darkpools

October 2026



Company profile 2026

See threats sooner, stop financial crime and keep critical systems secure

One accountable partner for intelligence, fraud and cybersecurity, for governments, financial institutions and the organisations that serve them.

Gov AI
Intelligence for government

FinCrimes
Fraud and anti-money laundering

Cybersecurity
Security products and services

Executive summary

Capability that protects the public, customers and critical systems

Who we are

Dark Pools is a South African technology company, founded in Cape Town in 2021, with offices in Johannesburg and Manzini and a company in the United States. We build software and run security services for governments, banks, insurers and enterprises.

What we sell

Three lines of business. Gov AI gives government agencies one picture across every intelligence source. FinCrimes detects fraud and money laundering before money moves and prepares the reports regulators require. Our cybersecurity business sells privileged-access and password products and runs a 24/7 security operations centre, testing, forensics and advisory services.

Why clients choose us

Clients get one accountable partner instead of several vendors, keep their data on infrastructure they control, and receive findings they can defend. We are built for Southern Africa, monitoring in local languages and covering mobile money, and we are a B-BBEE Level 1 contributor.

Who relies on us

The Presidency, the State Security Agency, the Electoral Commission of South Africa, SACNASP, Cell C, Sage and Gap Infrastructure Corporation. Virtueda Systems distributes our products and partners with us on services.

At a glance

2021 Founded in Cape Town	4 Offices in Cape Town, Johannesburg, Manzini and Dover
3 Companies: South Africa, Eswatini, United States	7 Named clients in government and industry
24/7 Security operations centre	Level 1 B-BBEE contributor

In this profile

The challenge	03
What we sell	04
Gov AI	05
FinCrimes	06
Cybersecurity	07
Why Dark Pools	08
Track record	09
Working with us	10
Our company	11

Our business proposition

Dark Pools sells the capability institutions need to protect the public, their customers and their own systems, delivered by one team and run on infrastructure the client controls.

One partner

Intelligence, financial-crime and security work from one accountable team, so nothing falls between vendors.

Your data, your control

Deployed on-premises, in government cloud or hybrid, including isolated networks. Sensitive records never have to leave your boundary.

Decisions you can defend

Every alert and assessment shows the evidence behind it, so boards, regulators and courts can see the reasons behind it.

01 The challenge

The risks our clients carry

Governments, financial institutions and the organisations that run critical systems face threats that move faster than their tools and teams. These are the problems they bring to us.

Governments and agencies

Threats move faster than teams can watch
Narratives and threats spread across platforms and languages, and are often seen late.

Intelligence sits in separate systems
Leaders wait while analysts piece together reporting from different tools.

Every response is a public act
Official responses need approval and a record of who decided what.

Data must stay in government hands
Sensitive records cannot leave government infrastructure.

At stake
Late warning, weaker decisions and loss of public trust.

Banks, insurers and mobile-money operators

Fraud moves faster than daily reviews
Mule accounts, SIM-swap takeovers and card attacks play out in minutes.

Organised rings look like ordinary customers
The links between accounts and claims only show when they are joined up.

Alerts that cannot explain themselves
Examiners question alerts that analysts cannot justify.

Reporting takes too long
Teams rebuild evidence by hand before they can file.

At stake
Direct losses, regulatory findings and reputational damage.

Enterprises and public-sector IT

Attacks do not keep office hours
Few organisations can staff a security watch at night and over weekends.

Too many people hold the keys
Shared administrator passwords and forgotten supplier access go unchecked.

Weaknesses are found too late
Gaps surface after an incident rather than before it.

Security leadership is hard to hire
Not every organisation needs or can recruit a full-time security chief.

At stake
Breaches, downtime, audit findings and data-protection exposure.

Our answer

Gov AI
One picture across every source and language, early warning, and responses with a named approver.

FinCrimes
Decisions before money moves, the whole network in one case, and reports ready for the regulator.

Cybersecurity
A 24/7 watch, control of privileged access, weaknesses found first and security leadership on demand.

02 What we sell

Three lines of business, one accountable partner

Each line of business can be bought on its own. Clients who take more than one get a single team, one security baseline and one point of accountability.

Intelligence for government

Gov AI

Turn scattered intelligence into decisions leaders can act on

What we sell

- Intelligence fusion
- Social media and messaging intelligence
- Open-source investigations
- Counter-disinformation
- Digital vetting
- Assessments and briefings

Bought by

- Presidency and cabinet offices
- Intelligence and security agencies
- Police and defence
- Electoral bodies and regulators

Fraud and anti-money laundering

FinCrimes

Stop fraud and money laundering before the money moves

What we sell

- Real-time fraud and AML detection
- Investigations and case management
- Regulatory reporting
- Insurance claims fraud
- Supply chain fraud detection
- Oversight for regulators
- Revenue leakage detection for tax authorities

Bought by

- Banks and payment providers
- Insurers and special investigations units
- Mobile-money and remittance operators
- Central banks, regulators and financial intelligence units
- Tax and customs authorities

Security products and services

Cybersecurity

Keep critical systems secure, around the clock

What we sell

- KeyCare Pass password management
- 24/7 security operations centre
- Penetration testing and vulnerability management
- Digital forensics
- vCISO, architecture and cloud security

Bought by

- Chief information and security officers
- Government departments
- Banks, insurers and telecoms
- Organisations without a security night shift

Side by side

	Gov AI	FinCrimes	Cybersecurity
The business problem	Agencies hold intelligence in separate systems and monitor in too few languages.	Fraudsters move money in minutes, while many institutions still review overnight.	Attacks happen at night and over weekends, privileged access spreads faster than anyone records it, and weaknesses are often found only after an incident.
First step	A mission briefing, followed by a demonstration on synthetic data or in your own environment.	A demonstration on synthetic data, then a scoping session on your products, data and reporting obligations.	A briefing on your environment, then an onboarding plan for monitoring or a scoped test.

Gov AI

Turn scattered intelligence into decisions leaders can act on

Gov AI brings every source an agency is entitled to use into one picture, flags what needs attention and produces the assessments and briefs decision-makers need, on infrastructure the agency controls.

The challenge

Agencies hold intelligence in separate systems and monitor in too few languages. By the time the picture is pieced together, the moment to act has often passed.

Bought by

- Presidency and cabinet offices
- Intelligence and security agencies
- Police and defence
- Electoral bodies and regulators

How it works for you

Collect
Every source the mandate allows

Connect
One record per subject

Warn
What needs attention now

Decide
Briefs leaders can act on

What it delivers

Earlier warning
Threats, narratives and emerging situations are flagged as they develop, across nine social platforms in 11+ languages.

One picture of every source
Open-source, social media, messaging, geospatial, financial and field reporting come together on each person, organisation and place.

Accountable action
Official responses and consequential decisions need named human approval, and every step is on record.

Sovereign by design
Runs on-premises, in government cloud or on isolated networks, so holdings never leave government control.

11+
Languages monitored, including isiZulu, isiXhosa and Sesotho

9
Social and messaging platforms, including WhatsApp and Telegram

6
Government missions served, from counter-terrorism to election integrity

What we sell

- Intelligence fusion
- Social media and messaging intelligence
- Open-source investigations
- Counter-disinformation
- Digital vetting
- Assessments and briefings

Track record

The Presidency
Intelligence (classified)

State Security Agency
Intelligence (classified)

Electoral Commission of South Africa
Social media monitoring

How to start

A mission briefing, followed by a demonstration on synthetic data or in your own environment.

FinCrimes

Stop fraud and money laundering before the money moves

FinCrimes checks every transaction and claim as it happens, exposes the networks behind fraud and laundering, and turns cases into the reports regulators require, with the evidence attached.

The challenge

Fraudsters move money in minutes, while many institutions still review overnight. Rings hide across accounts and claims that look unrelated, and compliance teams rebuild evidence by hand.

Bought by

- Banks and payment providers
- Insurers and special investigations units
- Mobile-money and remittance operators
- Central banks, regulators and financial intelligence units
- Tax and customs authorities

How it works for you

Score
Every transaction and claim

Connect
Expose the ring behind it

Investigate
Evidence in one case

Report
Filing-ready for the regulator

What it delivers

Decisions before money moves
Each transaction or claim gets an approve, review or block recommendation in milliseconds.

See the whole network
Shared phones, devices and identity numbers link accounts and claims into one case to work.

Alerts examiners accept
Every alert names the records, counterparties and amounts that raised it.

Faster regulatory reporting
Cases become filing-ready reports for the FIC in South Africa and SAR-style filings in the United States.

28
Named fraud and laundering patterns, each one explainable

2
Workspaces kept apart: banking and insurance

ms
To approve, review or block before money moves

What we sell

- Real-time fraud and AML detection
- Investigations and case management
- Regulatory reporting
- Insurance claims fraud
- Supply chain fraud detection
- Oversight for regulators
- Revenue leakage detection for tax authorities

Track record

South African Council for Natural Scientific Professions
Fraud detection

Gap Infrastructure Corporation
Supply chain fraud detection

How to start

A demonstration on synthetic data, then a scoping session on your products, data and reporting obligations.

Cybersecurity

Keep critical systems secure, around the clock

We sell software that controls who holds the keys to your systems, and run the services that watch, test and respond for you, from our operations centres in Cape Town and Johannesburg.

The challenge

Attacks happen at night and over weekends, privileged access spreads faster than anyone records it, and weaknesses are often found only after an incident.

Bought by

- Chief information and security officers
- Government departments
- Banks, insurers and telecoms
- Organisations without a security night shift

How it works for you

Prevent
Control access, find weaknesses

Detect
Watch around the clock

Respond
Contain and investigate

Improve
Fix and retest

What it delivers

A 24/7 watch
Analysts monitor, triage and respond around the clock, co-managed with your team or fully managed.

Control of everyday credentials
KeyCare Pass encrypts password vaults on the device and helps teams govern shared credentials.

Weaknesses found first
Testing and vulnerability management find and prove the gaps before an attacker does.

Leadership on demand
A virtual security chief sets strategy and prepares you for ISO 27001, NIST and POPIA.

24/7
Security operations from Cape Town and Johannesburg

1
Security software: KeyCare Pass

9
Services, from monitoring and testing to forensics and advisory

What we sell

- KeyCare Pass password management
- 24/7 security operations centre
- Penetration testing and vulnerability management
- Digital forensics
- vCISO, architecture and cloud security

Track record

Cell C
IT security

Sage
IT infrastructure

Gap Infrastructure Corporation
Digital forensics

How to start

A briefing on your environment, then an onboarding plan for monitoring or a scoped test.

03 Why Dark Pools

Why clients choose us

What sets Dark Pools apart is how the work is done, as much as what we sell.

One accountable partner

Intelligence, financial crime and security from one team on one platform. No hand-offs between vendors.

Your data stays yours

On-premises, government cloud or hybrid, including isolated networks. Nothing leaves your boundary without a decision.

Findings you can defend

Evidence behind every alert and assessment, and an audit trail of every consequential action.

People stay in charge

Consequential actions need named human approval. No covert bots, no fake accounts, and automation never moves money.

Built for this region

Monitoring in local languages, mobile-money and remittance fraud coverage, and security operations in Cape Town and Johannesburg.

Ready for procurement

B-BBEE Level 1 in South Africa, a Delaware company for US clients, and registration documents on request.

The difference in practice

	The common approach	With Dark Pools
Partners	Several vendors, each holding part of the picture	One accountable team across intelligence, fraud and security
Data	Sent to a vendor's cloud	Kept on infrastructure you control
Alerts	Scores without reasons	Evidence behind every alert and assessment
Coverage	English-only monitoring, card-centric fraud rules	Local languages, mobile money and remittance corridors
Security watch	Office hours, or none	Around the clock from Cape Town and Johannesburg

Who buys what

Client	Gov AI	FinCrimes	Cybersecurity
Government and security agencies	●	○	●
Central banks, regulators and FIUs	○	●	○
Tax and customs authorities	○	●	●
Banks and payment providers	○	●	●
Insurers	○	●	●
Mobile-money and remittance operators	○	●	○
Telecoms and enterprises	○	○	●

04 Track record

Who we work with

Our clients include the Presidency, the State Security Agency, the electoral commission, a statutory professional council and leading private companies. Where the work is classified, only the service area is named.

Client	Sector	What we deliver	Line of business
The Presidency	Government	Intelligence (classified)	Gov AI
State Security Agency	Government	Intelligence (classified)	Gov AI
Electoral Commission of South Africa	Government	Social media monitoring	Gov AI
South African Council for Natural Scientific Professions	Government	Fraud detection	FinCrimes
Cell C	Private	IT security	Cybersecurity
Sage	Finance	IT infrastructure	Cybersecurity
Gap Infrastructure Corporation	Private	Supply chain fraud detection, Digital forensics	FinCrimes, Cybersecurity



Clients by sector

Government	4	57%
Finance	1	14%
Private	2	29%



Engagements by line of business

Gov AI	3	38%
FinCrimes	2	25%
Cybersecurity	3	38%

Partner

Virtueda Systems

Distributes Dark Pools products and works with us on services.

Distribution partner | Services partner

05 Working with us

From first conversation to a running service

Every engagement starts with your mission and your constraints. Demonstrations are arranged to your security requirements.

1

Briefing

A conversation about your mission, risks and priorities. Book online or call us.

2

Demonstration

Arranged to your security requirements, on synthetic data or in your own environment.

3

Scoping

We agree the outcomes, the data and systems involved, and the deployment model.

4

Deployment

On-premises, in government cloud or hybrid, with onboarding for your team.

5

Operate and improve

Ongoing support and service reviews, with findings fed back into the next round.

Ways to buy

	What	How it is delivered
Platforms	Gov AI, and FinCrimes with Banking and Insurance workspaces	Deployed on infrastructure you control: on-premises, government cloud or hybrid
Products	KeyCare Pass	Password management as a hosted service or self-hosted
Managed services	24/7 security operations centre, vulnerability management and threat hunting	Ongoing service, co-managed with your team or fully managed
Projects and advisory	Penetration testing, digital forensics, architecture, cloud security and vCISO	Scoped engagements with defined deliverables
Through partners	Dark Pools products through Virtueda Systems	Distribution and joint service delivery

Deployment options

On-premises

Everything runs inside your own facilities, including networks with no outside connection. For data that cannot leave the building.

Government cloud

Runs in government cloud regions or with in-country providers, under sovereign controls. For scale without giving up control.

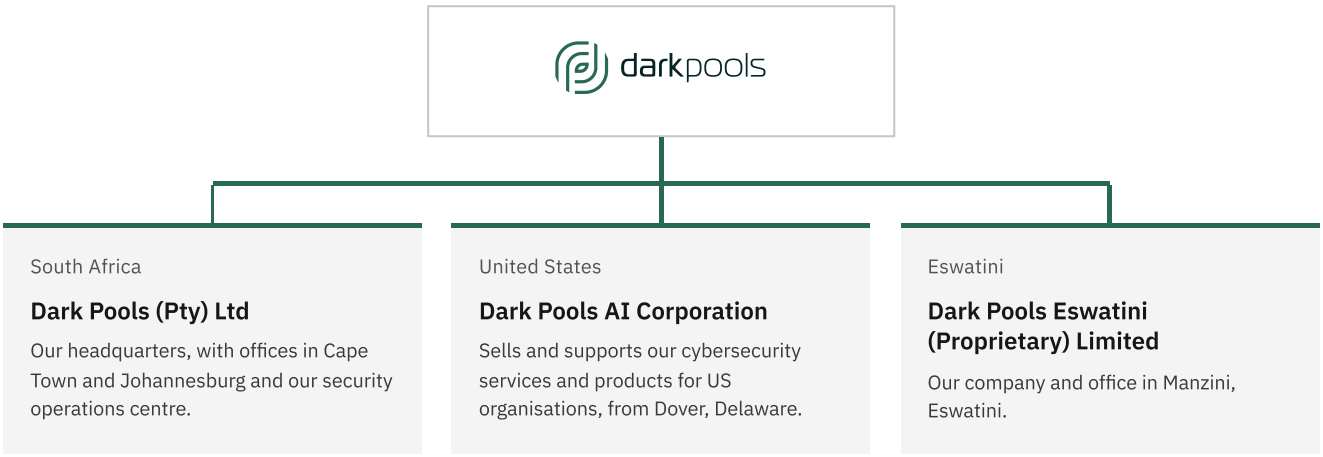
Hybrid

Sensitive records stay on-premises and only selected data is synchronised to the cloud. For the balance of both.

06 Our company

Three companies, one team

Dark Pools operates through a company in each of its markets, served by the same team and the same platforms.



Offices

Cape Town
South Africa

Georgestraat 89, Suite 2172, 7140 Kaapstad, Western Cape, South Africa

+27 10 502 2552

Johannesburg
South Africa

Wild Fig Business Park, Unit 10, Cranberry Street, Honeydew, Roodepoort, 2170, South Africa

+27 10 502 2552

Manzini
Eswatini

Plot 55, Manzini Town Centre, P.O. Box 1544, Manzini, Eswatini

+27 10 502 2552

Dover
United States

1111B S Governors Ave, Dover, DE 19901, USA

+1 (443) 426-3738

Company details for procurement

Company	Registration	Registered address
Dark Pools (Pty) Ltd Private company	2021/522920/07	Georgestraat 89, Suite 2172, 7140 Kaapstad, Western Cape, South Africa
Dark Pools AI Corporation Delaware corporation	7326901 SAM.gov UEI QG4MGXJYL6A5	1111B S Governors Ave, Dover, DE 19901, USA
Dark Pools Eswatini (Proprietary) Limited Private company	R7/78602	Plot 55, Manzini Town Centre, P.O. Box 1544, Manzini, Eswatini

darkpools

Let’s talk about your mission.

Book a briefing and we will show you what Dark Pools can do for your organisation, on synthetic data or in your own environment.

Book a briefing

calendly.com/darkpools/meeting

www.darkpools.co.za/contact

South Africa and Eswatini

+27 10 502 2552

Georgestraat 89, Suite 2172, 7140
Kaapstad, Western Cape, South Africa

United States

+1 (443) 426-3738

1111B S Governors Ave, Dover, DE
19901, USA

Dark Pools (Pty) Ltd, registration number 2021/522920/07
Dark Pools AI Corporation, delaware file number 7326901
Dark Pools Eswatini (Proprietary) Limited, company number R7/78602

© 2026 Dark Pools (Pty) Ltd. Company profile, October 2026.