visibility into all APIs, sensitive data flows, and risk posture. It works on three levels:

- Security teams can prioritize security issues based on attack possibilities obtained through a comprehensive attack surface view.
- DevOps teams can use CI/CD integrations to tackle security issues early in non-production environments.
- Risk and compliance teams use real-time, accurate API inventory and insights into the sensitive data exposure to comply with regulatory requirements effectively.

Market Opportunities

The company is operating in the global API management market.

- According to Markets and Markets, the market is expected to grow from $4.5 billion in 2022 to $13.7 billion by 2027, registering a CAGR of 25.1% during the forecast period.
- Data and services are becoming more accessible due to the fast development of the API economy. In that direction, the growth of the API management market can be attributed to the increased focus on critical business activities to drive business revenue and long-term growth.
- The increasing investments in digital transformation are also heavily influencing the market's growth. Additional market drivers include the growing utilization of AI, ML, and analytics capabilities to understand customer behavior.
- Notable dominant companies in the market include Google, IBM, Microsoft, Axway Software, Broadcom Inc., Oracle Corporation, Amazon Web Services (US), and more.

Achievements

To date, the company has achieved the following milestones:

- Traceable has raised circa $80 million in investments to date, with the most recent and largest round totaling $60 million. Closed in May 2022, its Series B was led by IVP with participation from BIG Labs, Unusual Ventures, Tiger Global Management, and additional undisclosed angel investors.
- In November 2021, CSO listed Traceable as one of the 18 cybersecurity startups to watch after the company won in the "Next-Gen Cyber Security Artificial Intelligence" category at the 2021 Global InfoSec Awards.
- In February 2021, Traceable announced that it had entered into a strategic partnership with Silicon Valley CISO Investments (SVCI), offering Traceable capital and strategic counsel.
- CRN featured the company among the 10 Coolest New DevOps Startups of 2020 as a recognition of the company's contribution toward enabling collaboration between developers and operators necessary to facilitate software release at the speed of the cloud.
- Traceable has obtained various security and compliance certifications, including the SOC 2 Type 1 and Type 2 certificates.

Executive Team

Jyoti Bansal

Co-Founder & CEO

Experience:

- Co-Founder & CEO at Harness (current)
- Co-Founder at Universal Ventures (current)
- Founder & CEO at BIG Labs (current)
- Founder, CEO, and Chairman at AppDynamics
- Architect at Willy Technologies/ Computer Associates
- Engineering Manager/Senior Engineer at Datasweep/Rockwell Automation
- Senior Software Engineer at netLens/ NextPage

Academic Background:

- Bachelor's degree in Computer Science from the Indian Institute of Technology, Delhi

Sanjay Nagaraj

Co-Founder & CTO

Experience:

- Investor at Harness (current)
- VP Software Engineering at AppDynamics
- Head of Engineering at emFAST Inc
- Principal Software Engineer at Optus Software

Academic Background:

- Bachelor's degree in Computer Science from the University of Mysore

Cloud Infrastructure

Cloud infrastructure refers to the collection of different hardware and software components as well as other elements required to provide cloud computing. Generally, cloud infrastructure is categorized into three parts that work together to create a cloud service: (1) computing power, (2) networking, and (3) storage. These are considered key features that provide users with the interface and ability to access their virtualized resources and assets.

The main responsibility of the cloud is maintaining and managing traditional on-premise hardware. e.g., servers or other storage devices, as well as visualization and networking to support the computing requirements of a cloud computing model.

From the Valuer platform:

Average year of founding of the Cloud Infrastructure companies:

2014

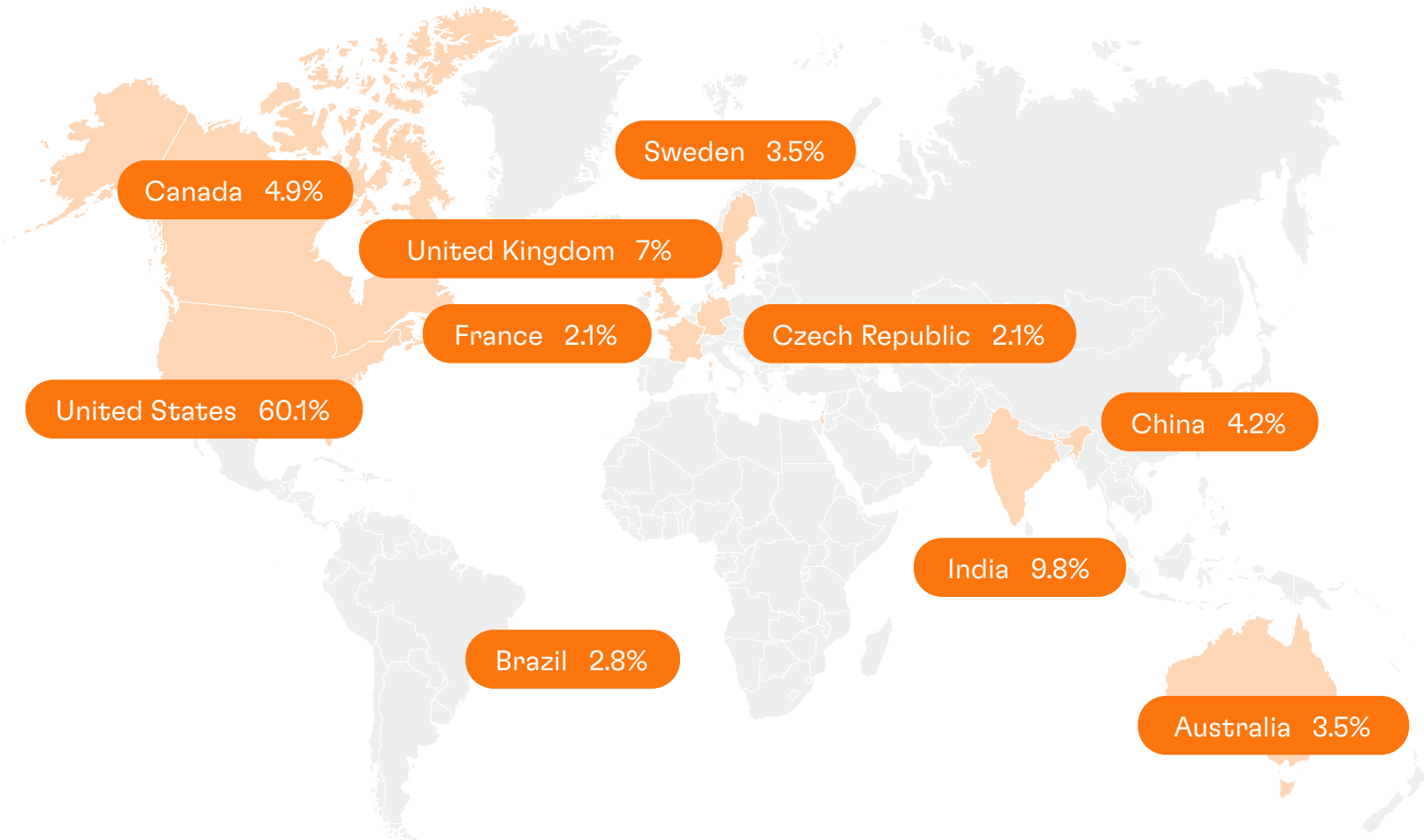
Average funding of the Cloud Infrastructure companies:

$15,842,194

Maximum funding of the Cloud Infrastructure companies:

$130,486,391

10 countries with the most Cloud Infrastructure companies on the Valuer platform:



Company Highlight:

VMware Tanzu

Year of inception:
2019

Location:
Palo Alto, CA, United States

Company stage:
Growth/Expansion

Funding:
N/A

Team size:
589

Website:
vmware.com

VMware Tanzu encompasses a portfolio of products and services that allow enterprises to run Kubernetes applications across cloud and on-premise environments. The offering features tools for building modern applications and managing the footprint from a central control point.

The core technology behind the Tanzu suite was developed by Pivotal Labs, an agile software development consulting firm that VMware acquired in 2019. Following this, VMware launched the Tanzu suite as an extended offering to help businesses solve challenges across the Kubernetes environment. Currently, the branch operates from its premises in Palo Alto (CA), employing a team of almost 600 members.

Customers:

T-Mobile

Hyundai Autoever

Yammer

Business Model

The company's business model is centered around the following characteristics:

- VMware Tanzu works primarily with B2B entities, helping them set up a consolidated operating model for virtual machines and containers within their private cloud.
- Its portfolio caters to software developers, IT operations teams, and businesses across the automotive, financial, healthcare, insurance, manufacturing, retail, and telecom sectors.
- The company also conducts business on a B2G basis, helping public sector entities build a multi-cloud Kubernetes environment for scalable app migration and management.
- VMware Tanzu generates revenue through software license fees.

Value Proposition

The company communicates the following as its main value propositions:

- VMware Tanzu's products and services enable full stack modernization, allowing businesses to simplify their software operations across multi-cloud infrastructures.
- The suite aids DevOps teams in accelerating the software deployment, providing them a platform with modern software supply chain frameworks and validated open source tech.
- Another advantage of VMware Tanzu's offering is the option to centrally run and manage cloud, cluster, and app operations.
- The company highlights that its portfolio, on average, delivers an 82% increase in software development and a 78% increase in operational efficiency.

VMware Tanzu's cloud-native portfolio features three main components:

1. Tanzu Application Platform - a modular, application-aware platform for accelerated design, development, and delivery of apps;
2. Tanzu for Kubernetes Operations - solutions for building Kubernetes-based infrastructure at scale across all clouds, and
3. Tanzu Labs - consulting services for advancing, building, and managing apps.

Tanzu Application Platform

VMware Tanzu's application platform accelerates software development via pre-configured cloud-native pattern templates for cloud-native applications. Its functionalities allow DevOps teams to automate app deployment with a customizable, built-in software supply chain, supported by a Kubernetes abstraction layer that hastens app product design, development, and delivery. The company claims its platform enhances developer velocity, allowing businesses to maintain a consistent GUI to deliver services and APIs from a single management portal.

The platform supports multi-cloud environment operations and can run on any on-premise Kubernetes cluster. It promises significantly enhanced DevOps efficiency, providing tools for quick onboarding, prompt access to dev tools for fast iteration, and debugging code directly from IDE. The solution also facilitates a frictionless Dev to Ops handoff, allowing developers to produce code without interruptions via an automatic supply chain trigger.

Tanzu for Kubernetes Operations

The Tanzu for Kubernetes Operations offering provides simplified container deployment, scaling, and management, acting as a foundation for creating Kubernetes-based infrastructure and optimizing its performance across cloud environments. The product selection features a centralized management hub that allows conformant, enterprise-ready runtime management. Moreover, it enables end-to-end app and data security by connecting microservices in multi-cloud environments. It also grants access to transaction-level insights, security policies, and all-encompassing data encryption.

The Kubernetes operations suite enables users to proactively optimize their performance by analyzing platform and app metrics and identifying anomalies, coherently devising fixes to resolve the issue. Other capabilities include:

- **Enterprise-ready Kubernetes runtime deployment,**
- **Multi-cloud Kubernetes management,**
- **End-to-end connectivity and security,**

- Load balancing and ingress integration functionality,
- Full-stack enterprise observability,
- Native VMware vSphere integration, and
- App modernization features

Tanzu Labs

Tanzu Labs aims to help businesses modernize and build applications that adequately capture their clients' vision. The service comprises a dedicated team that allows partners and organizations worldwide to speed up the software development process and advance legacy applications while decreasing the associated operating costs and risks. The consultancy covers business-critical app assessment that allows businesses to promptly migrate existing software and adopt practices along the way necessary for sustained efficiency and meaningful optimization.

Additional VMware Tanzu Offerings

Alongside its three flagship offerings, VMware Tanzu's suite also features a wide range of complementary products, including:

- Tanzu Kubernetes Grid,
- Tanzu Mission Control,
- Tanzu Application Service,
- Tanzu Build Service,
- VMware Application Catalog,
- Tanzu Service Mesh,
- Tanzu Data Services,
- Tanzu Observability,
- VMware Spring Runtime, and
- Azure Spring Apps.

Market Opportunities

The company is operating in the global application modernization market.

- According to Markets and Markets, the market is poised to grow from $11.4 billion in 2020 to an estimated $24.8 billion by 2025, at a CAGR of 16.8% during the forecasted period.
- The favorable market growth can be attributed to the proliferation of cloud services and large-scale migration of workloads to cloud-based and SOA (Service Oriented Structure).
- The prevailing transformation and modernization of legacy systems and the increased demand for modern infrastructure are set to further drive the global market.
- By application, the cloud application modernization segment is expected to grow at a higher CAGR during the forecast period. In terms of client size, the SME market will record the fastest growth.
- Regionally, the Asia Pacific region will rise at the fastest CAGR, owing to its large population size and strong software service demand.
- Notable market players include Accenture, IBM, Atos, HCL, Capgemini, Bell Integrator, and Blu Age.

Achievements

To date, the company has achieved the following milestones:

- VMware Tanzu Observability received Visionary recognition by Gartner in the 2022 Gartner Magic Quadrant for Application Performance Monitoring (APM).
- In 2022, the Tanzu for Kubernetes Operations suite expanded its reach to Canada and India to support VMware Tanzu customers across new regions.
- In 2020, the VMware Tanzu support community and knowledge management team were honored with a TSIA STAR Award for outstanding innovation, leadership, and excellence.

Executive Team

Raghu Raghuram
CEO at VMWare

Experience:

- Progressed to CEO at VMware
- Director of Product Management at Bang Networks
- Director of Product Management at Netscape

Academic Background:

- MBA from the Wharton School of Business
- MEng in Electrical Engineering from the Indian Institute of Technology, Mumbai

Sumit Dhawan
President at VMWare

Experience:

- Progressed to President at VMware
- CEO at Instart
- Group VP & General Manager at Citrix Systems

Academic Background:

- MBA from the Warrington College of Business at the University of Florida
- MSc in Computer Science from the University of Minnesota
- BSc in Computer Science from the Indian Institute of Technology (IIT)

Secure Access Service Edge (SASE)

Secure Access Service Edge, or SASE, is a framework utilized within network architecture that brings together cloud-native security technologies, such as secure web gateway (SWG), zero-trust network access (ZTNA), cloud access security broker (CASB), and firewall as a service (FWaaS) with SD-WAN capabilities.

This enterprise networking and security category was first introduced by Gartner as a response to the dynamic secure access needs across organizations. The expected outcome of this framework is a secure connection of users, systems, and endpoints to applications and services anywhere within the network. Additional benefits are lower effort and costs, typically linked to the complex and fragmented infrastructure of point solutions.

From the Valuer platform:

Average year of founding of the SASE companies:

2014

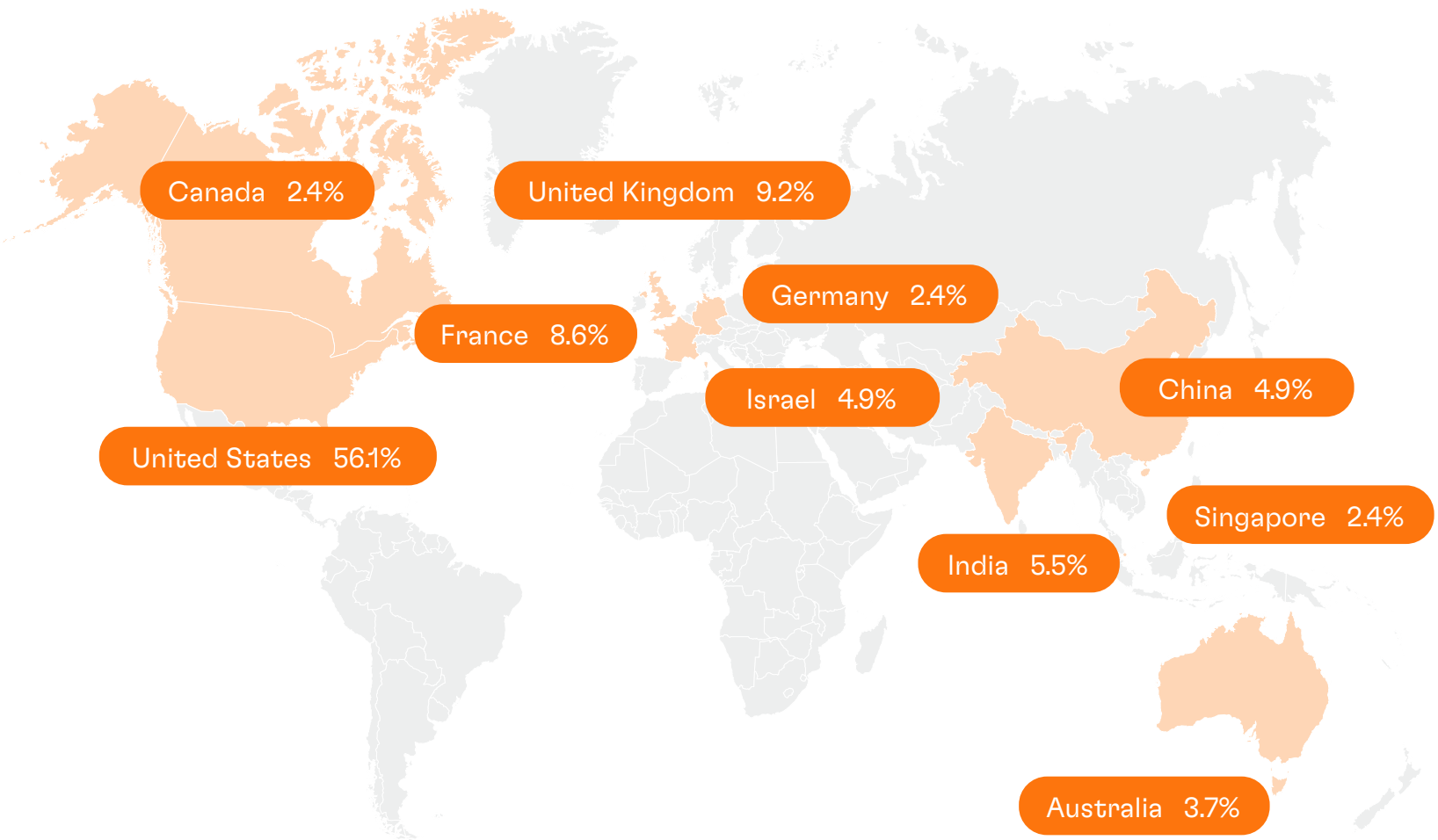
Average funding of the SASE companies:

$35,887,188

Maximum funding of the SASE companies:

$1,040,000,000

10 countries with the most SASE companies on the Valuer platform:



Company Highlight:

Cato Networks

Year of inception:
2015

Location:
Tel Aviv, Israel

Company stage:
Growth/Expansion

Funding:
532,000,000 USD

Team size:
596

Website:
catonetworks.com

Cato Networks brings clients a single-vendor SASE platform, combining Cato SD-WAN and a complete cloud-native security service edge, Cato SSE 360. A recognized Gartner Cool Vendor, Cato provides integrated networking and security platform that securely connects all enterprise locations, people, and data.

The company was founded in 2015 by network security expert and serial entrepreneur Shlomo Kramer and Gur Shatz, an experienced entrepreneur in the web application security sector. Since then, the company's team has grown by nearly 600 members, operating from the headquarters in Tel Aviv.

Customers:

BioIVT

Picanol Group

ADB Safegate

Innovex

Business Model

The company's business model is centered around the following characteristics:

- Cato Networks is a B2B company that has developed an offering centered around Gartner's enterprise networking and security category Secure Access Service Edge (SASE) and its subset Security Service Edge (SSE).
- The offering is suitable for organizations aiming to shift from rigid MPLS networks to a network architecture that does not require the costs, complexity, and risks associated with legacy IT approaches.
- As of 2021, Cato's customer portfolio counts over 1,100 enterprises with more than 17,000 branches and cloud instances and 300,000 remote users. Notably, Cato recorded 150% growth in large deals, shipped 75% more Cato Sockets edge SD-WAN devices YoY, and sold 77% more remote user licenses YoY.
- Cato's 2021 business results showed a growing revenue by 96% YoY, increased headcount by 66%, and a doubling in valuation to $2.5 billion with an added $200 million investment.

Value Proposition

The company communicates the following as its main value propositions:

- Cato enables simple migration from MPLS to SD-WAN. Additional benefits include optimized connectivity to on-premises and cloud applications, secure branch Internet access, and seamless integration of cloud datacenters and remote users into the network with a zero-trust architecture.
- Cato SSE 360 provides complete visibility, optimization, and control of all traffic, users, and applications.

Along with a seamless path to SASE, enterprises can benefit from improved security posture, cost savings, and business agility.

- Cato selected Forrester Consulting to conduct a Total Economic Impact (TEI) study, which found that Cato's ROI had come out to 246% over three years with total savings of $4.33 million NPV and a payback of initial investment in less than six months.

Cato's integrated network and security platform, Cato SASE Cloud, with SSE 360, connects all enterprise locations, users, applications, and clouds into a secure cloud-native service.

SSE 360: Security-as-a-Service

SSE 360, Cato Networks' cloud-native security stack, is built directly into the Cato SASE Cloud. Based on the Cato Single Pass Cloud Engine (SPACE) architecture, it allows security policies to be applied consistently across all traffic in the network, eliminating the need for disparate edge security devices. Additionally, it combines capabilities like Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), Zero Trust Network Access (ZTNA/SDP), and Firewall-as-a-Service (FWaaS) with Advanced Threat Prevention (IPS, Next Generation Antimalware).

Clients are provided access control capabilities through Cato's next-generation firewall (NGFW), gaining full application visibility with the opportunity to inspect the packet data payload and differentiate between diverse web traffic types. The NGFW inspects WAN and Internet traffic and can enforce granular rules based on network entities, time restrictions, and type of traffic. Moreover, the Deep Packet Inspection (DPI) engine classifies the relevant context without decrypting the payload. In addition to a full list of signatures and parsers to identify common applications, Cato provides custom application definitions that identify account-specific applications by port, IP address, or domain.

Furthermore, Cato's SWG enables organizations to track, control, and block access to websites based on predefined and customizable categories. This granular control over Internet-bound traffic enables corporate policy enforcement and prevents downloading unwanted or malicious software. Cato's management portal enables SWG management, covered by a full audit trail.

Cato's SASE Cloud covers cloud and data security. Its CASB provides in-depth visibility into SaaS usage, enabling IT leaders to better deal with shadow IT and data usage. Its DLP protects from attempts to upload or extract sensitive information. Cato's next-generation anti-malware (NGAM) protection and Intrusion Prevention System (IPS) capabilities, as part of the Advanced Threat Protection, inspect both WAN and Internet traffic. Furthermore, Cato PoPs inspect TLS-encrypted traffic in the highly-scalable Cato Cloud, eliminating scaling constraints with on-premises equipment or additional latency from cloud-based traffic inspection.

Notable features include:

1. Remote Access

Customers can gain zero-trust network access (SDP/ZTNA) to on-premises and cloud applications using

laptops, tablets, and smartphones. This service gives users Cato Client or Clientless browser access, allowing a secure connection to the nearest Cato PoP via strong Multi-Factor Authentication. The traffic is fully inspected by Cato's security stack during the session.

2. Edge SD-WAN

Cato's proprietary Socket SD-WAN device connects a physical location to the nearest Cato PoP via one or more last-mile connections. Its capabilities include active-active link usage, application- and user-aware QoS prioritization, dynamic path selection to deal with link blackouts and brownouts, and packet duplication to overcome packet loss.

3. Global Private Backbone

With its private global backbone of more than 75 PoPs connected via multiple SLA-backed network providers, Cato offers end-to-end route optimization for WAN and cloud traffic, and a self-healing architecture for maximum service uptime.

4. Multi-cloud / Hybrid-cloud

Cato offers integration with major cloud providers with secure IPSec tunnels or a Cato vSocket virtual appliance. Cato's SSE 360 inspects all traffic to and from the cloud DC.

5. SaaS Optimization

With public cloud applications, Cato can accelerate end-to-end throughput up to 20 times, enhancing application performance for bandwidth-intensive operations like file upload or download.

6. Cato Management Application

Cato's service can be managed through a cloud-based self-service management application, including full network and security policy configuration and detailed analytics on network traffic and security events. In collaboration with its partners, Cato also offers managed service options including Intelligent Last-Mile Management, Hands-Free Management, Managed Threat Detection and Response, and Site Deployment.

Market Opportunities

The company is operating in the secure access service edge (SASE) market.

- According to Markets and Markets, the SASE market is expected to grow from an estimated $1.2 billion in 2021 to $4.1 billion by 2026, at a CAGR of 26.4%.
- The main growth factors include the increasing preference for remote working in the wake of the COVID-19 pandemic and the rising need for a unified network security architecture with the capabilities of SD-WAN, FWaaS, SWG, CASB, and ZTNA solutions.
- IT and ITeS, along with retail and eCommerce, are the verticals expected to grow the fastest during the forecast period.
- In terms of regions, North America is considered the most mature market, owing to the rise in cloud security measures and authentication frauds. Moreover, this region houses some of the most prominent market players.
- Cato Networks is listed as a major player in the market among notable organizations such as Cisco Systems, VMware Inc., Fortinet, Inc., Palo Alto Networks Inc., etc.

Achievements

To date, the company has achieved the following milestones:

- Cato Networks prides itself on receiving 12 accolades by Gartner over its years of operations.
- More recently, in 2021, the company was listed as a Sample Vendor in the “Secure Access Service Edge” category of the Gartner® Hype Cycle™ for Enterprise Networking for a third consecutive year.
- Additionally, Cato was one of the two vendors identified in 2021 as Sample Vendor in the “SASE”, “Zero Trust Network Access (ZTNA)”, and “Firewall as a Service (FWaaS)” categories in the Hype Cycle for Network Security.
- In 2017, the company received numerous accolades. One recognition was TMC’s Internet Telephony SD-WAN Excellence Award in addition to being shortlisted for Layer123’s Network Transformation Awards as the Best SD-WAN Service. Other recognitions included Gartner Cool Vendor, a finalist as RSA Innovation Sandbox, and CRN for 25 Coolest Network Security Vendors.

Executive Team

Shlomo Kramer

Co-Founder & CEO

Experience:

- Founding Investor and Board Director at At-Bay (current), Aqua Security (current), and Exabem (current)
- Investor at Skinos Family Office (current)
- Founding Investor and Board Director at Gong.io, Indegy, Fundbox, and Insert.
- Founder, President, CEO, and Chairman of the Board of Directors at Imperva
- Founding Investor and Board Director at WatchDox (BBRY), LacoonSecurity (CHKP), Skyfence (IMPV), Trusteer (IBM), Sumo Logic, and Worklight (IBM)
- Investor and Board Director at LightCyber and Palo Alto Networks
- Founder of Check Point (CHKP)

Academic Background:

- MSc in Computer Science from The Hebrew University of Jerusalem
- BSc in Mathematics from Tel Aviv University

Gur Shatz

Co-Founder, President & COO

Experience:

- CTO and Board Member at Cato Networks
- CEO, Founder, and Board Member at Incapsula
- Progressed to VP Products at Imperva
- Software Engineer at IDcide
- QA at ICQ

Academic Background:

- BSc in Computer Science from Tel Aviv College

Data Security Management

Data security management refers to the oversight processes of an organization to prevent corruption, theft, or unauthorized access to its private data, regardless of the form. It is a blend of both digital (cyber) and physical processes to safeguard digital information throughout its entire life cycle, including planning, implementing, and verifying techniques, such as backups, data masking, data erasure, encryption, TDE, CASB, two-factor authentication, and electronic security tokens, among others.

For an all-encompassing data security management, organizations cover every element, from hardware to software, storage devices, user devices, access and administrative controls, and organizations' policies and procedures.

From the Valuer platform:

Average year of founding of the Data Security Management companies:

2014

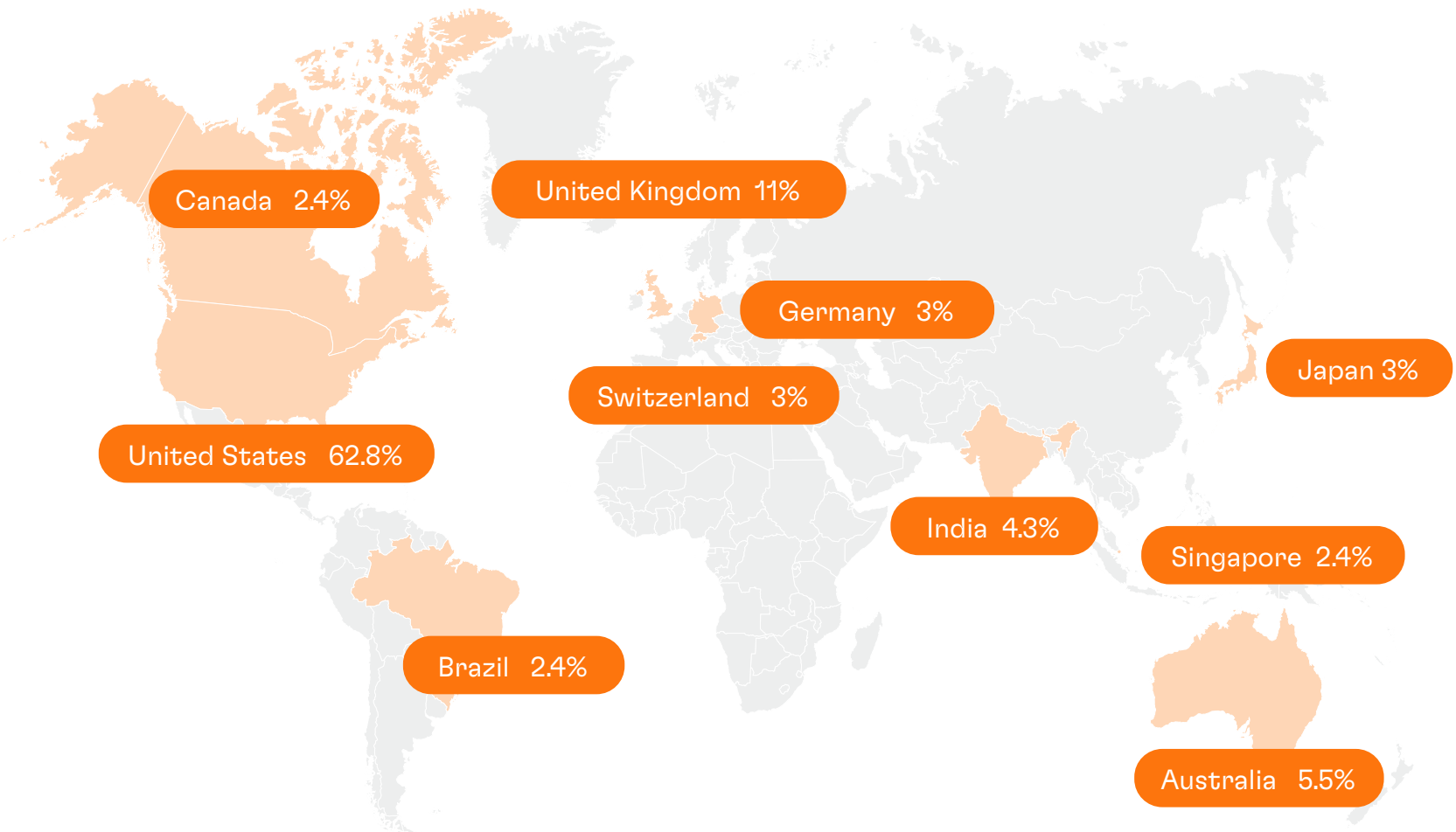
Average funding of the Data Security Management companies:

$12,931,688

Maximum funding of the Data Security Management companies:

$104,900,000

10 countries with the most Data Security Management companies on the Valuer platform:



Company Highlight:

Fortanix

Year of inception:
2016

Location:
Mountain View, CA, United States

Company stage:
Growth/Expansion

Funding:
45,300,000 USD

Team size:
208

Website:
fortanix.com

Fortanix is a software development company focusing on data-first network security solutions. The company is actively developing confidential computing, a novel technology that leverages processor enclaves, enabling it to protect data during its entire lifecycle.

Fortanix was co-founded in 2016 in Mountain View (CA) by cybersecurity experts Ambuj Kumar and Anand Kashyap, serving as CEO and CTO, respectively. Currently, the company employs around 200 professionals across its offices in the United States, the Netherlands, India, and Singapore.

Customers:

Google

Intel

U.S. Department of Justice

GE Healthcare

Form3

Business Model

The company's business model is centered around the following characteristics:

- Fortanix targets clients in need of multi-cloud data security, secrets management, hardware security modules, tokenization, key management, and application-level encryption.
- The company caters to enterprises and organizations of all sizes across the healthcare, FinTech, banking, manufacturing, and Web 3.0 industries.
- Fortanix applies a specific revenue model depending on the solution, such as SaaS or Bring Your Own License (BYOL).
- To date, the company has onboarded several notable clients, including Google, IBM, Intel, and Valeo, among others.

Value Proposition

The company communicates the following as its main value propositions:

- Fortanix takes a data-centric security approach by decoupling security from the infrastructure via its Runtime Encryption.
- The company claims its technology is the industry's first Web 3.0 infrastructure solution, securing blockchain infrastructure with a FIPS-certified product.
- The company's Runtime Encryption mitigates the risk of compromised credentials, network vulnerabilities, and bad actors threatening critical data.
- Moreover, Fortanix enables customers to run their software in confidential computing environments while securing their data at rest, in motion, or during use.

Product Portfolio

Fortanix is developing an emerging technology named confidential computing, a cloud-based approach that enables securing sensitive data while in use. Confidential computing is accomplished by leveraging hardware-based trusted execution environments (TEEs). In turn, the trusted environment is achieved through utilizing secure coprocessors inside the CPU's enclaves that use embedded encryption keys and attestation mechanisms accessible exclusively to authorized application code.

Data Security Manager is the company's main offering, which is based on confidential computing, runtime encryption, key management, and tokenization. The product encompasses solutions for cloud data control, business logic and database security, tokenization, key management service, DSM acceleration, and hardware security. Providing compliance with regulations such as GDPR, CCPA, and Schrems II, the product is a scalable cloud and on-premises solution that aims to secure data on all levels. It provides integration with data platforms and cloud providers such as Amazon S3, Microsoft SQL Server, Apache Hadoop, Google Big Query, VMware, and AWS.

Data Security Manager SaaS is Fortanix's subscription-based offering for data security that provides integrated encryption, multi-cloud key management, and tokenization bundled in an accessible platform. The web-based platform utilizes HSM-grade key storage, a highly resilient web-scale architecture, and Intel's SGX secure processor enclaves to deliver multi-cloud key management and visibility. The company claims its data security management platform provides benefits such as global coverage, integrated data security, ease of integration, and a lower total cost of ownership.

Confidential AI is a confidential computing platform that enables data teams and engineers to run AI models in confidential computing mode. The platform shares the same primary method of operation as the Data Security Manager with additional support and services for a broad range of AI and ML models and data security for the ingestion, learning, inference, and fine-tuning of ML operations.

The Confidential Computing Manager enables applications to run and execute in confidential computing environments, managing the environment's integrity and the application's lifecycle. Fortanix markets its confidential computing manager as a turnkey solution that supports a broad set of applications. It secures the computing process with identity verification, data access control, and attestation.

The Enclave Development Platform (EDP) enables engineers to develop Intel SGX enclaves using the Rust programming language. According to the company, its EDP solution delivers benefits such as ease of use, compatibility with existing Rust code, and enhanced security.

Market Opportunities

The company is operating in the cybersecurity market.

- According to Markets and Markets, the global cybersecurity market is expected to grow from $240.27 billion in 2022 to $345.38 billion by 2026, at a CAGR of 9.5% during the forecast period.
- One of the key market drivers is the rise in frequency and intensity of cyber attacks, which drives enterprises to channel their assets into developing advanced cybersecurity solutions. Additionally, the increase in remote working setups resulting from the COVID-19 pandemic has increased the vulnerability of enterprise networks, increasing attacks.
- Region-wise, North America is expected to dominate the market during the forecast period, principally due to the growth in Industrial Internet of Things solutions which are high-risk cybercrime targets. However, the Asia-Pacific region is expected to grow at the fastest CAGR during the forecast period.
- Notable market players include IBM, Cisco, CheckPoint, Amazon Web Services, Fortinet, and Microsoft.

Achievements

To date, the company has achieved the following milestones:

- In June 2022, the company won the Global InfoSec Awards, being named “Publisher’s Choice for Confidential Computing” by Cyber Defense Magazine.
- In February 2022, Fortanix won the Data Security, Artificial Intelligence, and Best Data Security Company awards at the 2022 Cybersecurity Excellence Awards.
- The Fortanix Confidential AI was named the winner of the 2022 BIG Innovation Awards sponsored by the Big Intelligence Group.
- In 2021, the company won the TMCNet Cybersecurity Excellence Awards and the CyberSecured Awards with its Data Security Management SaaS product.
- In 2020, Fortanix was listed as a Market Leader in the Encryption category at the Infosec Awards.
- In 2019, the company received the Best Product in Cloud Security and Most Innovative Encryption award at the Infosec Awards. It was also selected as a finalist at the CRN Tech Innovators and Women of the Channel Awards.
- The company’s Self-Defending KMS was awarded at the 2019 Cloud Computing Security Excellence Awards.
- In 2018, Fortanix was named a Cool Vendor in IoT Security by Gartner.

Executive Team

Ambuj Kumar

Co-Founder & CEO

Experience:

- Advisory Board Member at Axelar Network (current)
- Business Advisor at InfoSec Global (current; part-time)
- Contributor at Forbes Technology Council (current; part-time)
- Chief Architect of Cryptography Research at Rambus
- Hardware Design Lead at NVIDIA

Academic Background:

- MSc in Electrical Engineering from Stanford University
- BTech in Electrical Engineering from the Indian Institute of Technology Kanpur

Anand Kashyap, PhD

Co-Founder & CTO

Experience:

- Staff Engineer at VMware
- Member of Technical Staff at Arkin Net
- Principal Security Researcher at Symantec
- Research Intern at Microsoft Research India and NEC Laboratories America
- Research and Development Engineer at Tejas Network

Academic Background:

- PhD in Computer Science from the Stony Brook University
- BTech in Computer Science from the Indian Institute of Technology Kanpur

Executive Team

Faiyaz Shahpurwala

Chief Product & Strategy Officer

Experience:

- Advisory Board Member at View Inc. (current)
- Advisory Board Member at Platform 9 (current)
- Vice President and General Manager of IBM Cloud
- Advisory Board Member at Minjar
- Progressed to SVP of Cloud Infrastructure & Managed Services at Cisco
- Vice President of Andiamo

Academic Background:

- MSc in Computer Engineering from Western Michigan University
- BEng in Computer Engineering from Western Michigan University

About IoT Community

(Internet of Things Community)

The IoT Community is a privately held UK based and registered corporation, serving as the world's largest and longest standing CxO community of senior business leaders and IoT practitioners comprising 30,000+ members globally.

Founded in 2015, the function of the community is to focus on the adoption and application of IoT in commercial environments, seeking to understand and contribute to applying the technology or overcoming the wide variety of barriers, inhibitors, and technical and operational issues.

The IoT Community aims to be the place to be or place to come for IoT information and insights on the implementation and operation of IoT systems and applications. Their focus is on accelerating the adoption and implementation of IoT systems and applications, making these processes easier, widespread, and secure.

For more information, visit:

iotcommunity.net

@IoTCommunity
@IoTChannel
#IoTCommunity

IoT Community

About Valuer

Valuer's vision is to fuel and foster the world's innovation by mapping global innovation activities. By combining data about startups and technologies, they identify and present patterns to forward-thinking companies, startups, universities, and investors alike. Clients can use Valuer to dive headfirst into identifying relevant companies and technologies.

The company organizes +20 mio data points to spot trends, discover new technologies, and map industries. They use AI and machine learning to analyze, cluster, and identify data, and human researchers to enrich that data. Clients can start at the macro level by exploring industries and technologies and then move on to identifying relevant companies. Or start at the micro, company level and from there understand the industry and how it associates.

Valuer is a one-stop shop for innovation and opportunity discovery. Visit valuer.ai to find new technologies and collaboration opportunities, uncover strategic suppliers or find and follow acquisition targets.

For more information, visit:

valuer.ai

@ValuerAI

ValuerAI

Find innovative technologies that will give your company competitive advantage

Try Valuer for free

Valuer

Valuer.ai · Kristianiagade 7 · DK-2100 Copenhagen · Denmark · contact@valuer.ai