Navigating the Modern Threat Landscape

With a short

Trace3 Overview

01

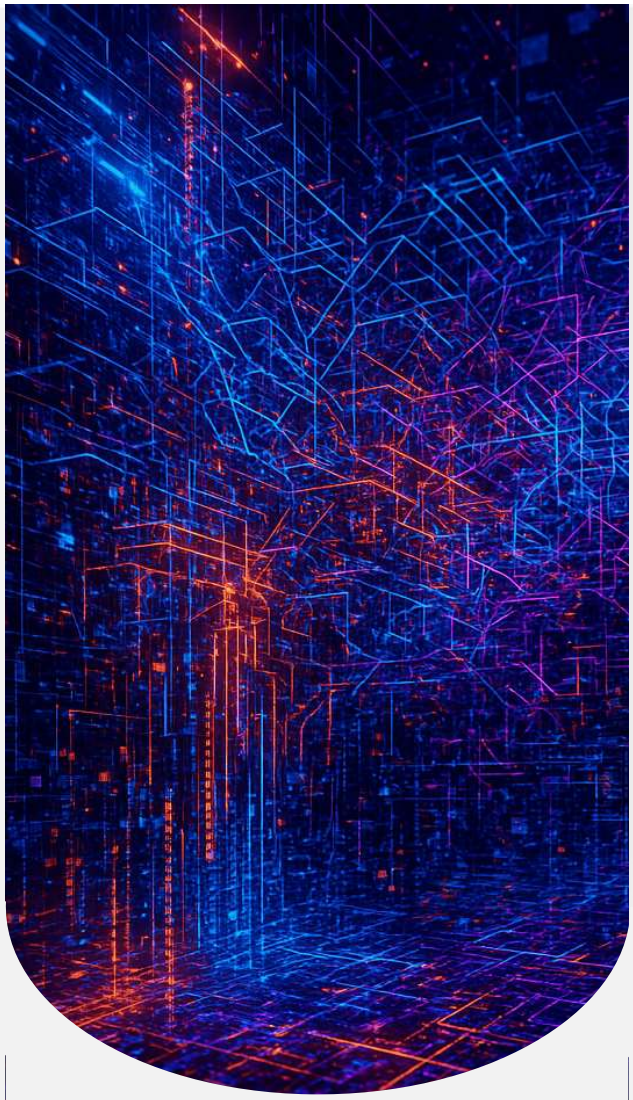
2025 Threat Landscape

TRACE3

2025 Threat Landscape

The increasing volatility and complexity demands more effective and proactive approaches to securing our complex ecosystems.

- **Escalating Threat Sophistication**
- **AI Integration and Security Risks**
- **Supply Chain Vulnerabilities**
- **Post Quantum Cryptography**
- **Regulatory and Government Changes**



Escalating Threat Sophistication

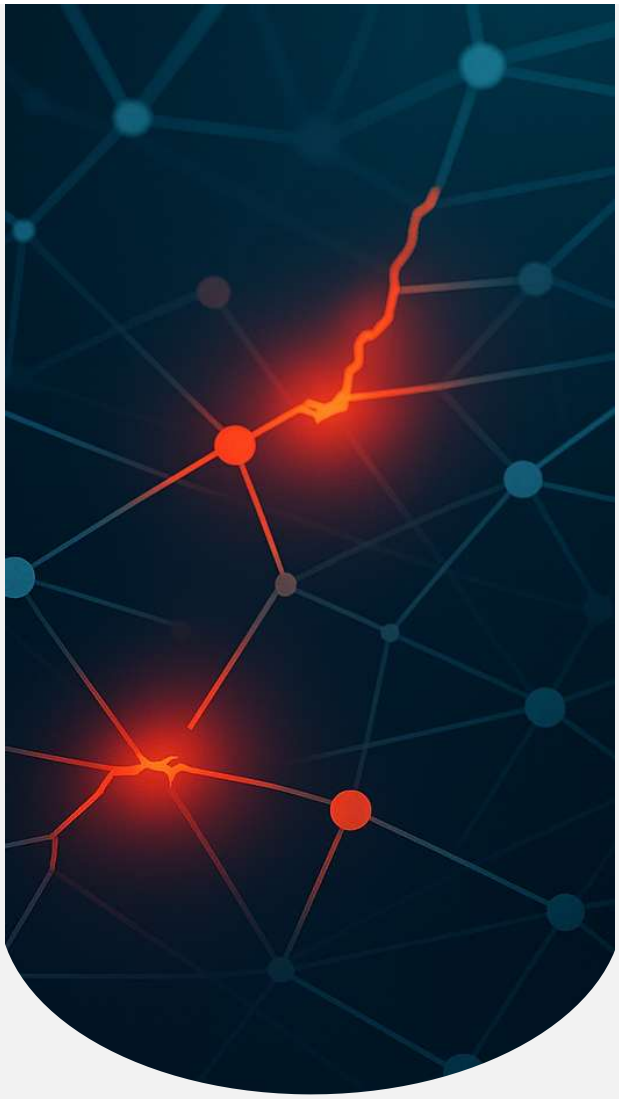
Increasing maturity and technology in attacks

- Ransomware
  - Top gangs for 2025 are Scattered Spider, Akira, CI0p, SafePay (maybe rebrand of LockBit, AlphV, or INC), and RansomHub
  - Many moving away from encryption and straight to exfiltration extortion
  - Targeting healthcare, retail, logistics, and education
  - Leaked builders like LockBit 3.0 are being used by copycats
- Nation State attacks heavily funded and targeting political rivals
- Fragmented eCrime ecosystems create a cybercrime supply chain with decentralized, diverse, and loosely affiliated bad actors to stay small and agile, collaborating only when needed
  - Initial access brokers who specialize in gaining and selling access/credentials
  - Malware developers
  - RaaS operators
  - Data brokers and information stealers/sellers

AI Usage and Risks

Burnout is real and AI usage is ever increasing to help close the gap … but at what cost?

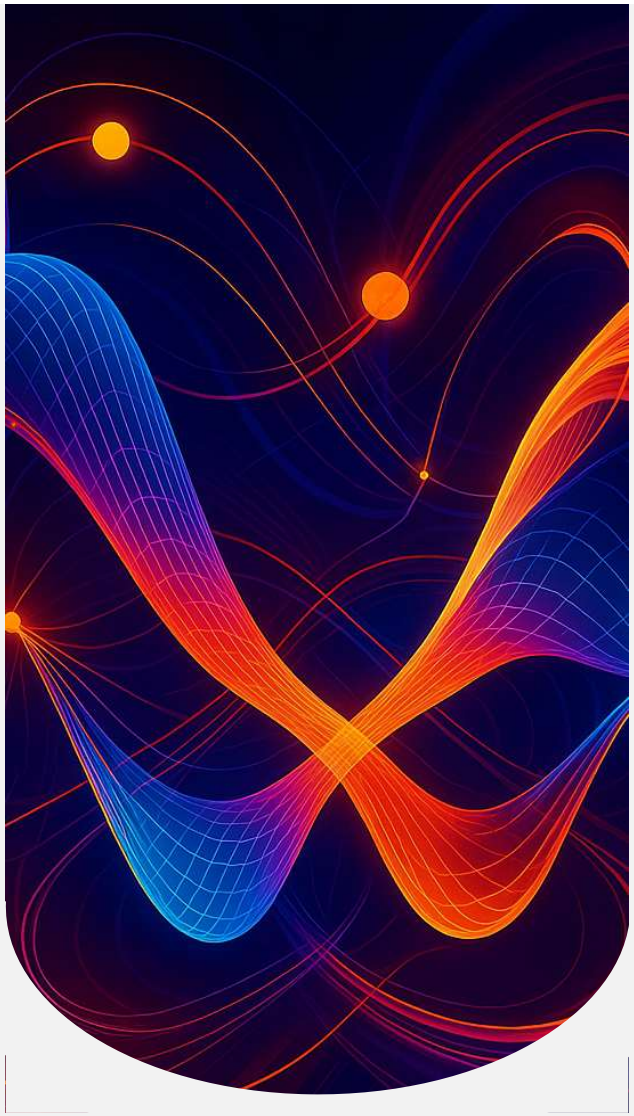
- Usage of AI by attackers decreases the time it takes to create and execute attacks
- Agentic AI risks including misalignment, brand harm, cascading failures, introduce bias and discrimination, ethical conundrums, and data privacy loss
- LLM AI usage risks like code and data leakage, hallucinations and misinformation leading to poor decision making, behavior manipulation, copyright infringement and lawsuits, lack of oversight, and access to unauthorized internal data
- Advanced disinformation campaigns - Utilizing AI to create impersonations, fake news, etc.
- AI assistant moonlighting / fake employee creation
- Digital doppelgangers created using AI, biometric data, and behavioral modeling can mimic the appearance, voice, expressions, and decision-making patterns of real individuals
    - Results in identity theft and impersonation, deepfake scams, privacy concerns due to data ownership and digital likeness rights, brand impersonations, and disinformation campaigns



Supply Chain Vulnerabilities

Software bill of materials (SBOMs), automated vulnerability scanning, version pinning, and auditing of all third-party components is critical

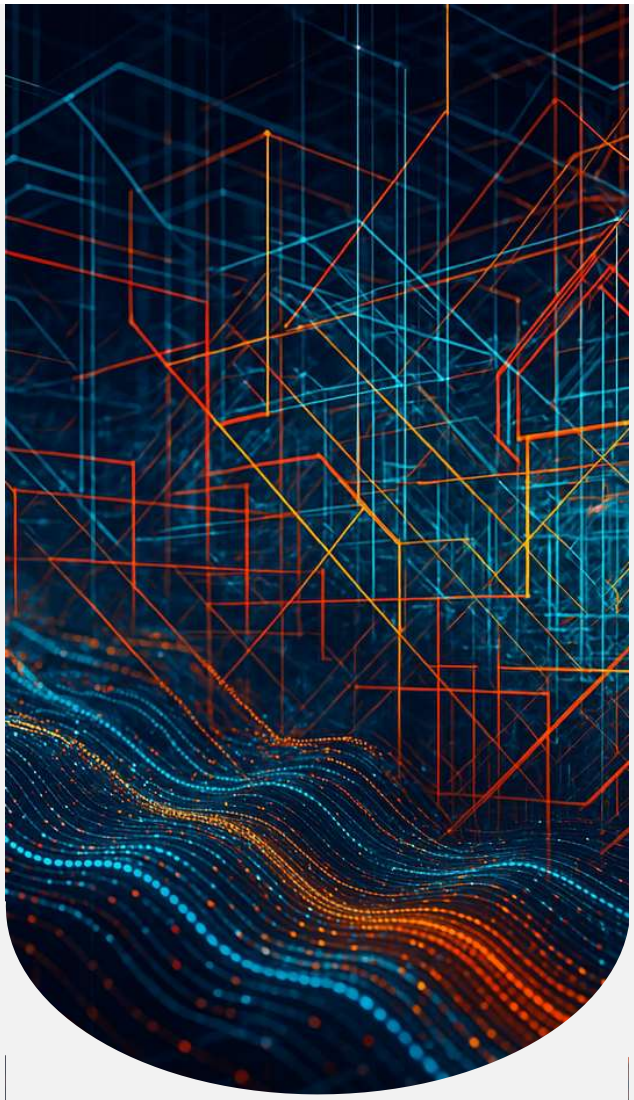
- **Software dependencies** of libraries, frameworks, modules, codebases create risks of unpatched open-source libraries, outdated or unsupported dependencies, dependency confusion attacks via malicious packages with the same name as internal dependencies uploaded to public repositories, malicious code injections, and exposed secrets risks
- **Lack of visibility across the software supply chain**, with only 23% of organizations reporting having high visibility, making it difficult to detect vulnerabilities in third party code, APIs, and dependencies.
  - Organizations with low visibility are **13x** more likely to suffer a breach
  - Attackers often exploit vulnerabilities in small vendors to infiltrate larger targets
- 39% of CEOs believe **AI adoption increases software supply chain risk**
- **IoT logistics like sensors, trackers, smart warehouses, expand the attack surface**, and risks include hijacked devices used in botnets, intercepted and manipulated sensor data impacting logistics, and exploits of insecure firmware and outdated protocols
- **Developer hubs are highly attacked**, like Open VSX registry, where a single vulnerability could compromise huge swaths of software and services
- **Open-source risks** including transitive dependencies that are rarely audited and often invisible to devs, missing SBOMs, license conflicts, and others
  - A vulnerable subcomponent of a popular library can compromise thousands of apps
  - Trusted contributors can go rogue or have their access compromised, like with xz Utils backdoor in Linux utilities



Post Quantum Crypto Attacks

It's no longer theoretical – it's imminent and strategically relevant

- New attacks are expected to be **created within seconds** using PQ computing, rather than hours or days
- **Harvest-now, decrypt later (HNDL)** attacks
- **Outdated encryption algorithms** (e.g., RSA and ECC) usage means quantum computers can decrypt at scale
- Quantum tools allow for decrypting sensitive data, including supply chain data like trade secrets, supplier contracts, and shipment manifests, customer records, proprietary information, and basically **anything that is currently encrypted**



Regulatory Changes and Government Impact

Keeping up with change

- **NIST updates** to v2.0, changes in cryptography recommendations
- **CVE debacle** and future impact
- **Privacy law changes** and discrepancies across individual states/countries
- **Critical infrastructure** / operational technology attacks
- **Strict regulations for supply chain** security including EU's NIS2 and US's CISA
- FinCEN compliance stipulations with the **Bank Secrecy Act**
- **PCI updates** for crypto payments
- SEC treatment of **crypto as securities**
- **Tariff impacts** on attacks with growing nation state rivalries and crypto kidnapping acceleration
- **Hacktivism** ever increasing
- **AI usage is outpacing regulations**
- **Digital surveillance authoritarianism** and loss of privacy continues

2025 YTD Attack Examples

01

Bybit – $1.5B Coinbase by Lazarus (NK)

- Safe wallet developer's laptop was compromised via social engineering
- AWS session tokens utilized to bypass MFA
- Malicious code set to execute on a specific cold wallet owned by ByBit
- ByBit employees initiated a cold to warm wallet transaction which allowed the attackers to transfer the funds to their own wallets, which was quickly exchanged and dispersed for rapid laundering

02

WhatsApp Spyware Attack

- Spyware was delivered via PDFs and multimedia files sent through WhatsApp, and required no user interaction
- Exploited zero day vulnerabilities and file type mismatches in the MM and video call processing systems that triggered the exploit immediately upon receiving
- Allowed access to encrypted messages, activated microphones and cameras, tracked locations
- Executed by a surveillance firm

03

Retail Attacks by Scattered Spider

- Attacks on Marks and Spencer, Harrods, and Co-Op UK
- Halted online transactions, froze gift card processing, and postponed deliveries
- M&S attack: Access was gained via 3rd party contractors, and AD password hashes were stolen and ransomware was deployed on VMWare ESXi servers. Estimated £300-700M loss
- Harrods was able to stop the data breach
- Co-Op UK was contained but data was exfiltrated.

2025 Updated Attack Vectors

Nation-state surveillance

API and web app exploitation

MFA fatigue and social engineering

SaaS misconfigurations

Social media and smishing

Agentic AI exploitation

Zero-click exploits

Third-party risks and vulnerabilities

Misconfiguration exploitation

Email and phishing

TRACE3

02

2025 Mitigation Strategies

TRACE3

Securing AI

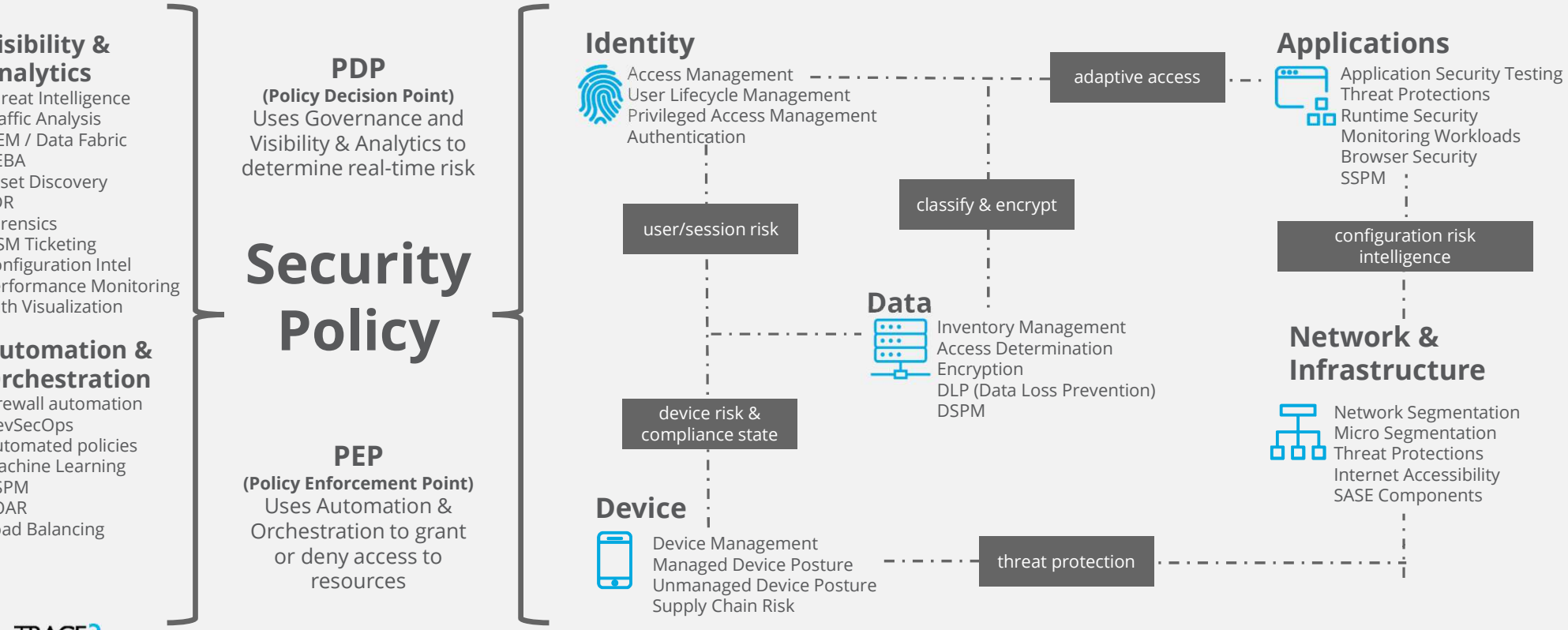
Securing the brand against rogue AIs and AI-powered attacks

- Using enterprise AI models with **privacy guarantees**
- **Training users** on AI usage
- **Monitoring** prompts and output
- **Misuse** detection
- AI **agentic security**
- AI **model scanning** and security
- AI **posture management**
- **Runtime** agentic AI security
- AI **red teaming**
- **Deploying AI-powered security tooling** for real-time threat detection, autonomous responses, and predictive analytics

Trace3's Zero Trust Reference Architecture

Governance & Configuration Risk Intelligence

Policies, standards, and regulatory requirements provide the basis for defining access to data: the who, what, where, when, and why. Governance guides architecture decisions and outlines the appropriate workflows. An organization's risk tolerance needs to be determined and incorporated into the solution planning for Zero Trust.



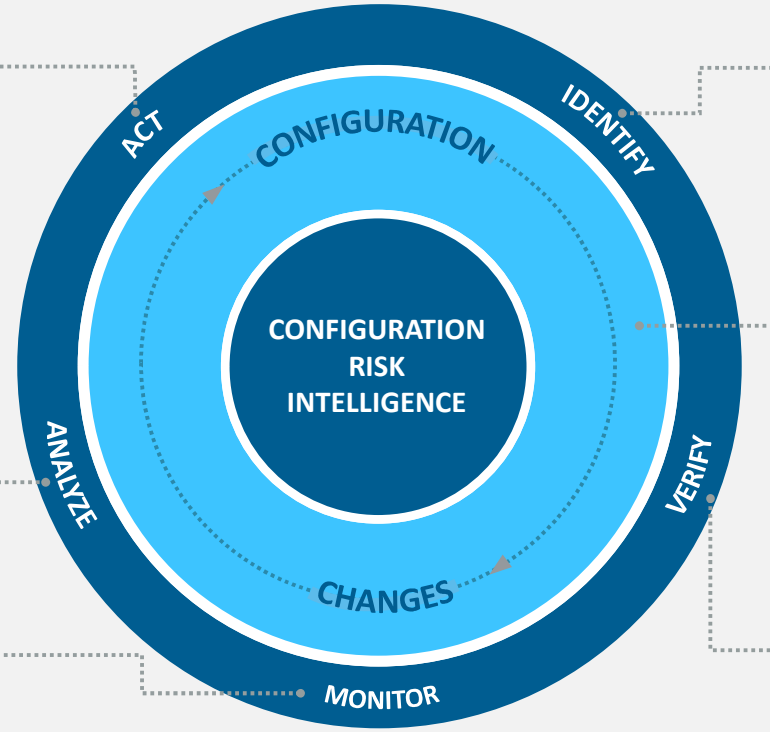
TRACE3

Configuration Risk Intelligence

Act on **mitigating risks by understanding their context**, including change remediation, repaving of environments, additional reviews, and more.

Analyze risk automatically to process the changes identified, and highlight only those **potential misconfigurations and drift** that can hurt stability, compliance and security

Monitor changes and drift across the identified assets and their detailed configuration after confirming configuration baselines



Identify all the digital assets and their detailed configuration

Integrate two data sets—configuration and changes—as a foundation for configuration risk intelligence. Configuration and changes are two sides of the same coin and need to be reviewed and analyzed together

Verify that **granular configuration** of the assets complies with the target standards and best practices while being accurate and consistent

Configuration intelligence in a Zero Trust model:

- Addresses **fragmented intelligence** on key risks associated with configuration changes
- Detects **risky (including unauthorized) changes** across the data, applications, network and infrastructure, identity, and device domains
- **Improved performance visibility and impacts**
- Centralized **change management** processes

Post Quantum Computing Readiness Considerations

Preparing for the demise of current encryption techniques before the attacks start

Keep informed

- Build and execute on an action plan to monitor developments in PQC and re-examine quarterly.
- Name a PQC leader internally to stay informed, educate others, and drive initiatives.
- Request PQC support status from vendors, including PQC roadmap

Model threats and Map Data Flows

- Inventory cryptographic assets to identify protocols, certs, and libraries
- Map dependencies on vulnerable algorithms (e.g., RSA, ECC) and asymmetric encryption, and see if public CA issued certs support PQC key exchange (use automated discovery tools)
- Evaluate long-term data sensitivity requirements
- Assess harvest-now, decrypt later attack risks

Develop a plan

- Consider hybrid cryptographic solutions that combine classical and quantum-resistant encryption
- Build a roadmap to transition to PQC secure products, encrypt data with NIST-approved cryptography
- Play with technology, test algorithms like Kyber, Dilithium, and SPHINCS+, and understand how different systems respond to the additional and significant demands

Human Risk Management

Maturing the approach to training, testing, and analytics with intelligence

- Human risk management focuses in part on training and understanding the way humans behave today, not in the past, with continuous training and adaptive techniques
  - Bite-size training modules delivered throughout the year
  - Gamification
  - Real-time training adaption based on answers
- It also focuses on categorizing and evaluating the active risks per user and group and allowing deep-dives into the intelligence behind those risk scores
  - Blocked/not blocked operations
  - Alert-triggering operations
  - Activities by categories
  - Content detectors


TRACE3
ALL POSSIBILITIES LIVE IN TECHNOLOGY

At Trace3, we:

Deliver business transformation.

We consult on, integrate, and operate convergent solutions across data, security, and cloud that embrace emerging technology and drive measurable value.

Vision

Our vision is to always be an innovator in the industry, with commitment to business value realization for our clients across technology.

Innovation

Trace3 empowers executives and their organizations with cutting-edge technology innovations, offering access to emerging tech from Silicon Valley. This enables them to stay ahead of evolving business needs and maintain a competitive edge.

Partnerships

We are the premier technology solutions provider for enterprise and commercial clients. Trace3 provides access to emerging tech from Silicon Valley coupled with elite engineering that drives end-to-end solutions in cloud, data and analytics, security, and the data center.

Trace3's Highly Differentiated Business Model

Emerging Technology

- Innovation embedded in Trace3 DNA
- Unique venture capital ecosystem
- Unmatched insight into new technology

Elite Expertise

- Significant investment in consulting and engineering talent
- Elite vendor partnerships and loyalty to the client
- Best-in-class service and delivery execution

Client Intimacy

- Regional model built to optimize client intimacy
- Thousands of clients across all industries
- Early client access to emerging technology

Trace3 Key Facts

We are a premier IT solutions and services provider, specializing in Cloud, Data Intelligence, Security, and Modern Infrastructures for large enterprise clients globally. Our cutting-edge solutions empower businesses to innovate, secure their data, and build robust infrastructures that drive success in the digital age.

1,511
Full Time Employees

1,000+
Certifications

800+
Engineers & Consultants

$3B
2024E Revenue

5,500
Clients

100+
Partners with $1M+ Annual Revenue

25%
Revenue from Emerging Tech Partners

5
M&A Transactions Completed

7
Worldwide Fulfillment Across Seven Continents

WHO WE ARE

20+ years of delivering innovative IT solutions to the Fortune 500.

Expert consulting, managed services, and engineering capabilities.

servicenow

Defacto expert in emerging technology.

KEY FACTS

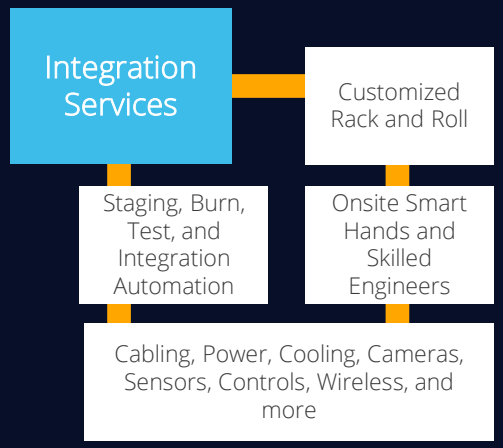
Founded in 2002. Currently PE owned by American Securities

Headquartered in Irvine, CA with regional presence in 50 states.

TRACE3

Trace3 Capabilities

Innovative Engineering and Advisory Services to Help Your Business **Run, Grow, and Transform**



Thank You!

Janel Schalk

Janel.Schalk@trace3.com

TRACE3