Internet of Things® Community

2021

IoT COMMUNITY

SECURITY

ZERO TRUST AS THE ENABLER OF IoT SECURITY

COMPANY CLUSTER ANALYSIS:

MULTI-FACTOR AUTHENTICATION

DIGITAL SIGNATURES

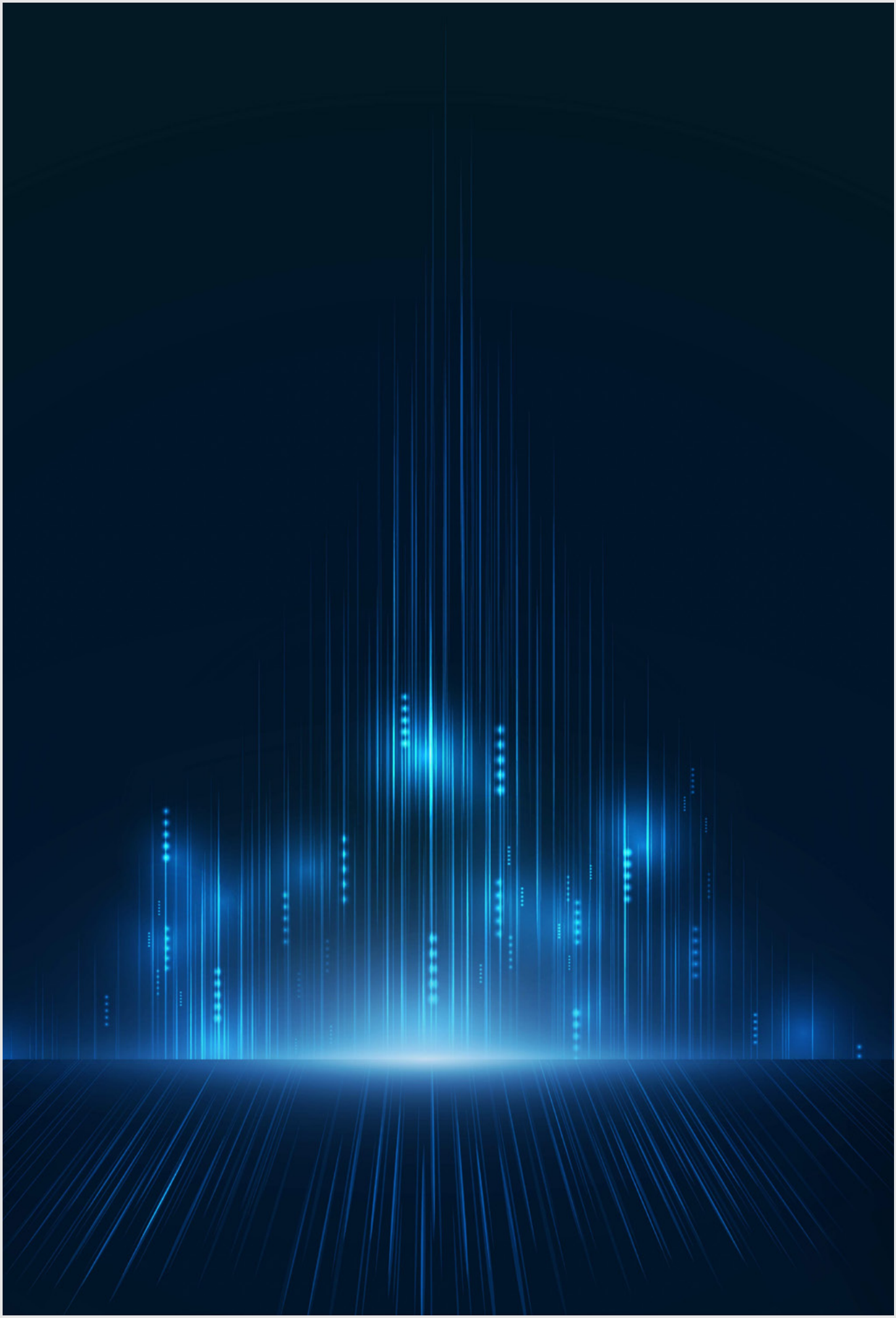
REMOTE WORK

FRAUD DETECTION

ENHANCED VISIBILITY

POWERED BY

VALUER



Index

Foreword

This report aims to explore the innovation ecosystem in the IoT security area by mapping trends, business models, and technologies.

To get familiar with both the “big picture” and specific solutions, the publication includes data analysis of clusters of companies that develop relevant technologies, as well as five case studies of companies.

The magazine takes an in-depth look at five areas of innovation relevant to IoT security: Multi-factor Authentication, Digital Signatures, Remote Work, Fraud Detection, and Enhanced Visibility.

To identify the companies most suitable for inspiration or potential collaboration with the IoT Community, the selection favored those with already-existent practical solutions and proof of concept.

Workflow Overview: How This Report Was Created

On these pages, you can learn how the development of this report unfolded: from defining areas of interest that match IoT Community's needs to preparing the publication's final design.

STEP 1.

COMPANY SEARCH

The process began with the IoT Community team defining areas of interest they would like to explore. Focusing on one area at a time, in this case on IoT Security, Valuer then processed its database to find all companies potentially relevant to it.

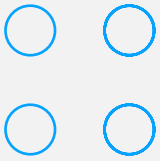
In the next step, the platform applied Natural Language Processing (NLP) to filter around 2000 organizations that best match the request's exact combination of words, terms, and semantics.

STEP 2.

COMPANY CLUSTERING

The circa 2000 identified companies were then analyzed using an unsupervised algorithm and referenced to five sub-areas.

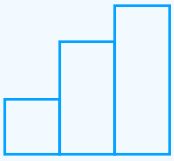
By choosing the ones nearest to a projected point, the platform then selected roughly 200 companies most relevant to each of the five sub-areas (this is how the company clusters were formed.)



STEP 3.

DATA INSIGHTS

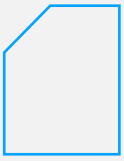
Each company cluster was then processed to generate useful quantitative data. Additionally, the Valuer platform applied its four proprietary validation algorithms to provide an objective ranking of each cluster's performance regarding its success potential, market maturity, degree of fit to the IoT Community's focus, and level of innovativeness.



STEP 4.

COMPANY CASE STUDIES

In the final step, to provide a successful business model representative for each cluster, Valuer prepared case studies of five companies that represent each area's common patterns.



Clusters of Companies That Develop IoT Security Solutions

Company clusters:

Multi-factor Authentication

Digital Signatures

Remote Work

Fraud Detection

Enhanced Visibility

Identifying companies relevant to security

The process starts with Valuer processing its database of more than 600,000 companies to identify all potentially relevant to IoT security.

The relevant company descriptions were then processed by Natural Language Processing (NLP), which finds patterns impossible to recognize with tags and regular search mechanisms. At this point, the number of organizations was narrowed down to around 2000 most-relevant ones.

The platform then referenced the companies to five focus areas deducted from the IoT Community's request (listed below). By choosing the ones nearest to a projected point, it selected roughly 200 most relevant to each of the five clusters.

Grouping companies from different focus areas

The illustration shows the clusters of companies (represented with dots) which are colored depending on their projection area. Their proximity to other companies depends on the commonalities of the products or solutions they provide.

Even though the platform processes the clusters in 1024 dimensions, we've included a 2D interpretation for demonstration purposes (this is also why some dots may seem very distant from their projection areas). The rendered image lets us make several straightforward interpretations.

Observations and company trends

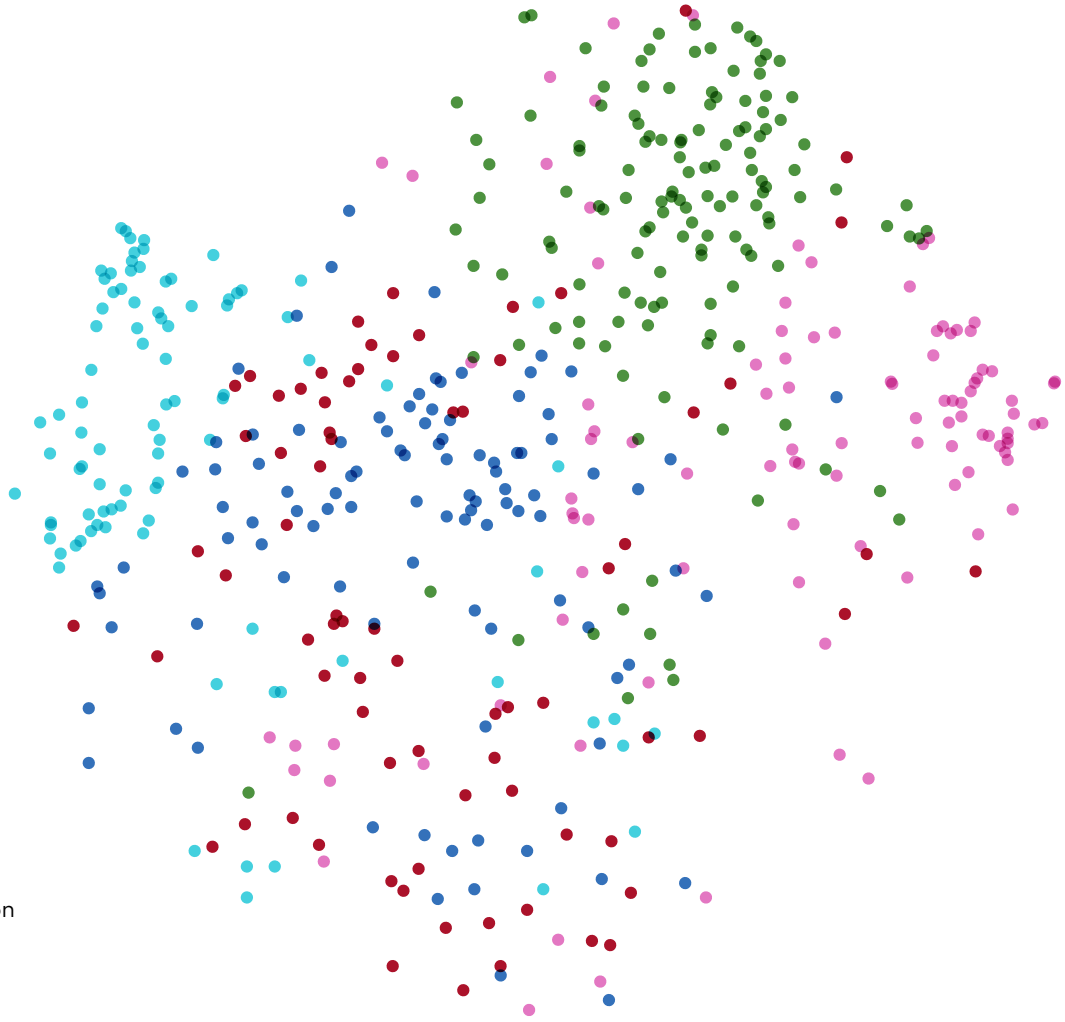
We can draw several insights from the company clustering image:

1. Overall there is a considerable amount of overlap between the clusters (with the exception of the **Fraud Detection** cluster). This may indicate similarities in the market approach and technologies of the four aforementioned clusters.

2. Despite the considerable spread of the clusters, there are two more distinct cluster groupings on the map: **Enhanced Visibility** and **Remote Work.** These standalone clusters may be addressing different issues or using technologies different from the other clusters.

3. The **Multi-factor Authentication** and **Digital Signatures** clusters are scattered in the middle of the map, which might indicate a variety of innovations in the clusters. The two clusters have considerable overlap with each other, which could be due to the use of similar technologies and approaches.

4. The **Fraud Detection** cluster is less spread than the **Multi-factor Authentication** and **Digital Signatures** clusters but has some overlap with them. This may suggest that the clusters utilize unique technologies but also occasionally combine their approaches to address similar issues.



CLUSTER SECTORS

- Multi-factor Authentication
- Digital Signatures
- Remote Work
- Fraud Detection
- Enhanced Visibility

Ranking the Clusters of Companies

The platform uses four parameters to assess the clusters' potential, market opportunity, degree of fit, and innovativeness:

1. **Success Potential:** The AI platform uses historical data from each company to evaluate the group's overall chance for future success.
2. **Market Maturity:** The AI platform analyzes companies' technologies to estimate the group's overall potential to generate profit. The algorithm analyzes the companies' financial history, the potential of attracting customers, and the maturity of their technology to compare it to the market's general development and trends.
3. **Degree of Fit:** The AI platform uses Natural Language Processing (NLP) to grade how well a cluster of companies aligns with the customer's challenges.
4. **Innovativeness:** The AI platform looks for original and previously unseen combinations of business models and technologies to grade how generally innovative a cluster is.

	Success Potential	Market Maturity	Degree of Fit	Innovativeness	**Total**
Fraud Detection	55	46	64	80	**245**
Multi-factor Authentication	55	46	67	71	**239**
Digital Signatures	54	48	63	71	**236**
Remote Work	50	48	61	72	**231**
Enhanced Visibility	53	40	62	72	**227**

Data Insights

General data observations:

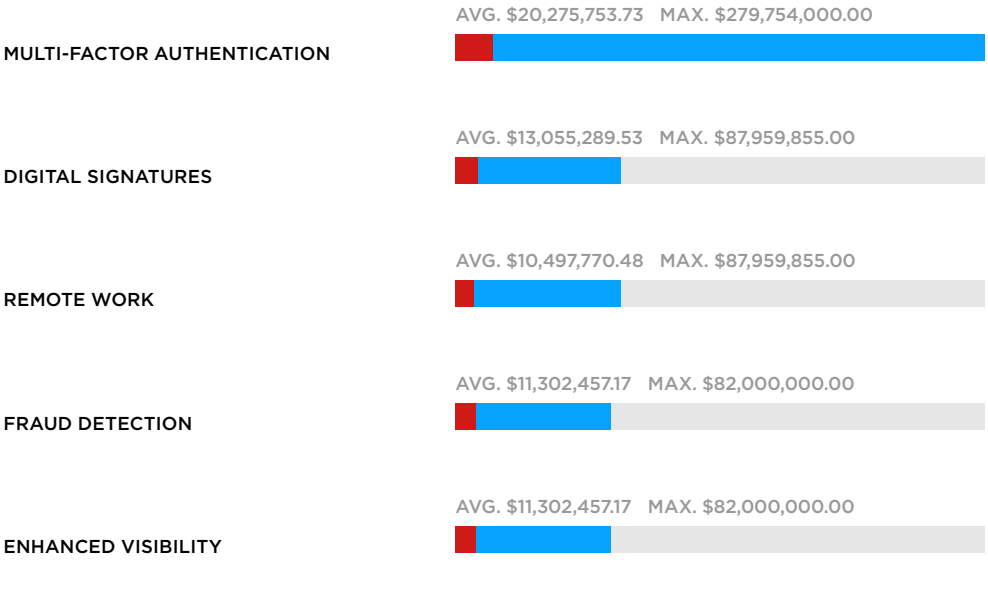
- The average funding of all companies covered in the cluster analysis is $13,286,746.00. The average minimum funding is $32,390.00, while the average maximum funding is $123,934,742.00.
- All the companies covered in the cluster analysis were founded between 1988 and 2020, with the average year of founding being 2016.
- Most of the companies (on average, 80 out of circa 200 in each cluster) are based in the United States. The second most common geographical locations are India and the UK.

Funding

Average funding recieved by the companies in the cluster

Maximum funding recieved by the companies in the cluster.

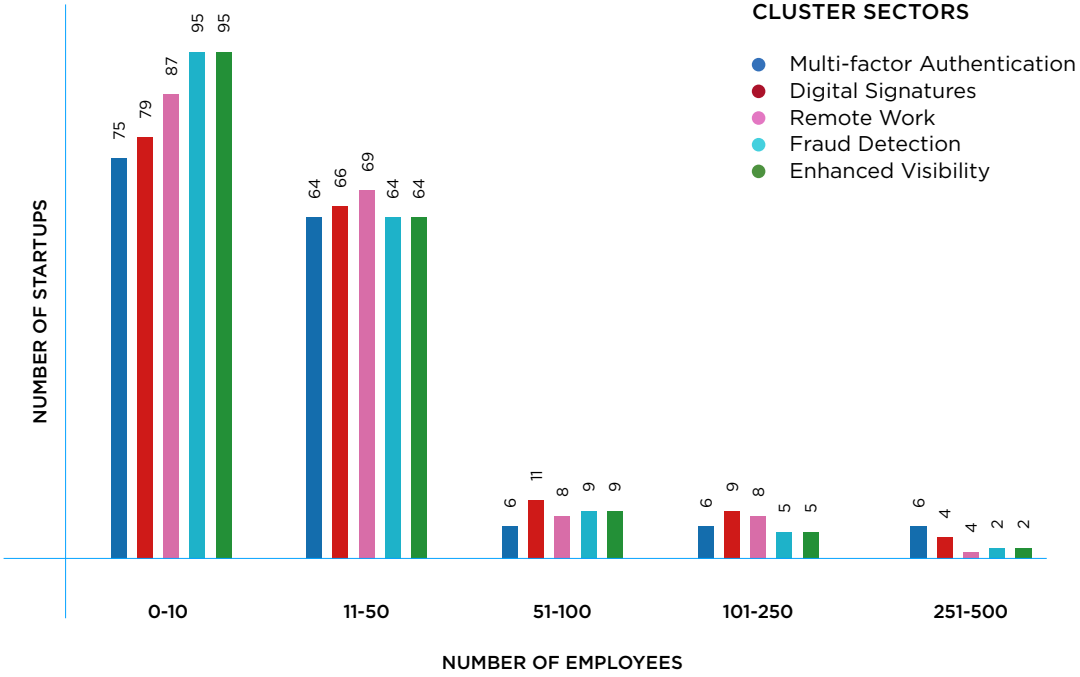
For reference, all numbers are compared to the largest funding sum ($279,754,000.00 in “Multi-factor Authentication”)



Year of inception

	MINIMUM YEAR OF FOUNDING	AVERAGE YEAR OF FOUNDING	MAXIMUM YEAR OF FOUNDING
Multi-factor Authentication	2000	2017	2020
Digital Signatures	1988	2016	2020
Remote Work	1992	2016	2020
Fraud Detection	2000	2016	2020
Enhanced Visibility	2000	2016	2020

Number of Employees



Geographical Distribution

Area	Most Frequent	Number of companies	Second Most Frequent	Number of companies	Third Most Frequent	Number of companies
Multi-factor Authentication	United States	**84**	Israel	**21**	United Kingdom	**17**
Digital Signatures	United States	**66**	India	**13**	Israel	**13**
Remote Work	United States	**84**	India	**15**	Canada	**14**
Fraud Detection	United States	**84**	India	**12**	United Kingdom	**12**
Enhanced Visibility	United States	**84**	India	**12**	United Kingdom	**12**

Data Summary for All Company Clusters

FUNDING

$279,75M
MAXIMUM

$13,286 M
AVERAGE

$7000
MINIMUM

YEAR OF FOUNDING

2020
MAXIMUM

2016
AVERAGE

1988
MINIMUM

NUMBER OF EMPLOYEES

0 - 10	50.59%
11 - 50	38.38%
51 - 100	5.05%
101 - 250	3.87%
251 - 500	2.11%

Five case studies of innovative companies

BLOCK ARMOUR

YEAR OF INCEPTION:	2017
LOCATION:	Singapore, Singapore & Mumbai, India
EMPLOYEES:	20
WEBSITE:	blockarmour.com

SECTORS	SUB SECTORS
Privacy & Security	Cyber Security
Information Technology	Network Security
	Cloud Security

IDEA | PRODUCT/ PROTOTYPE | GO TO MARKET | **GROWTH & EXPANSION** | ESTABLISHED

Executive Team

Narayan Neelakantan
Co-Founder & CEO

Narayan Neelakantan is an expert in IT security with nearly 20 years of experience in the field. He started his career at NSE.iT Limited as an Executive Engineer and after four years with the company, he went on to work for the National Stock Exchange of India (NSEI). There he held different roles, finally progressing to Head of IT Risk and Compliance. He left the NSEIT in 2016 in order to found Block Armour, where he serves as the company's CEO. Neelakantan holds a BE in Instrumentation from the University of Mumbai.

Abhijit Dhongade
Co-Founder & CTO

Abhijit Dhongade is a senior technologist with over 14 years of experience in cybersecurity. He previously headed the Security Operations Center (SOC) at India's National Stock Exchange. Dhongade graduated from the Mahatma Gandhi Mission College of Engineering and Technology, where he earned his BE in Information Technology, majoring in Information Security.

Floyd DCosta
Co-Founder

Floyd DCosta specializes in exploring use cases for distributed ledger technology in FinTech, RegTech, and cybersecurity. With a background in management consulting, he has over 19 years of international professional experience in setting up and growing enterprise business practices as well as advising senior client executives. His previous experience includes 11 years at Capgemini and spans a variety of industry sectors and technology platforms. DCosta holds a Masters in Computer Information Systems from ITM, Mumbai, and an Exec General Management Program from IIM-Bangalore.

Source: Adobe Stock Photos

Company Overview

Block Armour is a Singapore and Mumbai-based cybersecurity venture focused on harnessing emerging technologies such as blockchain to counter growing cybersecurity challenges in an efficient way. The startup was accelerated by Airbus and has developed a zero trust cybersecurity solution designed for today's hybrid and distributed IT environment. Its award-winning Secure Shield architecture enables holistic zero trust security for on-premise and cloud systems as well as connected devices in the Internet of Things (IoT) - all via a single integrated platform. The co-founders, Narayan Neelakantan, Floyd DCosta, and Abhijit Dhongade, are experts in the field of information security, cybersecurity, and business management, amassing nearly 50 years of combined industry experience.

Business Model

Block Armour operates on a B2B model, offering its products and services to organizations with both cloud-based and on-premise hosting. Its enterprise Secure Shield solution has been particularly successful in helping organizations provide secure and compliant remote access for employees working from home in "the new normal" post-Covid-19. Its client list ranges from oil and gas companies and manufacturers to BPOs and telcos. In terms of monetization, Block Armour generates revenue through licensing fees, the price of which is dependent on the scope of the project and is appraised by Block Armour. The company reported total revenue of $0.2 million in 2020.

Value Proposition

Block Armour offers a holistic solution for unified secure access with both server and application side protection, delivering integrated zero trust cybersecurity for on-premise as well as remote teams. They provide secure access from both enterprise and IoT devices through a single platform, which eliminates the need for investment in multiple point solutions like VPN for remote access and Network Access Control for on-premise networks. There is also no need for network hardware upgrades and no dependency on multiple vendor support personnel. Overall, this means a significant decrease in complexity and operational overhead, and a greater potential for return on investment.

Source: Adobe Stock Photos

Product Portfolio

Block Armour offers zero trust cybersecurity solutions for enterprise systems, cloud, as well as connected IoT devices. Their solutions are powered by Software Defined Perimeter (SDP) architecture and a private permissioned blockchain technology. The combination of these technologies securely "ring-fences" an organization's critical systems and provides secure access to authorized users and devices.

The solutions harness digital signatures—not just IP addresses—to identify, authenticate and authorize devices, thus making them well suited for today's distributed and hybrid enterprise IT ecosystems as well as smart city, Industry 4.0, and 5G security use cases.

Block Armour offers three products:

1. **IoT Armour:** a zero trust security platform for connected devices, integrated IoT systems, and communication networks;

2. **Secure Shield:** a zero trust cybersecurity platform for distributed and hybrid enterprise IT environments; and

3. **Digital Vault:** information encryption and server concealment storage platform.

Technology Overview

IoT Armour is a next-gen security solution created specifically for connected devices, integrated IoT systems, and related communication networks. IoT Armour uses digital signatures that are based on blockchain technology for correct identification, authentication, and authorization of the connected devices. It secures the core IoT systems, the devices, and the IoT communications network and delivers an enhanced Software Defined Perimeter (SDP) using private permissioned blockchain and Transport Layer Security (TLS) technology. SDP architecture hides core systems and IoT gateways, rendering them invisible to attackers, while customized agents along with private blockchain technology deliver a "new breed of digital identity" and access control for sensors and connected devices. By using decentralized blockchain architecture, IoT Armour makes sure that there are no points of failure and at the same time offers a scalable system for large IoT networks. IoT Armour's architecture is built around zero trust, therefore allowing micro-segmentation of connected devices as well as associated users. The platform facilitates access to resources and comprehensive management of the policy through its console. All access logs are stored on the blockchain, making it immutable and tamper-proof, thereby ensuring complete visibility in case an adversary should attempt to access the systems in an unauthorized manner or an administrator enforces an unauthorized change.

Block Armour's Secure Shield is a single-platform on-premise, Cloud, and connected IoT devices security solution, designed for distributed and hybrid enterprise IT environments. Secure Shield secures enterprise systems from a broad range of security threats. It provides security at a very fundamental level by cloaking vulnerabilities so that they cannot be exploited. It's integrated with 2-factor authentication, providing fine-grained, micro-segmented access and actively preventing the spread of malware and ransomware through the enterprise network. Similarly to IoT Armour, SDP architecture renders cloud and critical information systems invisible to attackers, and customized agents in conjunction with blockchain technology deliver a new breed of digital identity and access control for all users and devices. Secure Shield can be implemented in Microsoft's Azure Cloud and Amazon's AWS.

Source: Adobe Stock Photos

Digital Vault, Block Armour's final product, uses military-grade encryption and, with the help of blockchain technology, ensures the securing of sensitive information. The Digital Vault is capable of encrypting all of the stored content, and it also hides the server and uses blockchain signatures for the identification and authorization of the users. This allows organizations to thoroughly secure their networks while following regulatory requirements such as GDPR or HIPAA.

Market Opportunities

The rapid adoption of cloud technology, the proliferation of IoT, and the growing remote workforce resulted in highly distributed and hybrid IT ecosystems. Cyber attacks are on the rise and traditional tools like VPNs have been rendered ineffective in this new environment. Modern approaches like zero trust are swiftly becoming the preferred security paradigm for today's contemporary 'digital' enterprise.

According to a report by Markets and Markets, the global zero trust security market is projected to grow from $19.6 billion in 2020 to $51.6 billion by 2026, recording a CAGR of 17.4% over the forecast period. The major factors driving the market include the growing frequency of target-based cyber attacks and increasing regulations for data protection and information security.

Achievements and Future Plans

Block Armour records numerous successful use cases. One such example is the collaboration with Indian Oil Tanking LTD, a high-profile oil and gas distribution company, helping them in the transition towards remote working—a shift spurred on by the Covid-19 pandemic. Block Armour's client needed to enable remote access to a combination of on-premise and SaaS solutions to all employees while leveraging existing resources. Block Armour deployed its Secure Shield product to allow the employees to securely yet efficiently access the company's on-premise and cloud-based systems from home. As employees were accessing corporate applications through their personal computers, maximum security was enforced. As this client had relied on in-office access to business applications, Block Armour managed to enable a smooth transition to secure, application-based access for employees using their corporate and personal devices when working remotely.

Block Armour was also successful on the awards front. The company was a finalist at KPN's IoT 5G Challenge and NTT Startup Challenge 2020 and was named by Accenture among the Top 25 Cybersecurity Innovations worldwide. Additionally, they were listed among the Top 20 Global Cyber Security Startups for three consecutive years - 2017, 2018, and 2019. Block Armour has also been selected by the Tokyo Metropolitan Government for its support program to bring promising startups to Japan. Moreover, they have been selected to participate in the 2021 SelectUSA Investment Summit.

In the upcoming period, the company will remain focused on acquiring new customers and maintaining strong relationships with its partners, which include Airbus's BizLab, Capgemini, Microsoft, Accenture, Barclays, Google Cloud, and others. In a media mention, Narayan Neelakantan, CEO of Block Armour, commented:

"We are seeing a lot of traction for our solution since the beginning of 2019. Our approach is to acquire a few more strategic customers via direct sales and onboard partners to take our solution to market. This two-pronged approach will allow us to scale quickly and position our products to global clients. Our goal over the next five years is to become the preferred cybersecurity provider for critical infrastructure institutions and large enterprises."

CYBERCYTE

YEAR OF INCEPTION:	2019
LOCATION:	Reading, United Kingdom
EMPLOYEES:	7
WEBSITE:	cybercyte.com

SECTORS

- Information Technology
- Privacy & Security

SUB SECTORS

- Cloud Security
- Cyber Security
- Network Security

IDEA | PRODUCT/ PROTOTYPE | **GO TO MARKET** | GROWTH & EXPANSION | ESTABLISHED

Executive Team

Umut Yesilirmak
Founder & CEO

Umit Yesilirmak is an experienced professional in IT, project management, and consultancy services, having worked for a government agency as Head of IT and led four big government IT projects for 11 years. His professional experience also includes managing Bilgikent Information Technologies AS and consulting the World Bank in the field of establishing IT frameworks for National Social Security Systems. Yesilirmak holds a BSc and a Master's degree in Computer Engineering.

Necati Ertugrul
Founder & CSO

Necati Ertugrul brings more than 20 years of experience in cybersecurity, having previously founded MAY Cyber, the most prominent cybersecurity vendor in Turkey, where he led the company's R&D Division and product strategy. Before that, he held technical and managerial roles at Finansbank and TUBITAK. Ertugrul holds a BSc in Electrical-Electronic Engineering from the Middle East Technical University and an MBA from Marmara University.

Source: Adobe Stock Photos

Company Overview

—

CyberCyte is a UK-based cybersecurity company developing a unified platform to provide a framework based on the concept of Circle of Zero Trust for enabling 360° Security for organizations. The platform named CloudCyte is an innovative SaaS cloud platform that empowers organizations and MSSPs to solve emerging challenges in cybersecurity services through an integrated technology stack.

Business Model

CyberCyte develops B2B cybersecurity solutions that provide powerful support for an enterprise's cyber resilience strategy. Their SaaS-based solution, CloudCyte, powered by machine learning-based user behavior analytics, allows clients to gain real-time cyber threat intel and help build resilience against cyber breaches and hacks. The company provides a free trial of all CloudCyte's features for thirty days.

Value Proposition

Cybersecurity breaches force the community to upgrade existing malware detection and mitigation solutions as most of them require a longer time to identify breaches. To overcome this challenge, CyberCyte developed its platform CloudCyte. CloudCyte is a zero trust security platform to identify and block the hidden cyber threats bypassing the security infrastructure. It discovers the relationships between users, devices, and applications with the external world and how they interact. For faster and more accurate threat discovery, CloudCyte provides a simpler and rapidly scalable solution designed inside an AI platform for unmatched threat visibility.

Source: Adobe Stock Photos

Product Portfolio

CyberCyte is completely focused on CloudCyte, a multi-tenant, containerized SaaS platform for protecting users, networks, and applications from cyber threats. The platform allows organizations and MSSPs to deploy the solution on-premise or any cloud platform in minutes. The platform identifies the hidden cyber threats bypassing the security infrastructure by auditing every connection from end-users, applications, and devices to identify any unidentified communication attempt. The CloudCyte system offers two major modules: DefCyte and DNSCyte.

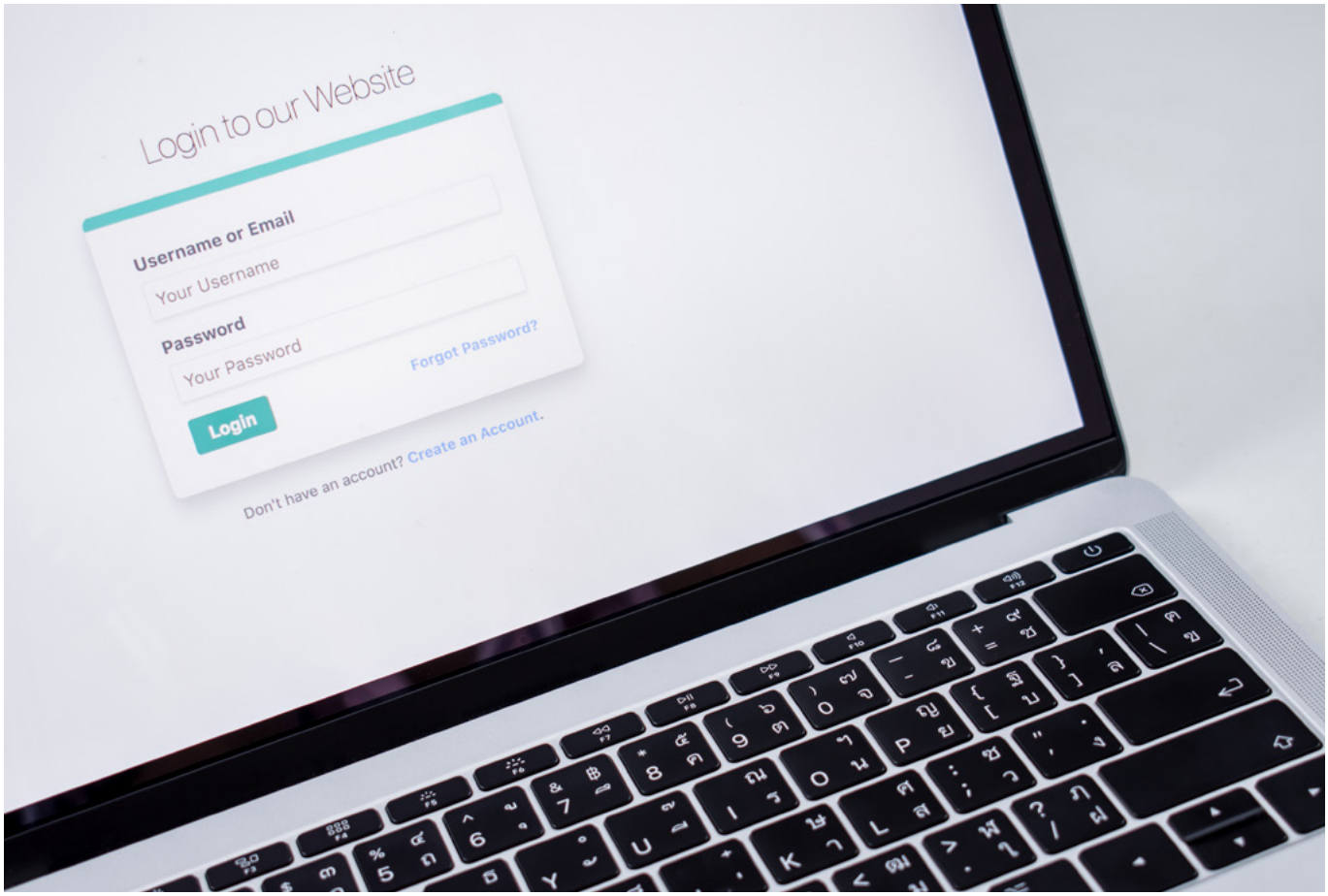
Technology Overview

Identification of cyber espionage, malicious data exfiltration, and zero-day attacks are the key focus areas of CyberCyte's cybersecurity solutions. Their main offering is the CloudCyte threat protection platform, which comprises two features: a secure DNS Service that blocks threats and targeted attacks in real-time and e-mail phishing detection and inbox security feature. CloudCyte offers 360° security for end-users by securing all communication for e-mail and Internet access, coupled with tools to increase end-user awareness. Both features are also available as stand-alone products.

Phishing attacks continue to play a dominant role in the digital threat landscape, and according to Deloitte, 91% of all cyberattacks begin with a phishing email to an unexpected victim. CyberCyte addresses this emerging cyber threat with the DefCyte module, a GDPR compliant email phishing detection and inbox security solution. Based on the CloudCyte platform, DefCyte provides a complete view of threats arising from phishing attacks using machine learning-based classification algorithms. DefCyte identifies phishing attacks that bypass the existing security controls by performing advanced metadata analyses involving extracting domain and matched keywords from email header and body. Additionally, it enables users to report malicious emails, and if flagged as malicious, the email is deleted from all user mailboxes. Some additional technical features include easy deployment through Office 365 and Microsoft Exchange, complete GDPR compliance and built-in templates for phishing attacks, simulations, and user awareness training.

The continuing evolution of cyber threats is overcoming traditional cyber defenses. Domain Name System (DNS) adds a layer of network security to any system, and with the DNSCyte module, organizations can be sure that any malicious activity will be blocked. DNSCyte has indexed 99.9% of the Internet, which includes more than 1.7 billion websites and 350 million

Source: Adobe Stock Photos



top-level domains growing daily. The system monitors and controls Internet access for the entire enterprise and enables secure Internet browsing while protecting from malicious software like ransomware, C&C, spyware, etc. In case of infiltration, infected users are quarantined, and their access to the network is blocked. On a more technical note, DNSCyte is deployable in minutes without modifying the existing physical infrastructure.

With the number of IoT-connected devices growing, the amount of personal data that can be compromised is beyond imagination. CloudCyte offers total control of every device's infrastructure and total visibility in the network as a network access control solution. It enables 100% accurate discovery, classification, and profiling of any device, involving advanced agentless threat analytics, port scans detections, unauthorized password discovery, and audit data tracking.

Market Opportunities

Globally, businesses are experiencing increased cyberattack volumes, and higher breach levels as attacks continue to grow in sophistication and complexity. According to Gartner's 2021 CIO Agenda Survey, cybersecurity was the top priority for new spending. The report states that 61% of the more than 2,000 CIOs surveyed have increased investment in cyber/information security this year and emphasize the need for zero trust security measures for protection against cyber-attacks.

The zero trust security market has experienced considerable growth in the previous. According to Markets and Markets, it is projected to reach $51.6 billion by 2026, registering a CAGR of 17.4% from 2020 to 2026. The report states the growing frequency of target-based cyber attacks and the high demand for improved visibility due to the rise in IoT traffic among enterprises as the main drivers of the market.

Achievements and Future Plans

The founders of CyberCyte have transferred their experience from their previous cybersecurity company which had more than 250 employees. Its customers included major international banks, enterprises, and government agencies. With its promise to efficiently verify the trustworthiness of every device, user, and application in an enterprise, CyberCyte plans to continue delivering high-quality services in the cybersecurity landscape, helping organizations in their journey to achieving zero trust. For that matter, the company has launched the CloudCyte platform, which became commercially effective from May 2021.

ELISITY

YEAR OF INCEPTION:	2018
LOCATION:	San Jose, CA, United States
FUNDING:	7,500,000 USD
EMPLOYEES:	28
WEBSITE:	elisity.com

SECTORS	SUB SECTORS
Information Technology	Cloud Security
Privacy & Security	Cyber Security

IDEA | PRODUCT/ PROTOTYPE | **GO TO MARKET** | GROWTH & EXPANSION | ESTABLISHED

Executive Team

James Winebrenner
CEO

James Winebrenner has a strong background in go-to-market network and security infrastructure and brings over 20 years of experience in building and scaling companies. He has held several executive roles in companies such as Viptela, where he led the go-to-market strategy from pre-launch through the sale to Cisco in 2017. Moreover, he held various managerial positions at Cisco Systems and served as Technical Marketing Engineer at Check Point Software.

Source: Adobe Stock Photos

Company Overview

Elisity is a software company developing enterprise edge security solutions that redefine security and access, allowing companies to protect their assets and data proactively. The company was founded in 2018 by Burjiz Pithawala, Sundher Narayan, and Srinivas Sardar, with James Winebrenner as its CEO. Currently, the company is headquartered in San Jose, California, and employs a staff of 28.

Business Model

Elisity has developed a solution for enterprises from various industries such as pharmaceuticals, manufacturing, healthcare, and financial services for cost savings, time savings, and risk mitigation. Instead of relying on various software to protect access to their assets, companies that use Elisity's product can use an end-to-end solution that helps them transition to zero trust across their digital footprint.

Value Proposition

Elisity's Cognitive Trust platform contextualizes identity, environment, and behavior, allowing companies to connect all of their assets across every domain securely. The vendor-agnostic platform is built for seamless integration, and it provides consistent policy across brownfield and greenfield edge and multi-cloud environments. Additionally, it includes continually evolving risk policy enforcement for all assets.

The company's solution detaches the security access policy mechanisms from the underlying network constructs and allows them to be defined based on identity and context rather than location. Additionally, Cognitive Trust will enable users to gain complete visibility to asset behavior, thereby observing and continually optimizing policy. The policy enforcement is backed by intelligence uncovered by the continuous monitoring of all access. Furthermore, the platform enables companies to control traffic flows with precision and efficiency and manage policy from a single, cloud-delivered portal.

Source: Adobe Stock Photos

Product Portfolio

Elisity's AI-powered Cognitive Trust combines software-defined perimeter capabilities and zero-trust network access to solve the challenge of securing access to enterprise assets and enterprise data. The company's Cognitive Trust product suite comprises three solutions:

1. **Cognitive Trust for Workforce Anywhere** provides smart zero trust access for users, apps, data, and devices in the data center or the cloud.

2. **Cognitive Trust for Connected Devices** provides secure convergence of IT and OT through identity-based and context-aware access to nano-segmented industrial environments.

3. **Cognitive Trust for the Distributed Enterprise** provides universal identity-based visibility and access policy across cloud, data center, campus, and branch.

Technology Overview

Elisity's Cognitive Trust for Workforce Anywhere provides security by granting least-privilege access to any user without compromising user experience and network performance. Besides relying on the user's identity and their device, this solution takes into account attributes and contexts such as time of day, geolocation, and device security posture. On top of that, the solution dynamically modifies trust, depending on the behavior over time.

Cognitive Trust for Workforce Anywhere is a scalable solution with full deep packet inspection (DPI) and security analytics, allowing enterprises to gain total visibility of all flows, device inventory with API connectors, and immediate recognition of unusual activity. This solution consolidates and simplifies the workflow by replacing some ACLs, firewalls, VRFs, IAMs, VLANs, and VPNs. Additionally, it allows for faster detection and reaction to anomalies early in the attacker's kill chain. This is made possible by integrating policy management with Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) tools to prevent data exfiltration and malware injection.

The second solution, Cognitive Trust for Connected Devices, provides a security structure on top of the existing brownfield OT infrastructure. It continuously monitors all access and recommends policies based on risk and vulnerability. This allows users to have complete real-time visibility into all OT users, devices, and applications. The solutions can increase the enterprise's overall cybersecurity strength without disrupting user productivity and business operations.

This solution ensures that no OT devices or applications have direct outside visibility. It provides identity-based access and nano-segmentation with an ISC Systems Segmentation integration option for vulnerable OT systems and devices. Additionally, it offers end-to-end encryption and AI-powered policy recommendations.

The third solution, Cognitive Trust for the Distributed Enterprise, combines identity-based segmentation, Zero Trust Network Access (ZTNA), and an AI-enabled Software-Defined Perimeter (SDP). It allows enterprises to create, manage, and scale policy across every domain without inter-domain policy translators.

The solution, which does not interfere with network operations and performance, ensures that enterprises have a cost-effective way of overcoming the traditional solutions' limitations. For example, the nano-segmentation of users, apps, devices, and data prevents lateral movement in the event of a breach. Furthermore, it allows enterprises to verify North-South and East-West network flows for anomalies continuously.

Elisity's solutions are composed of several components: Elisity Cloud Control Center, Elisity Edge, Elisity Access Service, and Elisity Connect. Elisity Edge subdivides into Elisity Edge, Elisity Edge Cloud, and Elisity Micro Edge.

Source: Adobe Stock Photos

The Cloud Control Center is a centralized, cloud-delivered platform with an AI layer that provides policy recommendations based on risk monitoring of all remote assets. Moreover, this platform pushes policies "just-in-time" and manages routing context via a control plane.

The second component, Elisity Edge (plus Elisity Edge Cloud and Elisity Micro Edge) functions as the IT/OT Access Edge and SDP Gateway. It also serves as the Policy Enforcement Point (PEP) of distributed policy. The typical Elisity Edge consists of an Elisity edge appliance or a virtual appliance. Elisity Edge Cloud provides site-to-cloud and cloud-to-cloud secure connectivity. Elisity Micro Edge installed on third-party switches enables identity-based segmentation and policies on those switches, turning them into SDP gateways in addition to enabling OT transactional segmentation.

The next component, Elisity Access Service, is a cloud-delivered service that can be integrated with data loss prevention (DLP), firewall-as-a-service (FWaaS), and threat prevention capabilities, among others. It ensures a secure connection between users and resources globally. Elisity Cloud Control Center, along with Elisity Access Service, enables Single Packet Authorization and Session-based Continuous Identity Verification to enable air-gapped security for enterprises.

Last but not least, Elisity Connect is the component that provides least-privilege zero trust access by initiating secure connections directly between the remote user's device and enterprise resources through Elisity Access Service.

Market Opportunities

According to a 2020 report by IBM, the average cost of a data breach is $3.86 million, with lost business costs being the largest contributing cost factor with a value of $1.52 million. Additionally, IBM reported that the average time to identify and contain the data breach is 280 days. Elisity has identified this problem and is continuously working on *"solving the challenge of securing access to enterprise assets and enterprise data in the complex modern world of blurring enterprise boundaries, the proliferation of cloud, connected devices, and mobile workforces."*

Market-wise, the trend for stronger cybersecurity is becoming more apparent. A report by Markets and Markets concludes that the zero trust security market is projected to grow from $19.6 billion in 2020 to $51.6 billion by 2026, registering a CAGR of 17.4% from 2020 to 2026. Among the key market drivers are the growing frequency of target-based cyber attacks and the high demand for improved visibility due to the rise in IoT traffic among enterprises.

Achievements and Future Plans

Elisity launched its Cognitive Trust solution in August 2020. This move was backed by $7.5 million in seed funding from Atlantic Bridge to assist Elisity in scaling its engineering, sales, and marketing teams.

"We believe the approach Elisity is putting forward for enterprise security makes them uniquely positioned to radically change how customers access and protect their data," said Brian Long, co-founder and Managing Partner at Atlantic Bridge. *"Transforming this market by delivering the technology to transform organizations to lean trust and protect them from accidentally exposing access to critical apps, either in the cloud or on-premises, is a big opportunity and will continue to grow."*

The company has already acquired several customers, such as GSK Consumer Healthcare. Elisity continues to lead the co-development of the Cognitive Trust platform and plans to scale to the broader enterprise market. Besides investing in its engineering team, Elisity intends to expand its sales and customer success functions and enable increased enterprise adoption.

SILVERFORT

YEAR OF INCEPTION:	2016
LOCATION:	Tel Aviv, Israel
FUNDING:	41,500,000 USD
EMPLOYEES:	78
WEBSITE:	silverfort.com

SECTORS	SUB SECTORS
Privacy & Security	Cyber Security
Information Technology	Network Security
	Cloud Security

IDEA | PRODUCT/ PROTOTYPE | GO TO MARKET | **GROWTH & EXPANSION** | ESTABLISHED

Executive Team

Hed Kovetz
Co-Founder & CEO

Hed Kovetz started his career as a Research Team and Group Leader for the Israeli Intelligence Corps, later becoming a Research Assistant at Tel Aviv University. Following this, he worked as a Cybersecurity Product Manager at Verint before co-founding Silverfort in 2016 and becoming CEO in 2017. Kovetz holds a Bachelor of Laws degree from Tel Aviv University.

Matan Fattal
Co-Founder & President

Prior to Silverfort, Mattan Fattal worked as an Algorithmic Researcher for Intucell, a Software Engineer for Intel, and conducted Algorithmic Research for the Israel Defense Forces. He has completed his studies for an MSc in Mathematics and holds a BSc in Abstract Mathematics from Bar-Ilan University.

Yaron Kassner, PhD
Co-Founder & CTO

Yaron Kassner holds a BSc in Applied Mathematics from Bar-Ilan University and an MSc and a PhD in Computer Science from Technion, the Israeli Institute of Technology. He began his career as a Team Leader, working for the IDF, later becoming a Software Development Engineer Intern at Microsoft. Following this, Yaron Kassner worked as a Data Science Consultant at Cisco before co-founding Silverfort and serving as the company's CTO.

Source: Adobe Stock Photos

Company Overview

Silverfort is a cybersecurity company based in Tel Aviv, Israel, with additional offices in Singapore, Belgium, and the USA. It provides a Unified Identity Protection Platform featuring advanced zero trust security with Multi-factor authentication (MFA). The company was founded in 2016 by Matan Fattal, Hed Kovetz, and Yaron Kassner, experts in security, mathematics, and software engineering.

Business Model

Silverfort operates on a B2B model, partnering with and offering its services to various clients, including identity and PAM providers, MFA providers, cloud providers, threat detection and risk analysis providers, security solution providers, and MSPs. The company provides access to its platform as a SaaS or VM, with no scale limitations or impact on productivity. Silverfort targets small companies and large enterprises alike, avoiding any modifications to existing assets and infrastructure. Moreover, the company offers comprehensive training and support for its partners and helps them develop their business.

Value Proposition

Based on its patent-pending technology, Silverfort provides risk-based Multi-factor authentication aimed at sensitive users, devices, and resources, including previously unprotected systems such as homegrown applications, IT infrastructure, file systems, machine-to-machine access, etc. The solution allows organizations to prevent data breaches and achieve compliance by preventing identity-based attacks across complex, dynamic networks and cloud environments. Rather than protecting assets one by one, this enables the company to provide a unified authentication and access system, covering all users, assets, and environments, with on-premise and in-cloud applications. Moreover, by restricting MFA requests to sensitive and high-risk situations, Silverfort enhances the user experience and reduces disruptions.

Source: Adobe Stock Photos

Product Portfolio

Silverfort offers a zero trust authentication platform for enterprises and SMEs, delivering strong authentication across entire corporate and industrial networks and cloud environments. The solution doesn't require any modifications to endpoints and servers and can monitor authentication and access requests without agents or proxies. Moreover, Silverfort enables clients to perform a holistic and continuous AI-driven risk analysis and a non-intrusive analysis of encrypted authentication protocols.

Technology Overview

Using an AI-driven Risk Engine, Silverfort can analyze user behavior to apply MFA and access policies accurately. The system is intended as a holistic and non-intrusive solution for secure authentication and access in enterprise networks and cloud settings. By adding a layer of security on top of existing authentication protocols, it eliminates the need to deploy agents and proxies or modify existing servers and applications. The authentication system can also be integrated with third-party threat indicators, including Palo Alto Networks, Check Point, and Microsoft.

Furthermore, the Next-Generation Authentication Platform incorporates agentless MFA technology that seamlessly enforces zero trust for applications in corporate, industrial, and cloud settings. The system also monitors network traffic for all access requests. It enforces secure authentication policies as needed, leveraging native features of existing IAM infrastructure and authentication protocols such as LDAP/S, Kerberos, NTLM, OpenID Connect, RADIUS, and others.

Unlike traditional MFA solutions, which are typically implemented for specific systems (such as VPN gateways and web applications), Silverfort's architecture ensures secure access to any system, regardless of location or type. This includes machine-to-machine, user-to-machine, and administrative access. Furthermore, Silverfort avoids any modifications to existing assets and infrastructure, allowing small agile companies and large traditional enterprises to achieve zero trust security throughout their networks.

Silverfort's innovative technology protects any access, regardless of the interface or access tool used. As opposed to conventional MFA solutions that serve to protect only specific server interfaces such as RDP or SSH, Silverfort works to block access from tools such as Remote PowerShell, PsExec, Remote Computer Management, file share access, etc. This enables the system to protect against hacking tools such as Mimikatz, which use these interfaces to perform lateral movement (for example, using Pass-the-Hash).

Moreover, Silverfort's platform monitors all human and machine access requests across all systems and environments, continuously analyzing risk and trust levels in real-time, applying adaptive risk-based authentication policies, and preventing unauthorized access to any sensitive asset.

Source: Adobe Stock Photos

Market Opportunities

The instances of massive cyberattacks are increasing globally. Cyber terrorists attack endpoints, networks, data, and other IT infrastructures, leading to substantial financial losses to individuals, enterprises, and governments. For example, the consequences of the 2018 SamSam ransomware included inaccessibility to multiple municipal services, data leakage, and financial loss. Such attacks are common in the healthcare, government, and education industry.

This environment necessitates the development of solutions such as Silverfort, boosting the global cybersecurity market. According to a report by Grand View Research, the global cybersecurity market is expected to grow from $167.13 billion in 2020 to $372.04 billion in 2028, at a CAGR of 10.9% from 2021 to 2028. The main factor driving the market is the growing sophistication, frequency, and intensity of cyberattacks.

Achievements and Future Plans

Over the years, Silverfort has received numerous awards and accolades, being recognized as an innovator in the cybersecurity sector. Notably, in 2019, the company was named a Gartner *"Cool Vendor,"* a 2019 *"FireStarter"* by 451 Research, and a CNBC *"Upstart 100."* Silverfort was also named Most Promising Cybersecurity Startup of the Year 2020 by Cyber Defense Magazine, the Best of MFA 2021 by Expert Insights, and was announced as a finalist for the 2021 Microsoft Security 20/20 Identity Trailblazer.

Moreover, in April 2021, Silverfort reported that its researchers have discovered a KDC spoofing vulnerability in F5 Big-IP, the fourth vulnerability that the company discovered. Prior to this, in 2020, Silverfort revealed three other vulnerabilities, which were subsequently patched.

The company has also attracted investor interest, raising over $41.5 million to date. Its latest investment came in August 2020, raising a $30 million Series B funding round led by Aspect Ventures, with participation from Citi Ventures, Maor Investments, TLV Partners, StageOne Ventures, and Singtel Innov8.

SPIDEROAK

YEAR OF INCEPTION:	2006
LOCATION:	Mission, KS, United States
FUNDING:	15,791,828 USD
EMPLOYEES:	35
WEBSITE:	spideroak.com

SECTORS	SUB SECTORS
Privacy & Security	Cyber Security
Information Technology	Network Security
	Cloud Security

IDEA | PRODUCT/ PROTOTYPE | GO TO MARKET | **GROWTH & EXPANSION** | ESTABLISHED

Executive Team

Dave Pearah
CEO

Dave Pearah's professional experience consists of several C-level and advisory positions. Some of the most notable ones are his position as CEO and Board Chairman at the HDF Group and CTO at Cision. Alongside his role at SpiderOak, Pearah is also an Advisory Board Member at Markit Medical and Accelerance. He holds a BS in Computer Engineering and Latin American Studies from the University of Illinois Urbana-Champaign and two MSc degrees in Technology Management and Computer Engineering from MIT.

Jonathan Moore
CTO

Jonathan Moore is an experienced software engineer with over 25 years of experience developing solutions for diverse applications. Prior to SpiderOak, he served as Software Engineering Lead at Driver, Software Architect at Planet Labs, and VP Engineering at Addvocate, among others.

Source: Adobe Stock Photos

Company Overview

SpiderOak is a US-based company headquartered in Kansas City that provides compliance, security, and usability software solutions. The company was founded in 2006, starting as a provider of end-to-end encrypted cloud storage and file hosting solutions. Over the years, its portfolio increased substantially, focusing on developing and providing security and privacy technology.

Business Model

SpiderOak operates using a combined B2C, B2B, and B2G business model, primarily targeting clients in the legal, banking, healthcare, and life science sectors. Recently, the company has launched an ongoing expansion into the government market, developing solutions aimed at defense and intelligence, civilians, contractors, and space applications. In terms of revenue, SpiderOak offers its solutions through a SaaS-based model, which includes subscriptions for regular consumers and tailored contracts for large enterprises and government clients.

Value Proposition

SpiderOak's solutions are built with security in mind, with the company employing a design philosophy centered on data protection. This is emphasized through its zero trust architecture that is utilized across the company's entire portfolio of solutions. Through this approach, no user of SpiderOak's products is trusted, both internally and externally. As a result, it eliminates inside threats, permission creep, and unintentional exposure.

Furthermore, the company uses blockchain to ensure integrity, which provides complete attribution and non-repudiation of all data transactions. Using this method, every change made to the ledger is digitally time-stamped and signed, ensuring full traceability and integrity. Thus, by utilizing both zero trust no knowledge encryption and distributed ledger technologies, SpiderOak facilitates the development of virtual collaborative environments for datasets that were previously considered too sensitive.

Source: Adobe Stock Photos

Product Portfolio

Through its offering, SpiderOak provides dedicated and custom security software solutions to a wide range of clients. Its portfolio includes:

1. **CrossClave,** complete zero trust communication and collaboration suite intended to provide speed, ease of access, and security.

2. **OrbitSecure,** agile and secure communications for managing spacecraft, payloads, and other forms of space assets.

3. **One Backup,** end-to-end encrypted cloud storage and file-sharing tool that can sync across all popular devices and platforms.

4. **SpiderOak Platform,** a secure software platform that facilitates the development of cryptographically secure software in business-critical environments.

Aside from these, the company also develops custom cybersecurity solutions based on the client's needs, including providing zero trust functionality.

Technology Overview

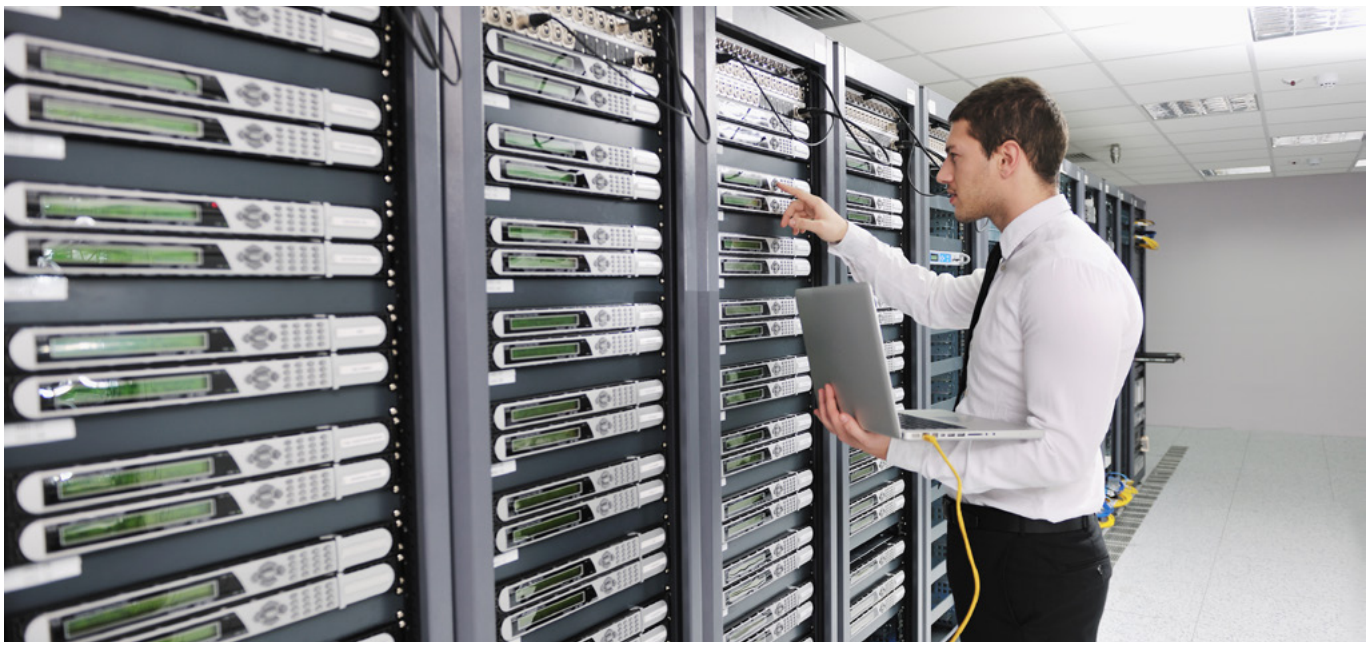
SpiderOak offers a range of solutions for clients that need to securely and swiftly communicate and protect their data.

For example, its secure remote telework solution is intended as the gatekeeper to the world of networks for organizations dealing with sensitive information that can't be exposed to risk. The solution incorporates zero trust principles to enable forced need-to-know, which guarantees that valuable information assets remain safe and secure, regardless of where they're created or accessed. The system is designed to de-trust the network, servers, and administrators, protecting its clients' data regardless of location. This is achieved by using key management for identity, blockchain for irrefutable authority, a policy engine for managing roles and attribute-based controls, and end-to-end encryption for data. These features are available in a lightweight package installed on-premises or via AWS servers, with the solution only requiring client software to be installed on the user devices.

Next, the secure multinational collaboration system is designed to meet the global companies' exact security needs and requirements. It manages the confidentiality, integrity, and availability of strategic data assets and communications as they traverse the global communications network. To this end, the solution leverages Distributed Ledger and No Knowledge Encryption, ensuring the confidentiality of the used data sources. This approach provides confidentiality, integrity, and availability for its client's virtual communications and collaborations. Furthermore, users can share any file type, message, or voice call with SpiderOak's team, all with the same level of security and without any loss in performance. The solution is built on the SpiderOak Platform, which allows it to be easily deployed to any device in less than thirty minutes, on-premises, or hosted as a service.

The company also offers the Secure Intellectual Property Sharing solution, designed per application to protect the intellectual property

Source: Adobe Stock Photos



during transit between secure endpoints. The company relies heavily on the zero trust model, using coded messages that can only be read/decoded by a shared key that identifies the target users with the correct permissions. Moreover, if an outside user acquires the key and the message, it would be useless, as they're not bound to a user external to the negotiation. Thus, each user's data is protected regardless of the security of the working infrastructure. Additional features include an irrefutable ledger of events for detecting mismatched data, a safety net to prevent users from wrongly sharing information, and a programmable policy engine that provides technological enforcement for various data security requirements and regulations.

Market Opportunities

Driven by the rapid growth of the Internet and digital tools over the past two decades, cybersecurity also evolved to respond to the changing environment. With cybercrime attacks such as identity thefts and data ransomware rising considerably, an opportunity has emerged for companies to provide innovative solutions to address these challenges. This development is further fueled by the lack of security companies implement. One study from Yahoo Finance shows that nearly 80% of senior IT and IT security leaders believe that their organizations lack sufficient protection against cyberattacks.

Companies such as SpiderOak are utilizing this gap, providing a wide range of solutions that address customers' security challenges. According to Grand View Research, the global cybersecurity market was valued at $161.13 billion in 2020 and is expected to reach $372.04 billion by 2028, at a CAGR of 10.9%. The market is driven by the increase in the number and intensity of data breaches across enterprise networks.

Achievements and Future Plans

As part of its ongoing expansion into the government market targeting DoD and intelligence clients, in March 2021, SpiderOak won a Small Business Innovation Research (SBIR) contract to adapt its OrbitSecure protocol to meet critical military needs.

"This contract is a key waypoint in the evolution of our company and our success in space. We see this as a vote of confidence in our technology by the Air Force, and the chance to demonstrate that success in military applications will follow our recent advances with commercial clients. Satellites and space travel are poised to expand dramatically and we expect that our software will play a major role in this new world," explains Michael Campanelli, VP of Federal at SpiderOak.

Prior to this, SpiderOak established its Federal Advisory Board, consisting of experienced leaders from civilian, defense, and intelligence agencies, to help the company align its CrossClave and other solutions with government requirements.

Moreover, in July 2020, SpiderOak reached an agreement with Carahsoft Technology, which will act as the master government aggregator of SpiderOak's suite of products. As part of the deal, Carahsoft will offer the CrossClave file sharing platform through its reseller network and its spot on NASA's Solutions for Enterprise-Wide Procurement V vehicle.