DARKTRACE 2024 Implementing and Enforcing Zero Trust Instructions

DARKTRACE 2024 Implementing and Enforcing Zero Trust

Contents

Introduction

of organizations have deployed a zero trust security architecture, while 41% haven’t IBM Cost of a Data Breach Report 2023

By 2025 45% of organizations worldwide will have experienced attacks on their software supply chains [Gartner]

Zero trust reduces the average cost of a data breach by $1M IBM Cost of a Data Breach Report 2023

The term “zero trust” describes a cyber security paradigm —a mindset for making important decisions—that aims to protect data, accounts, and services from unauthorized access and misuse. Zero trust describes a journey versus a particular collection of products or even a destination.

In fact, most experts agree that while zero trust charts the right path forward, its ultimate promise may never fully be achieved.

With digital risk and regulatory challenges looming large, this paper provides a timely update on:

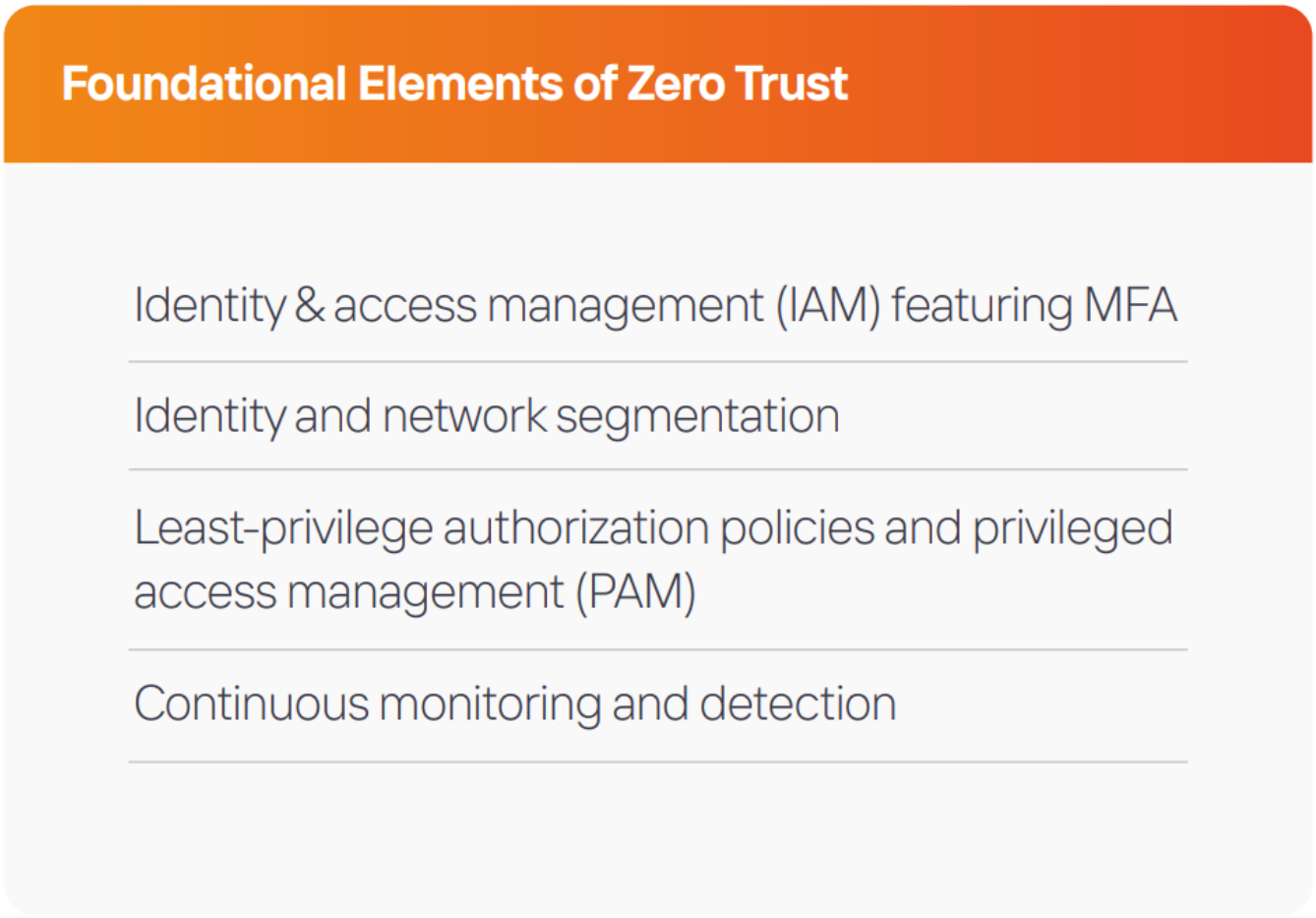
- The current state of zero trust cyber security
- Challenges and realistic goals for implementing and enforcing zero trust in 2024
- How smarter use of AI helps organizations advance quickly on their zero trust journeys

Where Do We Stand with Zero Trust?

Beyond the resounding hype, the principles behind zero trust remain sound. Legacy security presumes devices should be trusted simply because they were issued by trusted organizations. The implicit-trust model wasn’t working even before digital estates exploded with “bring your own device” (BYOD), remote work, and unprecedented interconnection to third parties via the cloud, home Wi-Fi, and legacy VPNs.

Zero trust replaces “castle and moat” with “trust but verify.”

A zero trust philosophy outlines a more dynamic, adaptive and realistic posture that assumes breaches have or will occur and seeks to reduce exposure by eliminating unnecessary access and maintaining dynamic control over privileges. In other words, building workflows that confirm those attempting to access company data are who say are and have only the privileges needed to get their jobs done.



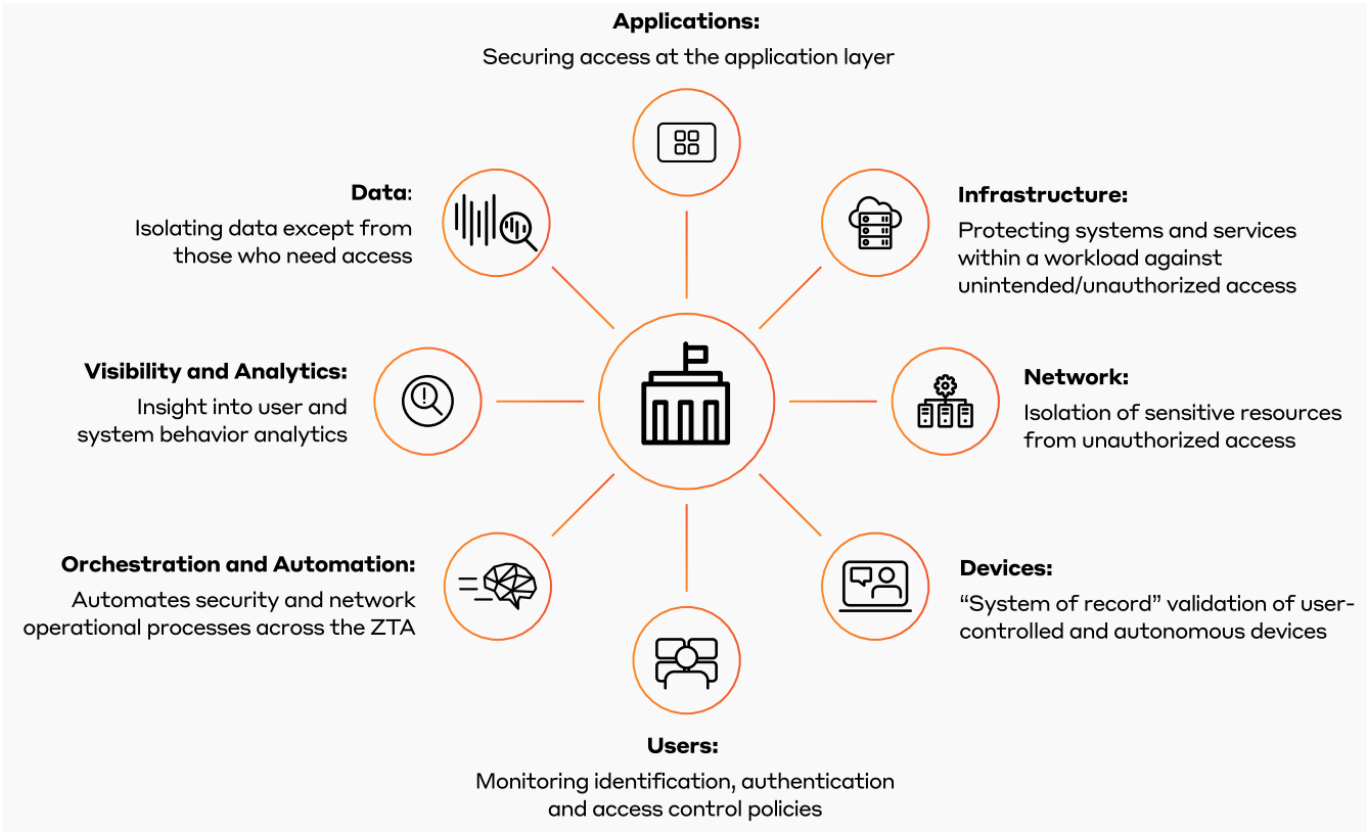
How are companies implementing zero trust?

To date, most zero trust strategies and technologies enforce guardrails via rules and policies. A zero trust security posture starts with requiring would-be users to verify their identity before devices can access company assets and privileged data.

As a foundational step, many organizations implement multi-factor authentication (MFA) to strengthen identity verification.

MFA improves upon reliance on user credentials by adding steps to complete authentication into systems. These include installing authenticator apps on smartphones, carrying hardware tokens, entering PIN numbers sent via email or text, and using biometrics (face, retina, and voice recognition scanners). Companies further along in their zero trust journeys may also adopt “least-privilege access” authorization policies to offset risks associated with insider threats and compromised identities. Least-privilege curtails lateral movement and resulting damage by limiting what users can do within your environment based on their role or function.

Figure 1: The eight pillars of zero trust [(U.S. General Services Administration)]



What needs to change in 2024?

E TO IMPLEMENTING AND ENFORCING ZERO TRUST IN 2024 3 What needs to change in 2024? Back in 2020, remote work ignited the first sustained wave of the zero trust movement. Vendors raced to release point products and security teams rushed to install them and start ticking the boxes.

With that initial crisis behind us, and early investments in technologies coming due for review, organizations can reassess plans and goals for zero trust with a pragmatic eye. Ongoing digitalization and use of cloud — not to mention a slew of changing industry and federal regulations — make moving the needle on your zero trust journey imperative for 2024.

Security leaders must think holistically about:

- What the desired end-state should look like.
- Where they are in their overall zero trust journeys.
- Which technologies and approaches have or will deliver the greatest value.
- How to enforce, evaluate, and maximize the value of investments on a continuous basis.

Because zero trust outlines a multi-year journey, strategies must reflect the fact that attack surfaces continue to change with artificial intelligence (AI) enabling unprecedented attack scale, velocity and security stacks ballooning in complexity as companies struggle to keep up. Even “legacy” approaches to zero trust itself must continue to modernize and incorporate AI to keep pace with today’s machine-speed risk.

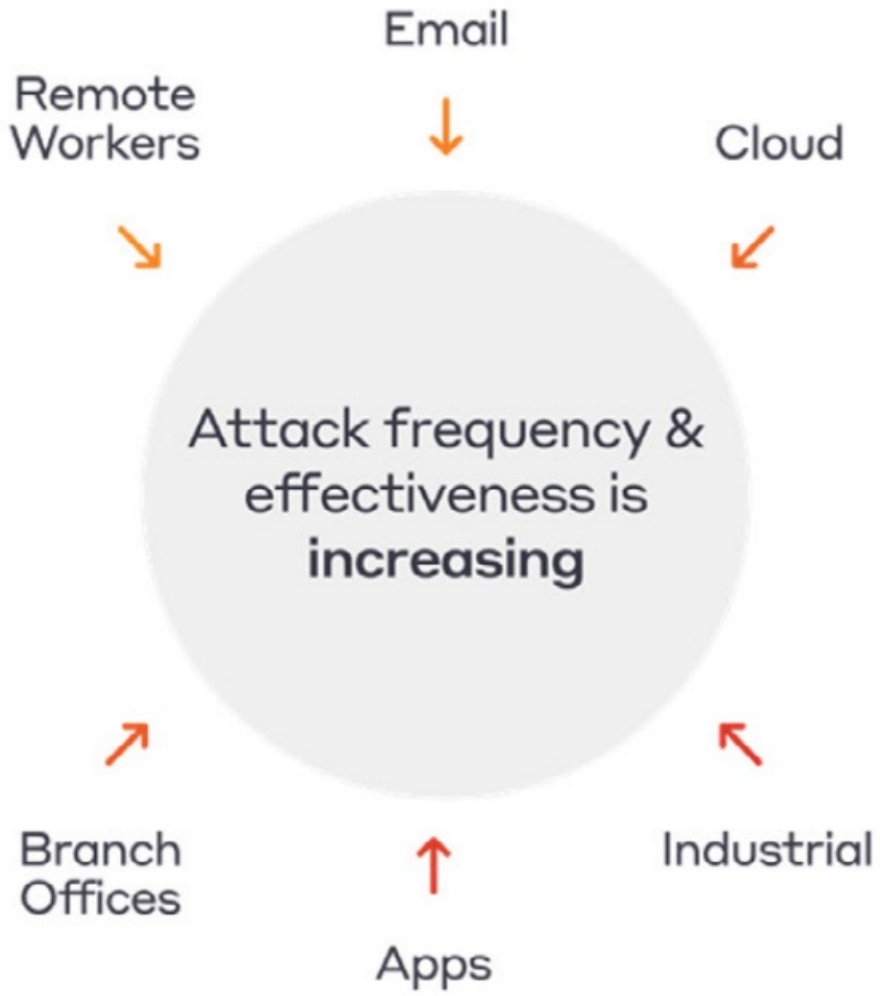
The time is right

A multi-layered approach to security based on AI and machine learning (ML) aligns well with the facts that:

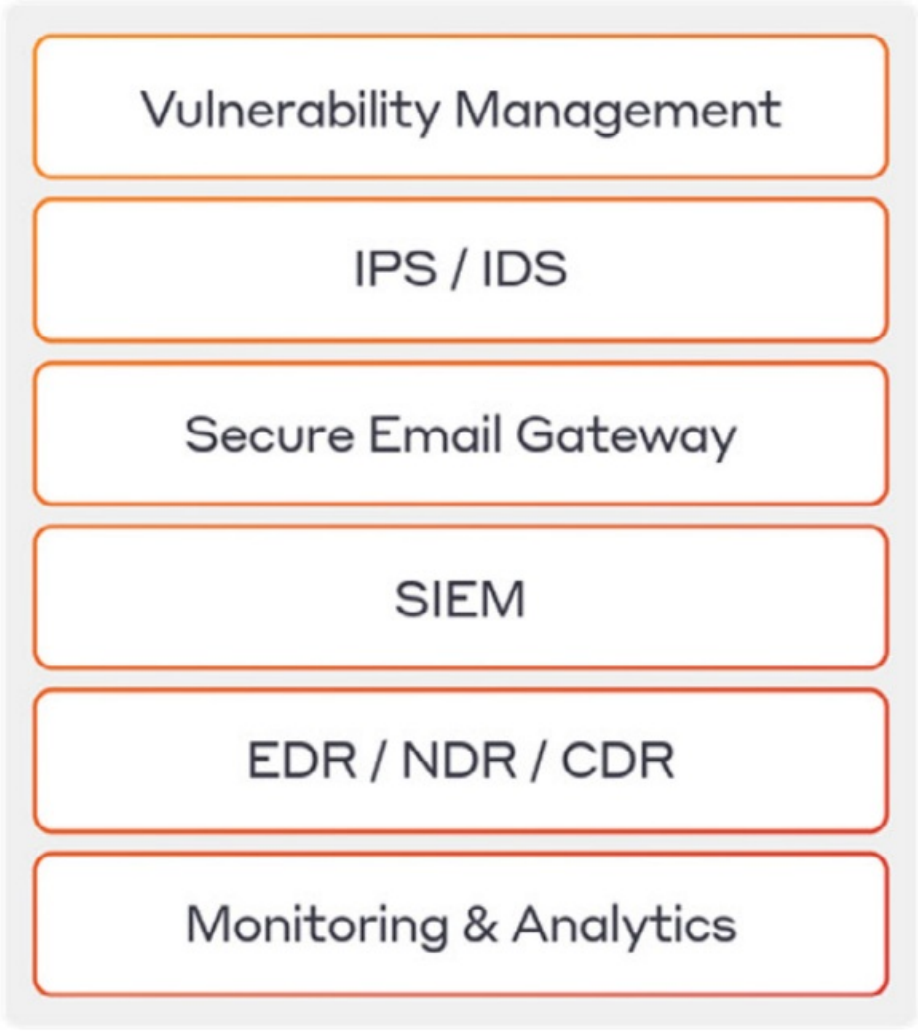
- Zero trust is more a philosophy and a roadmap than a collection of point technologies and checklist items.
- The ultimate goal of security investment is not in fact more security, but rather less risk.

As we'll see, the right approach to AI makes significant advances on the zero trust journey more practical and viable than ever before.

- **Figure 2: Attacker sophistication is increasing while the security stack gets more costly and time-consuming for IT staff**
    - Attackers are exploiting an expanding attack surface



    - Security stack proliferation increases cost



- Complexity consumes staff resources

Challenges to Moving the Needle in 2024

Zero trust technologies alone fail to provide a ‘one-stop-shop’ solution to every security problem, so strategies must evolve to the next level to bring the desired results closer.

Near-term goals for 2024 should include:

Moving beyond checking boxes

For starters, the industry must evolve beyond viewing zero trust from the perspective of point products and even line-item requirements within standards and guidelines set forth by the likes of NIST, CISA, and MITRE ATT&CK. Instead, we should view zero trust as a “true north” guiding principle and litmus test for every investment, making sure security postures become more preventive and proactive in eliminating risk.

Raising the bar on strong authentication

MFA, while a foundational element of zero trust, can’t provide a magic bullet, either. Adding multiple steps and devices to the authentication process becomes “too much of a good thing” that frustrates and makes users less productive. Threat actors even build targeted attacks based on the reality that, the more users experience “MFA fatigue,” the more likely they’ll be to click “Yes, it’s me,” when they should be clicking “No” to authentication requests

Worse yet, MFA that retains passwords as the first authentication factor may fail to meet its ultimate goal: stopping phishing that leads to compromised credentials and, in turn, to 80% of all security breaches [1]. When trusted identities become compromised, neither MFA nor the controls that follow will automatically detect when an imposter starts acting strangely

Managing trust dynamically

Security leaders continue to wrestle with the question of “how much trust is enough?” Clearly, the answer can’t always, or perhaps ever be “zero” or you couldn’t do business. A real-world approach to zero trust balances the challenges of a connected world with ensuring users prove their identity on a dynamic basis.

Static protection undermines zero trust

Legacy security systems were designed to protect static data at centralized locations like offices and datacenters. Traditional security tools lose visibility, and their ability to respond, when employees shift to working from home, hotels, coffee shops, and other hot spots.

Static role-based security fails to keep pace as today’s digital estate—and risk—grows more dynamic. Once someone “proves” their identity to MFA’s satisfaction, full trust kicks in. The user (or intruder) gains the full access and authorizations linked to that identity.

Without constant dynamic updates, zero trust security becomes “point in time” security. Policies grow dated and decrease in both value and effectiveness.

[1] Verizon, 2022 Data Breach Investigations Report

Insider threats, supply chain risk, and novel attacks fly under the radar

Defaulting to allowing trusted users’ actions to proceed undeterred makes detecting insider threats and third-party attacks much more challenging. Security that watches for previous threats also has no reason to flag novel attacks

that increasingly use AI to generate new techniques on the fly

Enforcing zero trust autonomously

Cyber security by necessity remains hyper-focused on detection. Security leaders acknowledge that modern threats arise too quickly for defenses to spot everything, and that investigating every alert proves counterproductive and may allow more threats to slip by undetected.

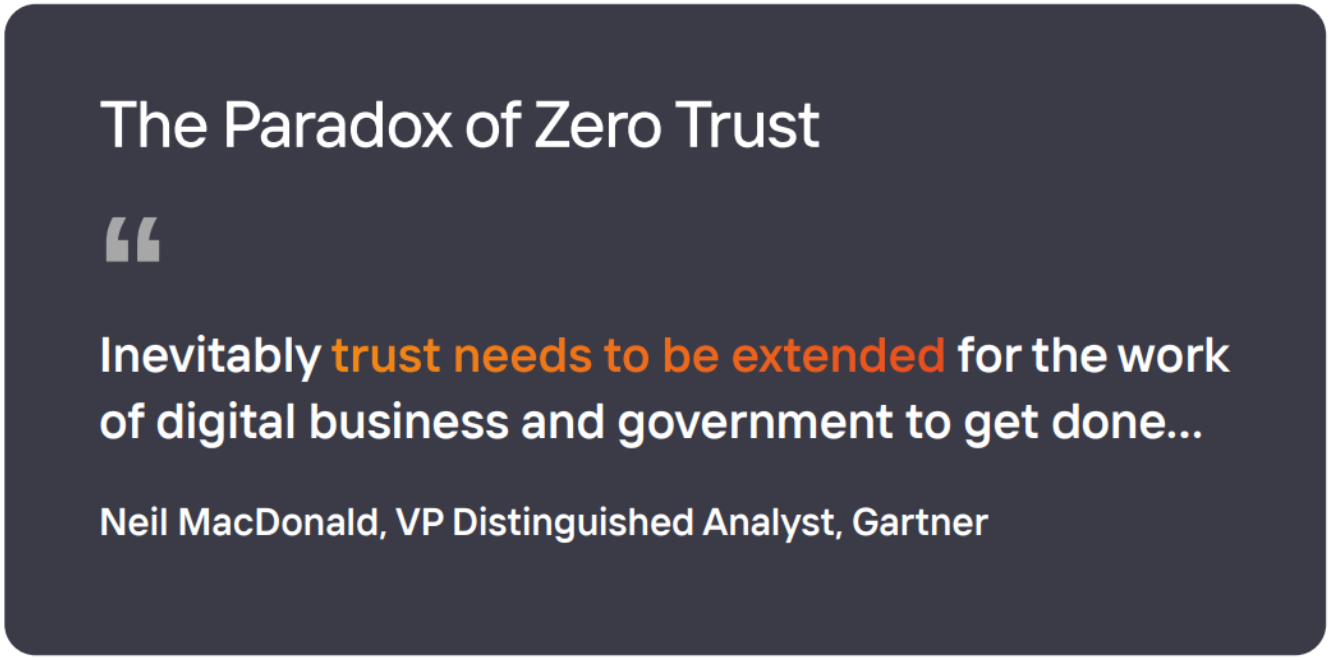
Zero trust requires autonomous response for complete protection.

Monitoring and detection play an invaluable role in implementing zero trust but the pivotal lever for netting full value from investments is getting to the point where security solutions mount the right response in real time, all on their own.

Overcoming resource gaps

Companies of all sizes battle constant constraints from a global cyber-skills shortage. For small and medium-sized organizations, the complexities of zero trust, privileged access management (PAM), and even MFA may seem out of reach from a sheer resource standpoint.

The long-term impact of any investment in cyber security on operations should be to reduce risk—and advance adoption of zero trust—while also lowering cost and the effort required to maintain technologies themselves. Companies must take care to ensure the next steps on their zero trust journeys don't overtax resources short-term.



Darktrace Self-Learning AI Advances the Zero Trust Journey

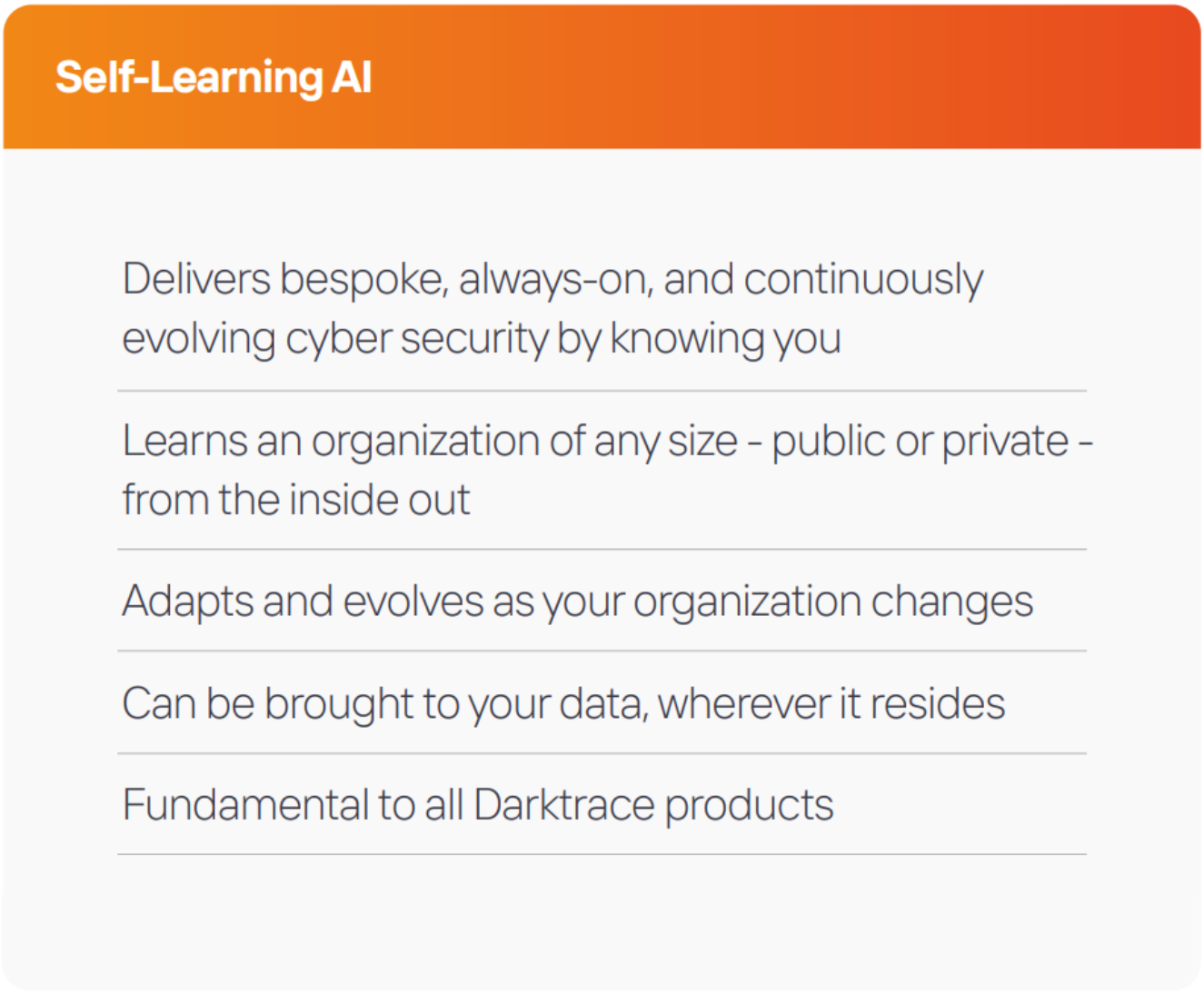
Darktrace uniquely bridges the gap between the vision and reality of zero trust. The platform takes a dynamic, adaptive approach to implementing zero trust across heterogenous, hybrid architectures that include email, remote endpoints, collaborative platforms, cloud, and corporate network environments [operational technology (OT), IoT, industrial IoT (IIoT), and industrial control systems (ICS)].

Darktrace taps into the ethos of what zero trust promotes — dynamic, adaptive, autonomous, and future-ready cyber security protection. Unique in its ability to inform and enforce policies continuously as your environment

changes, the Darktrace platform adds a cohesive overlay that uses multi-layered AI to:

- Improve trust management
- Mount an autonomous response
- Prevent more attacks
- Bridge resource gaps
- Pull the pieces of zero trust together in a cohesive, agile, and scalable framework.

Darktrace Self-Learning AI analyzes data points for every laptop, desktop, server, and user, to ask:"Is this normal?"



Self-Learning AI uses your business as a baseline

Darktrace Self-Learning AI builds a complete picture of your organization everywhere you have people and data and maintains an evolving sense of 'self' bespoke to your organization. The technology understands 'normal' to identify and piece together abnormalities that indicate cyber threats. Rather than rely on rules and signatures, the platform analyzes patterns of activity and never defaults to presuming actions should be trusted by virtue of source.

Darktrace Self-Learning AI looks beyond established trust to detect, investigate, and respond immediately to telltale signs of risk other solutions ignore. No matter how long users stay logged in, the platform notices immediately when device activity seems inconsistent. Darktrace's Cyber AI Analyst indiscriminately inspects asset

activity (data, apps, devices) for suspicious behavior that might signify insider and advanced persistent threats (APTs), nation states, and third-party identities “gone rogue.”

The system immediately calls out these subtle deviations in behavior like visiting different websites, unusual clustering activity, strange login times, and attempts to use different systems. The AI continuously updates its own working definitions of normal, ‘benign’ and ‘malicious.’

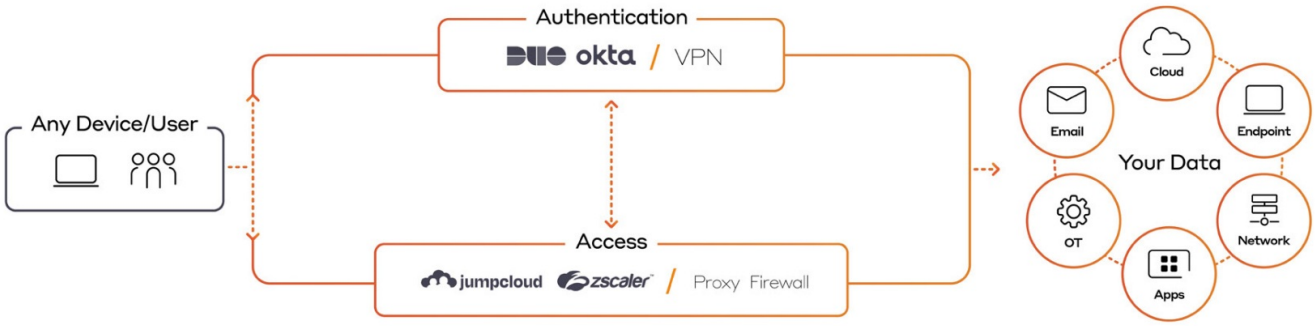
Continuous Self-Learning AI enables the system to:

- Spot novel threats at the first indication
- Perform effective autonomous response actions to interrupt attacks with surgical precision
- Investigate and report on the full scope of security incidents
- Help harden your security posture across your entire digital estate as your business evolves

Security your zero-trust journey

Figure 3: Darktrace continues to monitor even once a user has been authenticated, so it can spot when malicious activity occurs despite the enforcement of zero trust rules and policies .

- **Under Darktrace / Zero Trust Protection**



Early detection conserves resources

Self-Learning AI promotes faster detection that helps prevent attacks from happening. When the WannaCry and SolarWinds breaches struck in 2017 and 2020, investigations showed Darktrace had been notifying customers of anomalous behaviors for several months before other solutions alerted on signs of a possible breach. Autonomous response early in the attack kill chain reduces triage time and the administrative burden on Internal SOC teams exponentially. In keeping with the zero trust “assume the breach” philosophy, the ability to detect anomalous behavior on the part of trusted users – and automatically enforce normal behavior while you investigate – adds an invaluable failsafe for enterprise security.

Dynamic protection promotes greater trust

Having Self-Learning AI and Autonomous Response underpinning your zero trust strategy allows trust management to become more adaptive and continuous. So long as defenses can detect unusual behavior the second it happens, enterprises can grant greater trust with greater confidence, assured that Darktrace will step in automatically when needed.

Autonomous response makes zero trust a reality

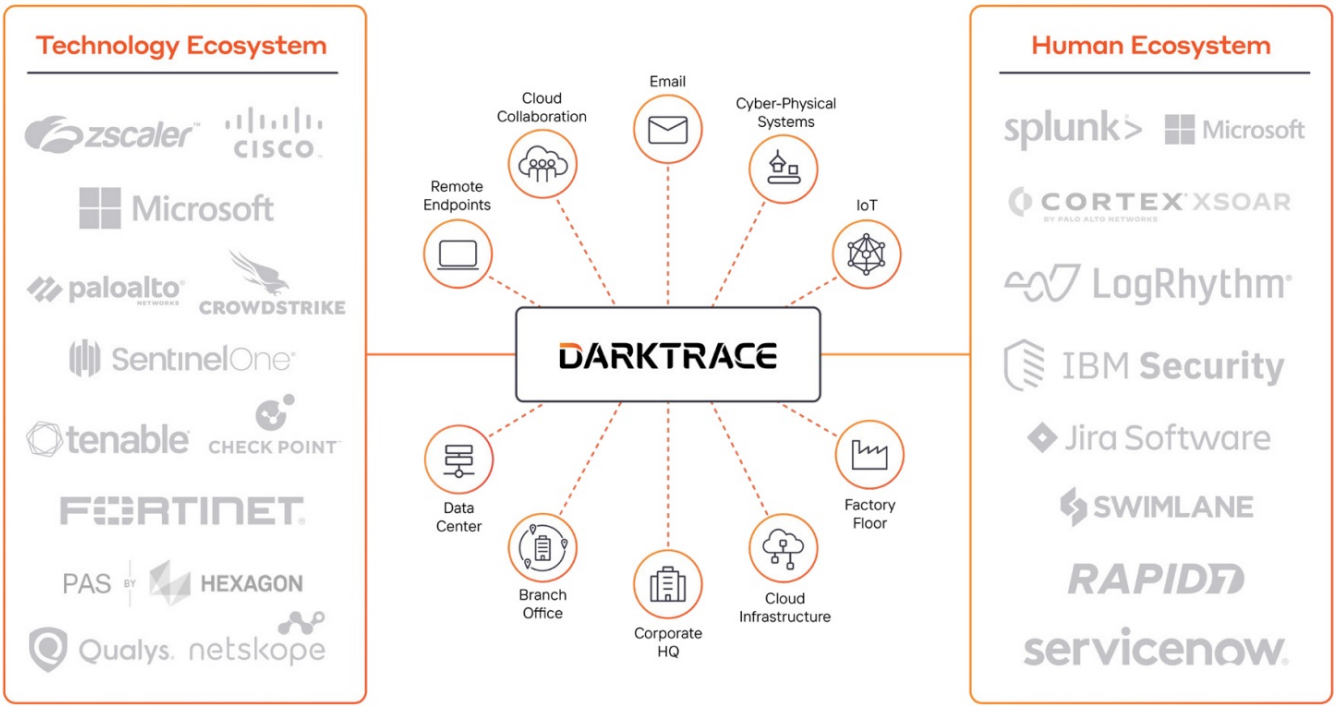
Enforcement is critical to maximizing the value of your zero trust investments.

Darktrace complements and enhances existing investments in zero trust postures by identifying, disarming, and investigating threats that get by defenses, even if they operate over legitimate paths. When trust barriers get breached despite the implementation of zero trust rules and policies, Darktrace autonomously enforces normal behavior to resolve and halt lateral movement. The platform can instantly alert and trigger a response proportionate to the attack. Autonomous actions include surgical responses like blocking connections between two endpoints or more aggressive measures like complete termination of all device-specific activity.

A cohesive approach pivots security toward prevention

A lifecycle, platform-based approach to assessing and enforcing zero trust should include constantly managing your digital risk and exposure with an eye toward prevention. To this end, the Darktrace platform includes attack surface management (ASM), attack path modeling (APM), and innovative use of graph theory that equips security teams to monitor, model, and eradicate risk.

Figure 4: Darktrace interoperates with zero trust technologies, validating zero trust policies and informing future micro-segmentation efforts



Pulling it all together

Unified visibility and response ensure a cohesive approach and amplify the benefits of individual zero trust solutions. Darktrace helps your team pull all the pieces of your strategy together and move forward.

APIs streamline integration

As you implement zero trust, your data gets funneled to multiple point products. Darktrace **integrates with Zscaler, Okta, Duo Security, and other leading zero trust solutions** to enhance visibility and response.

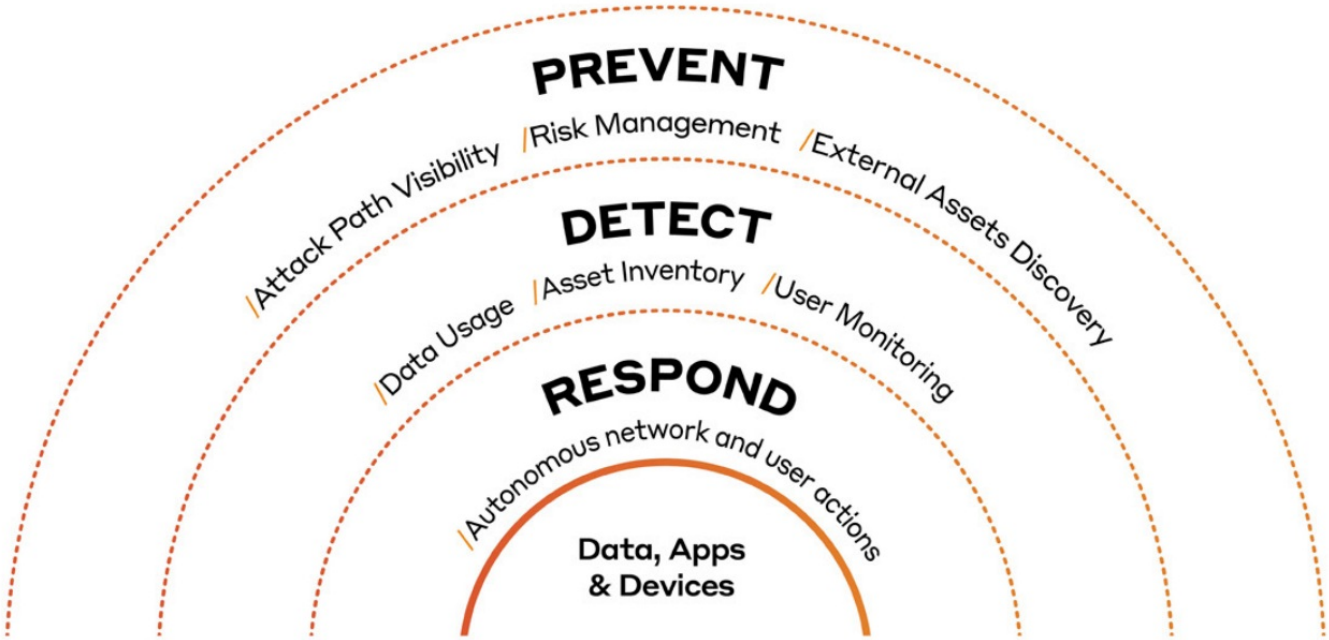
When deployed with these technologies, the scope of activity visible to Darktrace widens along with AI's ability to analyze, contextualize, and act via the relevant APIs as necessary.

Native API integrations allow organizations to:

- Accelerate their adoption of zero trust architectures
- Feed data into Darktrace's Self-Learning AI engine to Identify and neutralize anomalous behaviors
- Validate current zero trust policies and inform future micro-segmentation

Securing zero trust architecture at every layer

Figure 5: Darktrace supports key zero trust tenants throughout every stage of an incident lifecycle – securing what matters most to your business



The “What to Do Next in 2024?” Checklist

To bridge the gaps between the promise and reality of zero trust in 2024, strategies must eclipse buzzword and even “check box” status. Before taking their next steps, security leaders should review and update implementation plans holistically with an eye toward moving beyond buying point tools.

The first step should be choosing a holistic, adaptive platform that can deliver unified visibility, mount an autonomous response, and streamline operations. Questions to ask in baselining progress on this journey — and formulating achievable, measurable goals for 2024 — include:

1. How do we scale security when the perimeter and user base is constantly expanding?
2. Do we have all the elements we need to ensure successful movement toward zero trust?
3. Do we have the right zero trust products in place?
   Are they configured and managed correctly?
4. Have we thought through oversight and governance?
5. Can we consistently enforce our zero trust strategy?
   Does enforcement include autonomous response?
6. How do we evaluate and calculate the value of existing and potential investments?
7. Are we still getting phished? Able to spot insider threats?
8. Do we have (and have a way to spot) “access float”?
9. Can we ensure access and identity controls remain adaptive and keep pace with the business?
10. Does our zero trust strategy evolve dynamically and continuously without analyst intervention?

Take the next step

Once you complete a gap analysis, your organization can prioritize and develop step-by-step strategies for hardening your zero trust security posture over time with smarter, more effective use of machine learning and AI.

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.

Customer Support

Scan to LEARN MORE

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

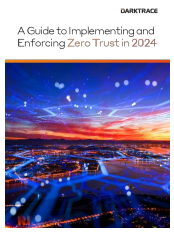
info@darktrace.com

darktrace.com

DARKTRACE

Evolving threats call for evolved thinking™

Documents / Resources

	**DARKTRACE 2024 Implementing and Enforcing Zero Trust** [pdf] Instructions 2024 Implementing and Enforcing Zero Trust, 2024, Implementing and Enforcing Zero Trust, Enforcing Zero Trust, Zero Trust

References

- **Darktrace | Cyber security that learns you**
- **Start Your Free Trial | Darktrace**
- **Self-Learning AI for Zero Trust Environments | White Paper | Darktrace Resource**
- **User Manual**