DARKTRACE

6 Challenges to Securing the Modern Network

Abstract

With the cloud at the forefront of cyber security discussions, traditional, on-premises networks get less attention from the media – but still get plenty from hackers. A recent report found 45% of breaches were cloud-based in 2022 [1], which means that, despite decades of investment in security, most successful attacks still targeted traditional networks.

This white paper looks at six critical challenges to securing today's modern, integrated networks and how security teams can keep them safe and compliant in today's fast-changing threat landscape. We'll see how professional threat actors leverage artificial intelligence (AI) to up their game, and how the right AI-led approach helps defenders scale operations to keep up and harden security postures to prevent more attacks.

6 Top Challenges to Securing Today's Networks

Ransomware

Supply chain / third-party attacks

Insider threats

Novel attacks

Perennial cyber skills shortages

Pulling it all together

[1] Snyk, The State of Cloud Security Report 2022, 2022.

Introduction

Securing a borderless network attack surface

Not long ago, protecting the corporate network mainly meant keeping bad traffic from suspicious IPs out — a difficult but reasonably straightforward job. Today's security posture assumes attackers have or will find their way onto corporate networks and places greater emphasis on enabling responders to act quickly to stop unfolding attacks.

> Enterprise networks today barely resemble their counterparts from just a few years ago. Resources and users are now spread across a variety of enterprise, cloud and remote locations, making the perimeter amorphous and difficult to define. [2]
>
> **TECHTARGET**

Digital threats evolving faster than defenses

Network borders are in constant flux.
Ongoing digitalization leaves IT with a fragmented tapestry of on-premises networks, VPNs, cloud services, SaaS applications, email platforms, industrial devices, and other endpoints to protect. Today's fluid network boundaries make it harder to see and prioritize digital threats that come in many forms and from many more directions than ever before.

Modern threats elude detection.
Threat actors use multiple techniques like social engineering and encryption to sneak malware into networks without being flagged by perimeter, endpoint, and cloud security, or dozens of specialized point tools found within an enterprise SOC. Firewalls, intrusion prevention systems (IPSs), and email security that inspects and blocks suspicious traffic still provide a vital front line of defense, but it only takes one set of lost or stolen credentials for threat actors to gain initial access.

Once they come aboard your network, cyber criminals abuse privileges to move laterally deploying malware that exfiltrates or holds data hostage. Attacks may detonate quickly, taking defenders by surprise, or proceed stealthily for months to avoid triggering detection.

Security needs a stronger force multiplier

Many security solutions use AI to surface possible threats faster than humans can, but basically leave it up to analysts to investigate and prioritize them all. Since most teams don't have unlimited cycles to field alerts — and threat actors use the same techniques to turbo-charge new attacks — AI must do more than add sheer horsepower.

To give network defenders a valuable time advantage, network security needs to make smarter use of AI. For starters, it should continuously analyze nuanced behavior by authorized users to detect subtle indicators of risk, but AI's value shouldn't end there.

Advanced implementations of AI can update network security strategies to combat new and perennial threats with:

- Behavioral analysis at machine speed and scale
- Advanced anomaly detection based on your unique organization
- Autonomous surgical response to contain threats within seconds without disrupting business operations

AI should learn and act on its own.
AI-led solutions should train and maintain their own intelligence without consuming analyst cycles to stay current. In the next sections, we'll see how a Self-Learning AI approach gives defenders the advantage against today's leading attacks.

[2] TechTarget, "Ransomware trends, statistics and facts in 2023," Sean Michael Kerner, 26 January 2023.

Darktrace: AI That Learns Your Business to Stop Disruption

Whoever uses AI most skillfully wins. As security analysts and threat actors race to out-innovate one another, they increasingly leverage AI and machine learning (ML) as their weapons of choice. For cyber defenses, smarter use of intelligence means using AI to do new things and do them better as well as faster.

Where other approaches rely on training AI on historical attack data, Darktrace's Self-Learning AI understands 'normal' for your unique organization, and then identifies subtle deviations that indicate a cyber-threat. This unique approach means it can identify novel, unknown, or targeted threats on the first encounter – without needing to have been trained on a similar past attack. This type of anomaly detection also effectively identifies abuses of trust, such as insider threats and attacks that use stolen credentials.

Better detection is only half the battle. Darktrace also delivered the world's first proven Autonomous Response technology able to intelligently fight back against in-progress attacks before they do damage. Rather than generate massive quarantines that may lead to downtime, Darktrace/Network neutralizes only the threats in seconds by enforcing normal behavior for a user or device that gets compromised.

Darktrace's Cyber AI Analyst automates workflows at speed and scale but preserves the flexibility of human expertise. The system generates incident summaries that equip resource-constrained security analysts to take immediate action. The context provided includes insights on incidents involving novel attack techniques that cannot be countered using pre-defined playbooks.

CHALLENGE 1

Stopping Ransomware at Every Stage

Avoiding ransomware attacks ranks at the top of most CISOs' and risk managers' priority lists, and with good reason. Extortion was involved in 25% of all breaches in 2022, with front-page attacks wreaking havoc across healthcare, gas pipelines, food processing plants, and other global supply chains. [2]

"What else is new?"

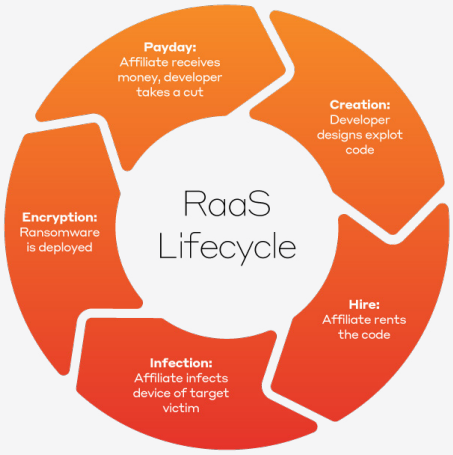
The availability of "DIY" toolkits and subscription-based ransomware-as-a-service (RaaS) on the dark web equips novice threat actors to launch highly sophisticated attacks at machine speed. For less than $500, virtually anyone can acquire and tweak RaaS offerings such as Philadelphia that come with accessible customer interfaces, reviews, discounts, and feature updates — all the signature features of commercial SaaS offerings.

$5.13M **average cost of a ransomware attack**

IBM, "Cost of a Data Breach Report 2023," July 2023.

$900M **predicted amount to be extorted by ransomware in 2023**

Chainalysis, "Crypto Crime Mid-year Update: Crime Down 65% Overall, But Ransomware Headed for Huge Year Thanks to Return of Big Game Hunting," 12 July 2023.



Malware developers' budgets keep growing. As the market for automated cybercrime matures, surging demand has given rise to profit-sharing models that split ransomware proceeds between developers and "affiliate" attackers.

Many developers funnel these new revenues back into the business, making it harder than ever for security vendors and controls to out-innovate and keep up with attacks. Modern malware masterminds even invest in their own off-the-shelf security solutions so they can test and perfect new releases to evade detection by network security.

[2] TechTarget, "Ransomware trends, statistics and facts in 2023," Sean Michael Kerner, 26 January 2023.

Self-Learning AI breaks the ransomware cycle

The preeminence of ransomware keeps security teams on high alert for indicators of attack but hypervigilance — and too many tools churning out too many alerts — quickly exhausts analysts' bandwidth. To reverse this trend, AI needs to help prioritize and resolve versus merely detect risk.

Darktrace/Network uses Self-Learning AI to recognize and contextualize possible signs of ransomware attacks as they appear in your network and across multiple domains. Viewing behaviors in the context of your organization's normal 'pattern of life' updates and enhances detection that watches for a repeat of previous techniques.

A self-learning approach brings the added advantage of continuously analyzing behavior in your environment at machine speed.

Darktrace AI performs an Autonomous Response to shut down attacks at every stage of the ransomware cycle, including the first telltale signs of exfiltration and encryption of data for extortion purposes.

Darktrace/Network uses Autonomous Response to shut down ransomware attacks at the outset to keep the worst from happening. Darktrace enforces the normal pattern of life for devices attempting to encrypt data, saving organizations from data and financial loss, clean up, and repeat attacks that often follow.

CHALLENGE 2

Avoiding Supply Chain Attacks

Broader ecosystems create broader risk.
Supply chain attacks show just how dangerous technology can be when it falls into the wrong hands. Digitalization allows more companies to interconnect their IT environments using Application Programming Interfaces (APIs). But these same potent APIs can be used by threat actors to sneak into your environment through your affiliates' networks and deploy malware or execute modern denial of service (DoS) and distributed denial of service (DDoS) attacks that bring down systems.

Instead of targeting a single organization, threat actors can exploit a single weakness in a popular vendor's architecture to compromise hundreds, even thousands of environments in record time. Even a zero trust security posture won't protect your data and brand reputation from supply chain attacks if you don't detect signs of misuse very quickly.

"Known bad" detection won't find unknown vulnerabilities

New vulnerabilities appear — and old ones become newly exploited — all the time.
The infamous attack on SolarWinds took the world by surprise, creating heightened awareness of how difficult third-party attacks can be to avoid. Newly active exploitations might fail to trigger alerts by Network or Managed Detection and Response (NDR and MDR) solutions, SOAR, and other traditional security tools that rely on pre-defined sets of rules to identify malicious behaviors. These tools usually require manual efforts to train AI to identify dangerous behavior based on known attacks and vulnerabilities. Even with integrated threat intelligence, this static approach requires regular updating — and tools still might not spot subtle indicators that authorized users are doing something unorthodox within your environment. For example, a partner or vendor who typically accesses one set of corporate resources attempting to access another.

> I was amazed to see how [Darktrace's] AI works and alerts for any abnormal behaviour on the network. Darktrace has separate models for multiple behaviours that learn about normalities and detect and alert for any abnormalities.

IT Security and Risk Manager
/ Healthcare (Gartner Peer Insights)

Self-Learning AI detects anomalies faster

By understanding 'normal' for your business and revealing anomalous behavior, Darktrace detects third-party attacks faster than traditional network security. The platform's Cyber AI Analyst does the work of piecing together and contextualizing seemingly unrelated anomalies to connect the dots and show analysts the full pattern of newly coined threats unfolding within your network.

Instead of taking overzealous actions like quarantining entire systems to contain lateral movement — which may cost partners money for which your business may be liable — Darktrace/Network mounts a more surgical autonomous response. The platform pinpoints and neutralizes only potentially risky activities until analysts can investigate threats.

Promotes collaboration without adding risk.
Where many NDR providers store customer data in the cloud, Darktrace places its Self-Learning AI into your environment to protect your organization's data privacy. This approach does not require your data to be encrypted, stored, or cross-contaminated in third-party cloud data lakes.

CHALLENGE 3

Managing Trust

Granting access and privileges to your workforce and select affiliates has profound implications for cyber security, brand reputation, regulatory compliance, and financial liability. In a traditional network security model, traffic gets divided into two categories — trusted and untrusted — with some entities and segments of the network deemed more creditable than others.

But how do you tell which is which?

Zero trust is too little, but any is too much.
Modern network security challenges point to an urgent need for organizations to review and update their approaches to managing trust. External pressure to adopt zero trust security postures literally suggests trusting no one, but that impedes your freedom to do business. IT leaders need a proven but practical process for deciding who should be allowed to use your network and how.

> By 2026, 10% of large enterprises will have a comprehensive, mature and measurable zero-trust program in place, up from less than 1% today. [3]
>
> **GARTNER**

At the programmatic level, questions to ask in updating Trusted User policies include:

- What process should you follow to place trust in third parties and applications?
- Do you subject trusted entities to testing and other due diligence first?
- How often do you review this process — and trusted relationships themselves — after making initial decisions?
- How do you tell when trusted users should no longer be trusted?

Once trust has been established, security teams need new and better ways to autonomously verify that those transacting within your network are indeed those trusted users that they claim to be, taking only the authorized actions you've allowed them to take.

USE CASE

AI spots an insider threat out of the Box

Suspicious requests within a global produce supplier's Box platform suggested a user account had been compromised. After logging into Box successfully, the actor downloaded expense reports, invoices, financial documents, and unlocked a file containing passwords.

Darktrace AI recognized that the activity was taking place at an unusual time of day from an unusual location for the legitimate user. Cyber AI Analyst autonomously investigated and illuminated the broader pattern — the unauthorized file exposures were part of a connected incident —and alerted the security team to a possible breach.

Anomaly detection drives trust

Insider threats have a major head start. The opposite of attacks launched by nameless, faceless strangers, insider threats originate through parties once deemed trustworthy. That might mean a current or former member of your workforce or a partner, vendor, investor, or service provider authorized by IT to access corporate systems and data. Threats also arise when a "pawn" gets unwittingly tricked into disclosing credentials or downloading malware.

Common motives for insider attacks include revenge, stealing or leaking sensitive data, taking down IT systems, stealing assets or IP, compromising your organization's credibility, and simply harassing your workforce.

Rules and signatures won't flag insider threats. Because an insider does not immediately present as an intruder, their nefarious plans may unfold undeterred by security teams until it's too late. Insider threats can only be stopped by an evolving understanding of 'normal' for every user that immediately alerts your team when trusted users do something strange.

[3] Gartner, "Gartner Unveils Top Eight Cybersecurity Predictions for 2023-2024," 28 March 2023.

$5.13M

Attacks initiated by malicious insiders were the costliest, at an average of USD 4.90 million, which is 9.6% higher than the global average cost of USD 4.45 million per data breach.

IBM, "Cost of a Data Breach Report 2023," July 2023.

308 Days

This year, it took about 10 months (308 days) to resolve breaches that were initiated by a malicious insider.

IBM, "Cost of a Data Breach Report 2023," July 2023.

AI provides a failsafe

Self-Learning AI prevents "trust issues." AI augments traditional network security by continuously asking the question:

"Are trusted users behaving strangely?"

When the answer is yes, the system should both alert analysts and be able to act autonomously to contain threats and revoke privileges until IT can investigate.

Darktrace's AI Analyst immediately investigates and alerts security teams to anomalous behavior by trusted users. The platform also responds on its own to shut down unusual activity by enforcing normal behavior.

Investigation and containment take place in real-time before authorized bad actors can abuse active privileges.

Instantaneous detection and rapid response can prevent data exfiltration, crypto-mining, and breaches from occurring.

Relationships never stop changing so AI never stops learning. Darktrace AI continuously observes your environment and user behavior to stay current. Reliable data helps to refine Trusted User policies so that users can take greater initiative without sounding alarm bells.

Surgical response keeps business moving. If every company blocked access to their networks at the first sign of abnormal third-party behavior, daily business would come to halt.

Darktrace's AI Analyst goes beyond detecting uncharacteristic behavior (whether it seems dangerous or not) to contextualize threats so security professionals — or the platform itself — can mount an effective but practical response.

CHALLENGE 4

Recognizing Novel Attacks

You can't predict tomorrow's weather by reading yesterday's forecast, yet that's essentially what happens when network security tools only look for known attacks.

"Novel" includes new attacks and remixes.
Depending on how threats get executed, the term "novel" can refer to brand new tactics, techniques, and procedures (TTPs), or to subtle new twists on perennial threats like DoS, DDoS, and Domain Name Server (DNS) attacks.

Old tools may be blind to new threats

Stopping novel threats is less about deciding whom to trust than it is about learning to spot something brand new. As we've seen with ransomware, the growing "aaS" attack market creates a profound paradigm shift by allowing non-technical perpetrators to tweak, customize, and coin never-before-seen threats that elude traditional network, email, VPN, and cloud security.

Tools based on traditional rules and signatures lack a frame of reference. This is where AI's ability to spot and analyze abnormalities in the context of normal patterns of life comes into play.

Self-Learning AI spots what other tools miss

Instead of training in cloud data lakes that pool data from unrelated attacks worldwide, Darktrace AI learns about your unique environment from your environment. By flagging and analyzing everything unusual — instead of only known signs of compromise — Darktrace's Self-Learning AI keeps security stacks from missing less obvious but potentially more dangerous events.

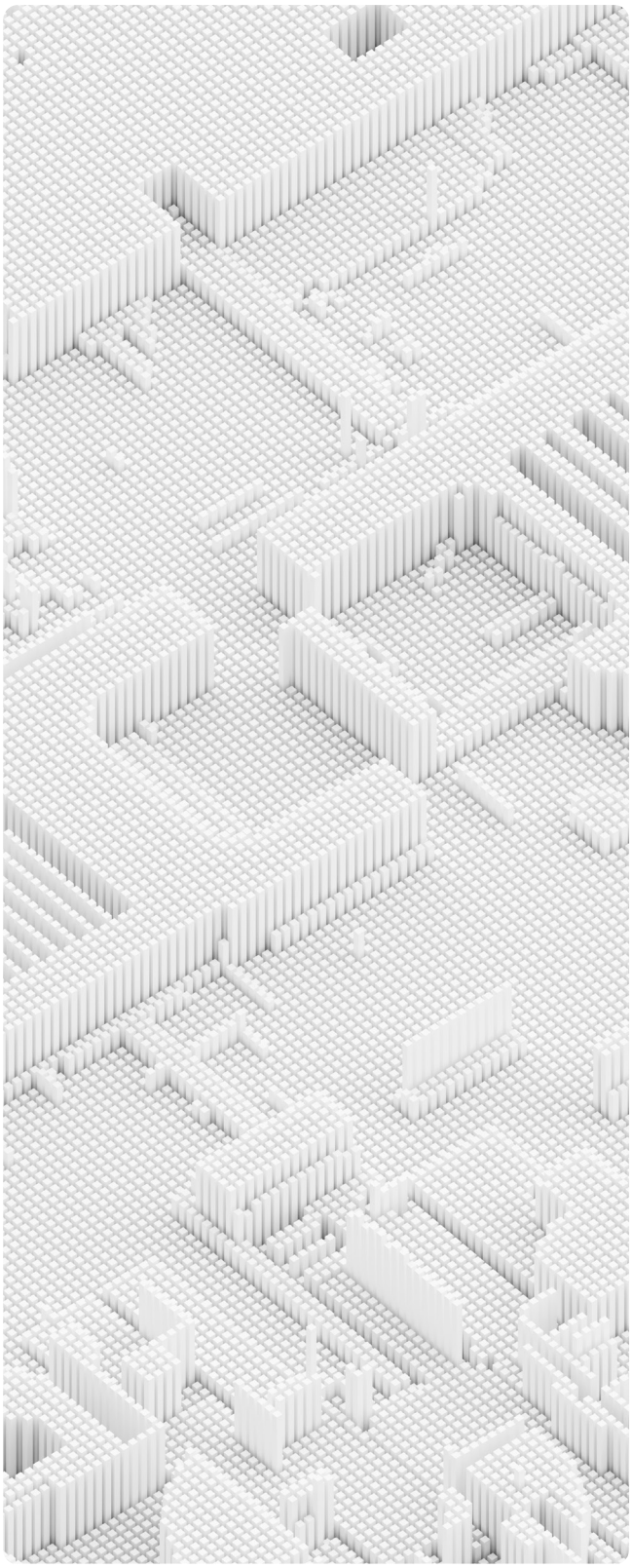
The real challenge here is achieving faster "time to meaning" and contextualizing behavior that might — or might not — be part of a novel attack. Darktrace/Network does not require a "patient zero" to identify a novel attack, or one exploiting a zero-day vulnerability.

"Nothing new under the sun?"

Though DDoS, DNS, and other network attacks haven't changed much over the years, attacker innovation allows them to unfold at unprecedented scale and speeds. Google and Amazon recently reported fending off the world's largest known DDoS attack (Google estimates the attack peaked at 398 million requests per second making it more than 7x larger than the previous biggest attack) and warned security leaders at enterprises to invest in upping their game.

CHALLENGE 5

Bridging Perennial Skills Gaps



We've seen how AI can augment network security teams at every stage of the threat lifecycle by continuously asking the same questions analysts ask:

- Is this behavior suspicious?
- Are these incidents connected?
- Which anomaly should we investigate first?
- Can we fix this issue without losing business?

In doing so, AI should help validate and escalate incidents that require analyst attention within seconds or minutes instead of hours, days, weeks, and months. Saving time on detection and fast-tracking response changes the game for defenders, but AI that requires continuous tweaking by analysts consumes cycles of its own.

AI should be more self-sufficient

We've seen how AI enables fast, simultaneous scanning and visualization of incidents and how autonomous response can contain threats and avoid lengthy recovery efforts. AI that trains and maintains itself frees up even more analyst cycles for higher-level security operations (SecOps) such as incident response, threat hunting, threat and attack path modeling — things that improve your security posture to proactively prevent attacks.

Darktrace Self-Learning AI augments human efforts with:

- No steep up-front effort required to train the system
- Detailed incident reports that get delivered, consumed, and actioned within minutes
- Data to baseline risk and add to SOC teams' playbooks for fast-tracking investigations
- Integrations that extend existing investments in traditional network security so your "legacy" technology remains a modern asset

> The evolving threat landscape is leading to a shortage of cybersecurity professionals, with an estimated gap of 3.5M globally. This shortage will continue to be a concern in 2023, forcing companies to invest in training and retaining talent or outsourcing cybersecurity tasks. [4]
>
> **FORBES**

[4] Forbes, "Securing the Future: The Most Critical Cybersecurity Trends of 2023," Satish Shetty, 28 February, 2023.

CHALLENGE 6

Beyond Network: Implementing a Platform Approach

Movement away from standalone solutions suggests that a forward-looking network security strategy favors a holistic approach, one that unifies visibility across an entire network in one platform. That's clearly more efficient than aggregating piecemeal telemetry into actionable insights but must extend visibility beyond traditional borders.

Analysts now need to view risk in the broader context of local, remote, and third-party users transacting on-premises, across VPNs, in industrial environments, and multiple clouds. The faster individual investigations take place and incidents get resolved across domains, the more time security professionals get back. The end-goal then becomes extracting correlated insight from the "D/R" process to further streamline operations and avoid even more attacks.

AI drives comprehensive, business-wide protection

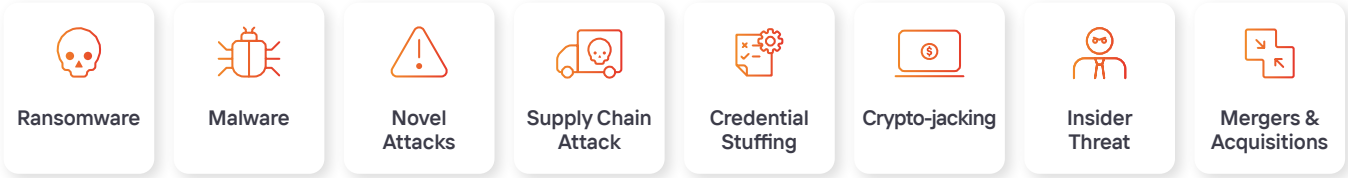
Darktrace's self-taught understanding of normal behavior in your network is augmented by insight into cloud, SaaS, endpoint, and email services for a holistic view of internal risk — but that's only one side of the coin.

Security should size up your network from the attacker's point of view.
Combining internal data from detection and response efforts with an external view of your network completes the puzzle for anticipating attacks. As the lifecycle renews, Darktrace's attack surface management (ASM) and attack path modeling capabilities let analysts see what threat actors see as they build targeted techniques to infiltrate and exploit your network.

The external view includes digital exposure from public-facing websites and code repositories, expired certificates, misconfigurations, abandoned domains, vulnerabilities, and more. Creating a cohesive view of internal and external risk makes AI better able to recognize anomalies that need immediate attention, but also allows IT to shut down exposure that traditional security controls can't even see.

Darktrace/Network: A Lifecycle Advantage

Neutralizes all network threats including:



Deployed in the world's largest, most complex digital environments, Darktrace/Network protects hundreds of thousands of devices at enterprises, small and midsized businesses (SMBs), government agencies, and critical infrastructure (CI) providers worldwide. Darktrace's self-taught understanding of normal behavior in your network helps to surface diverse threats ranging from 'low and slow' data theft to machine-speed ransomware.

Darktrace/Network goes beyond delivering complete and unified visibility — seeing threats in your environment and gaps in your security stack — to understand the significance of behaviors and autonomously resolve events. Detection triggers Darktrace's Cyber AI Analyst to investigate the full scope of an event on its own and generate a detailed incident report that can be consumed and actioned in minutes. Upon spotting deviations from normal activity, Darktrace/Network mounts an autonomous response to surgically interrupt attacks unfolding across your network without disrupting normal business operations. Detailed reports speed analyst reactions and inform future prevention.

Darktrace/Network bolsters defenses against modern attacks.
Leveraging Self-Learning AI, Cyber AI Analyst, and ASM capabilities, the Darktrace platform delivers four essential advantages needed to secure traditional networks against modern threats:

- End-to-end visibility into network and beyond
- Real-time anomaly detection
- Machine-speed behavioral analysis
- Surgical autonomous response

With these tools at their disposal, teams defending today's network can see, interrupt, and avoid modern attacks that count on the fact that the industry as a whole has its head in the clouds.

Customers' Choice for Network Detection and Response

Gartner Peer Insights Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates.

Learn more at darktrace.com/products

Contact Darktrace for a free demo today.

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. Breakthrough innovations from its R&D Centers have resulted more than 145 patent applications filed. Darktrace employs 2,200+ people around the world and protects over 9,000 organizations globally from advanced cyber-threats.

Scan to
LEARN MORE

DARKTRACE

Evolving threats call for evolved thinking™

North America: +1 (415) 229 9100
Europe: +44 (0) 1223 394 100
Asia-Pacific: +65 6804 5010
Latin America: +55 11 4949 7696
info@darktrace.com
darktrace.com