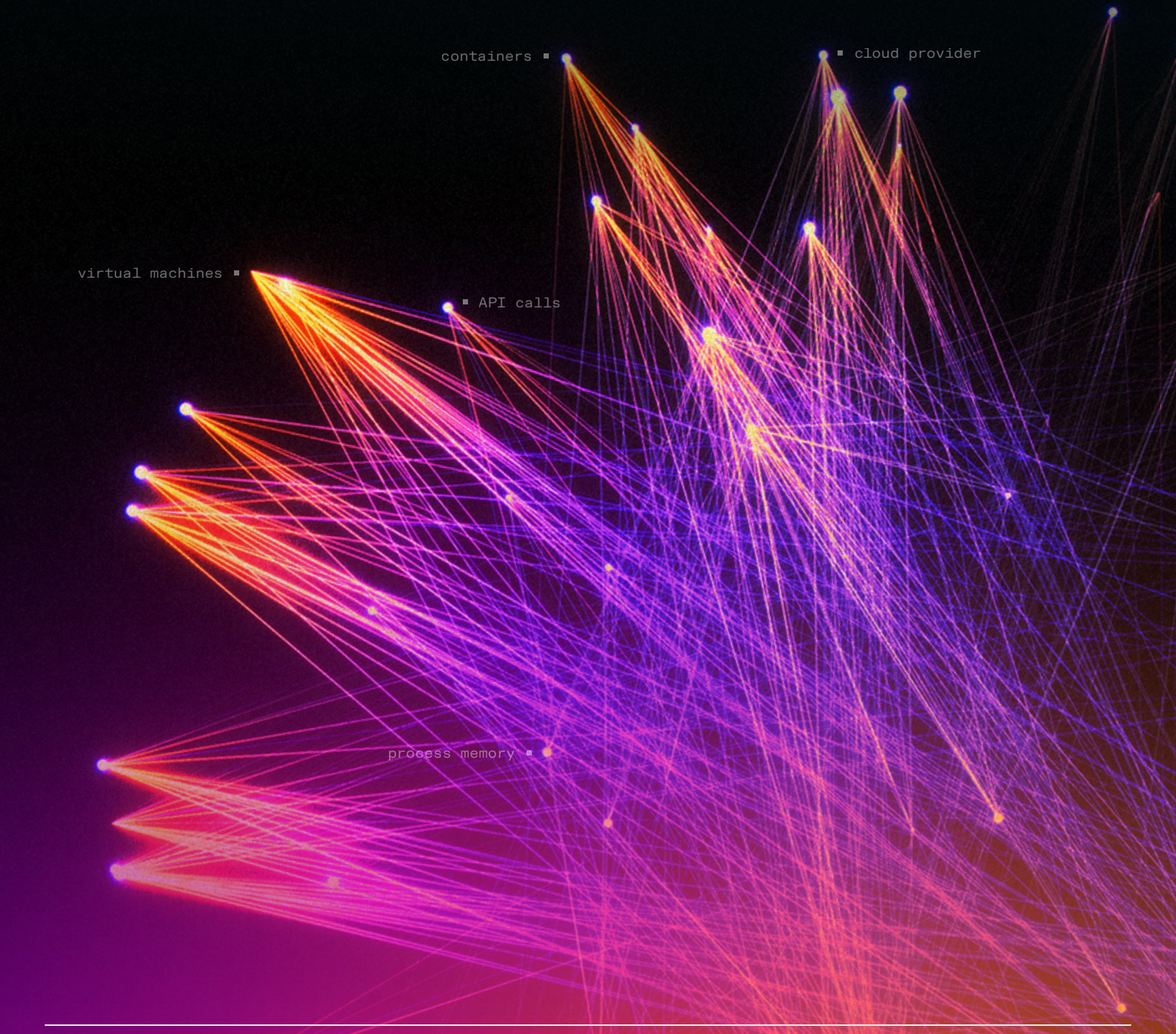
DARKTRACE

From Detection to Resolution:

Enhancing CDR with Advanced Forensics



Contents

Abstract

As organizations continue to embrace digital transformation and migrate their operations to the cloud, the security landscape has evolved dramatically. Traditional on-premises security tools and approaches often fall short when it comes to protecting dynamic cloud infrastructure.

This gap has given rise to a new category of security solutions: Cloud Detection and Response (CDR). In this comprehensive guide, we'll explore what CDR is, why it's crucial for modern organizations, and how it can be further enhanced with cloud forensics.

The cloud security challenge

Before diving into CDR, it's important to understand the unique security challenges posed by cloud environments:

Rapid scalability:
Cloud resources can be spun up and down in minutes, making it difficult to maintain visibility and control.

Shared responsibility model:
Cloud providers secure the infrastructure, but customers are responsible for securing their data and applications.

Complex architectures:
Multi-cloud and hybrid cloud environments create intricate ecosystems that are challenging to monitor and secure.

New attack surfaces:
Cloud-native technologies like containers and serverless functions introduce new potential vulnerabilities.

Increased attack sophistication:
Adversaries are developing cloud-specific Tactics, Techniques, and Procedures (TTPs) to exploit cloud environments.

These challenges have created a need for security solutions specifically designed for cloud environments. Enter CDR.

What is CDR?

CDR is a combined solution that enables continuous monitoring, threat detection, and incident response capabilities. This allows organizations to quickly identify and respond to security threats in their cloud environments.

The key components of a CDR capability include:

- Continuous monitoring of cloud activity and configurations
- Threat detection leveraging cloud-native detections, logs, and telemetry
- Automated investigation and contextualization of alerts
- Incident response capabilities tailored for cloud environments

Below, we explore each of these components in more detail.

Continuous monitoring

CDR solutions provide real-time visibility into cloud environments by continuously collecting and analyzing data from various sources, including:

- Cloud provider logs
  - e.g., AWS CloudTrail and Azure Activity Logs
- API calls and management plane activities
- Resource configuration changes
- Identity and Access Management (IAM) activities
- Application and workload logs

This comprehensive monitoring allows organizations to maintain a clear picture of their cloud estate and detect anomalous activities quickly.

Threat detection

CDR platforms leverage advanced analytics, machine learning, and threat intelligence to identify potential security threats in cloud environments.

Some key threat detection capabilities include:

Behavioral analysis:
Identifying unusual patterns of activity that may indicate compromised credentials or insider threats.

Known threat detection:
Recognizing Indicators of Compromise (IoCs) associated with known malware or attack campaigns.

Misconfiguration detection:
Identifying security misconfigurations that could leave resources vulnerable to attack.

Compliance violations:
Detecting activities that violate regulatory requirements or organizational policies.

Automated investigation

When a potential threat is detected, CDR solutions can automatically gather additional context and evidence to help analysts quickly understand the scope and severity of the incident.

This may include:

- Collecting relevant logs and telemetry data
- Capturing snapshots or images of affected resources
- Performing initial triage to determine the likelihood of a true positive
- Correlating the alert with other related events or indicators

Incident response

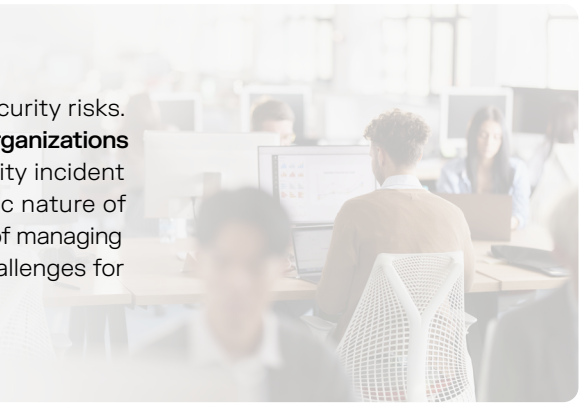
CDR platforms provide cloud-native incident response capabilities to help organizations quickly contain and mitigate threats.

These may include:

- Automated response actions
  - e.g., isolating affected resources and revoking access tokens
- Integration with existing Security Orchestration, Automated, and Response (SOAR) platforms
- Guided response playbooks for common incident types
- Forensic data collection and preservation for in-depth investigations

Why is CDR important?

As cloud adoption accelerates, so do the security risks. According to our recent survey, over **90% of organizations** have experienced some form of cloud security incident in the past year. The ephemeral and dynamic nature of cloud resources, coupled with the complexity of managing multiple cloud environments, creates new challenges for security teams.



Some key reasons why CDR is critical:

Improved visibility:
CDR provides deeper visibility into cloud activity, configurations, and potential threats across your entire cloud estate. This comprehensive view is essential for maintaining a strong security posture in complex, multi-cloud environments.

Faster threat detection:
By leveraging cloud-native telemetry and advanced analytics, CDR can detect threats more quickly than traditional tools. This speed is crucial in cloud environments where attackers can rapidly spin up and down resources to evade detection.

Reduced alert fatigue:
CDR solutions can provide richer context around alerts, helping prioritize and reduce false positives. This allows security teams to focus on the most critical threats and avoid wasting time on benign activities.

Cloud-specific response capabilities:
CDR enables faster, more effective response to cloud incidents through automation and cloud-native remediation. This is particularly important given the ephemeral nature of cloud resources and the potential for rapid lateral movement in cloud environments.

Regulatory compliance:
Many compliance standards now require organizations to implement cloud-specific security controls and monitoring. CDR solutions can help organizations meet these requirements and demonstrate due diligence in securing cloud environments.

Cost optimization:
By providing visibility into resource usage and potential security risks, CDR can help organizations optimize their cloud spending and avoid unnecessary costs associated with misconfigured or compromised resources.

Support for DevSecOps:
CDR solutions can integrate with Continuous Integration and Continuous Deployment (CI/CD) pipelines and provide security feedback early in the development process, supporting a shift-left approach to cloud security.

Key capabilities of CDR solutions

When evaluating CDR platforms, some essential capabilities to look for include:

Multi-cloud support:
The ability to monitor and protect workloads across major cloud providers like AWS and Azure, as well as hybrid cloud environments.

Cloud-native telemetry:
Ingestion and analysis of cloud provider logs, API calls, VPC flow logs, container logs, and other cloud-specific data sources.

Cloud-aware threat detection:
Integration with cloud sources for detection logic that understands cloud-specific attack vectors and TTPs, including those targeting serverless functions, containers, and managed services.

Automated investigation:
Capabilities to automatically gather context and evidence around alerts, reducing the time and effort required for initial triage.

Cloud-native response:
Ability to take response actions via cloud provider APIs, such as isolating resources, revoking access, or applying security group changes.

Integration with existing tools:
Seamless integration with SIEM, SOAR, ticketing systems, and other security tools to fit into existing workflows.

Scalability and performance:
The ability to handle large volumes of data and scale horizontally to support growing cloud environment.

The role of forensics in CDR

While many CDR solutions focus primarily on real-time monitoring and detection, the importance of forensic capabilities should not be overlooked. Cloud forensics presents unique challenges due to the distributed and ephemeral nature of cloud resources.

Key benefits of integrating forensics into your CDR strategy include:

Comprehensive evidence collection:
Forensic tools can capture a complete snapshot of affected resources, ensuring no critical evidence is lost.

Deep analysis capabilities:
Forensic analysis can uncover subtle indicators of compromise that may be missed by real-time monitoring alone.

Historical investigation:
Forensic data allows for in-depth investigation of past events, even if the original resources are no longer available.

Compliance and legal requirements:
Proper forensic data collection and preservation is often necessary for regulatory compliance and potential legal proceedings.

Root cause analysis:
Forensic investigation can help identify the root cause of incidents, informing long-term security improvements.

By combining real-time monitoring and detection with robust forensic capabilities, organizations can build a more comprehensive and effective CDR strategy.

Automated data collection

When an alert is triggered, the ideal cloud security tool should automatically collect full forensic data from the relevant cloud resources.

This includes:

- Disk images of virtual machines and containers
- Process memory snapshots
- Cloud provider logs and metadata
- Application and system logs

This automated collection ensures investigators have all the data they need, even if the original resource has been terminated. This is particularly valuable in cloud environments where resources may be short-lived or quickly changed.

Deep forensic analysis

Cloud security today should leverage advanced forensics techniques to extract critical artifacts and timeline data from collected evidence. This automated analysis provides rich context around alerts, helping analysts quickly understand the full scope of an incident.

Key capabilities include:

- File system analysis to identify malicious or suspicious files
- Log parsing and correlation to reconstruct event timelines
- Malware detection and analysis
- User and account activity profiling

Cloud-native architecture

Built specifically for the cloud, the ideal security tool should scale horizontally to process large volumes of data in parallel. This cloud-native architecture enables rapid investigations, even for large enterprise environments.

Benefits include:

- Distributed processing for faster analysis of large datasets
- Automatic scaling to handle varying workloads
- Cost-effective storage of forensic data using cloud object storage

Multi-source data ingestion

In addition to collecting data directly from cloud resources, the ideal cloud security solution should ingest data from a variety of sources including:

- Endpoint Detection and Response (EDR) and eXtended Detection and Response (XDR) tools
- Logs in cloud storage and APIs
- Cloud Security Posture Management (CSPM) solutions
- Threat intelligence feeds
- Custom log sources

This provides a centralized platform for cloud investigations, allowing analysts to correlate data from multiple sources and gain a comprehensive view of security incidents.

Automated reporting and integration

The ideal security tool should automatically generate detailed reports on investigations and integrate with ticketing systems, messaging platforms, and other tools to streamline workflows.

This includes:

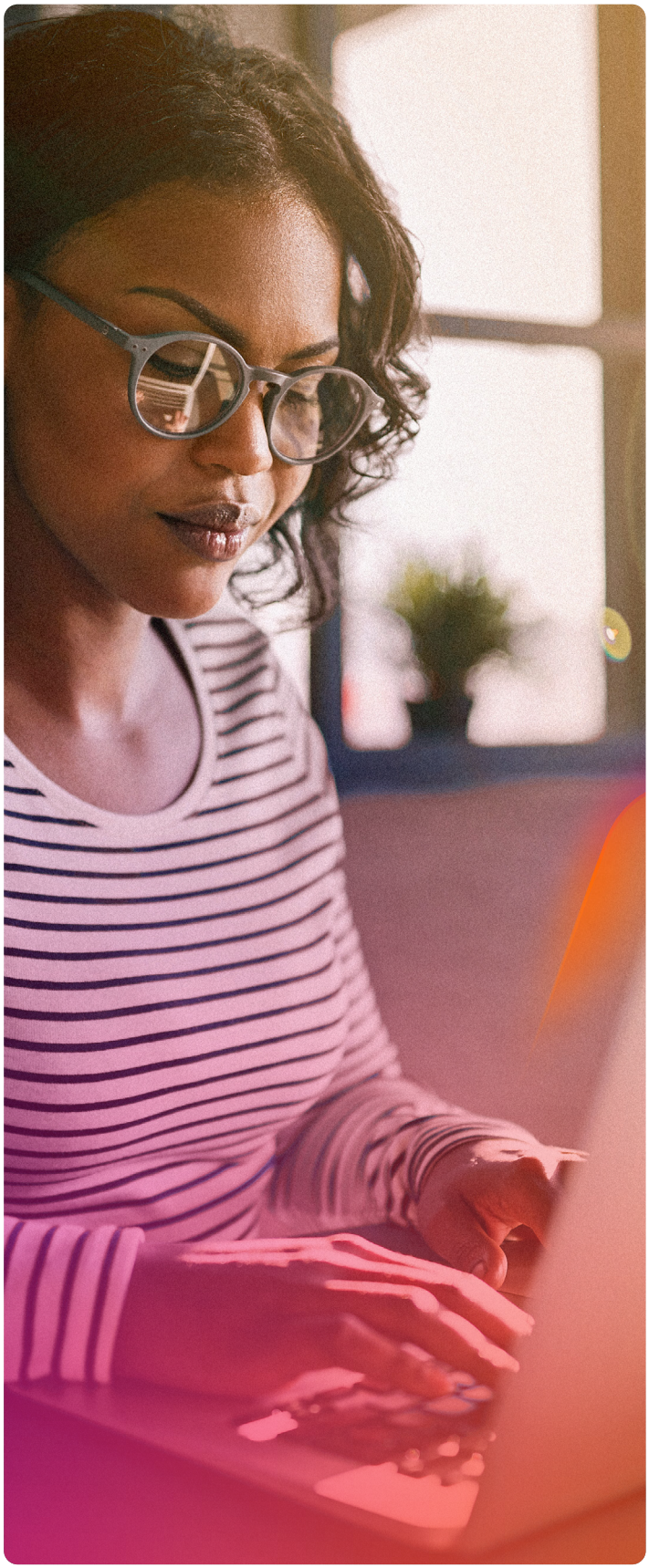
- Customizable report templates for different stakeholders
- Integration with popular ticketing systems like Jira and ServiceNow
- Automated alerting via Slack, Microsoft Teams, or email
- API-based integration for custom workflows

Advanced threat hunting capabilities

In addition to automated analysis, the ideal cloud security solution should provide advanced threat hunting capabilities that allow skilled analysts to perform deep, targeted investigations.

These include:

- Custom search and filtering options across all collected data
- Visual relationship mapping to identify connections between entities
- Timeline analysis tools for reconstructing attack sequences
- YARA rule support for detecting specific indicators of compromise



Bringing it all together: A comprehensive CDR strategy

An effective CDR strategy combines continuous monitoring, threat detection, automated investigation, and streamlined response. By leveraging cloud-native technologies and automation, organizations can dramatically improve their abilities to detect and respond to cloud security incidents.

Here's an overview of what a comprehensive CDR strategy might look like:

Implement continuous monitoring:
Deploy CDR tools to continuously collect and analyze data from all cloud environments, including multi-cloud and hybrid setups.

Establish baseline behavior:
Use analytics to understand normal patterns of activity in your cloud environment, making it easier to detect anomalies.

Develop cloud-specific detection rules:
Create and maintain a set of detection rules tailored to your cloud infrastructure, taking into account common attack vectors and your organization's unique risk profile.

Automate initial triage:
Use CDR platforms to automatically gather context and perform initial analysis of potential threats, reducing the workload on human analysts.

Integrate with existing workflows:
Ensure your CDR solution integrates seamlessly with your existing security tools and processes, including SIEM, SOAR, and ticketing systems.

Implement automated response actions:
Define and implement automated response playbooks for common incident types to enable rapid containment and mitigation.

Conduct regular threat hunts:
Use advanced threat hunting capabilities to proactively search for hidden threats or IoCs that may have evaded automated detection.

Continuously improve:
Regularly review and update your detection rules, response playbooks, and overall CDR strategy based on new threats, lessons learned from incidents, and changes in your cloud environment.

Train and educate staff:
Ensure your security team is well-versed in cloud technologies and CDR tools and provide ongoing training to keep skills up to date.

Leverage managed services:
Consider partnering with Managed Detection and Response (MDR) providers specializing in cloud environments to augment your internal capabilities.

Darktrace / CLOUD makes CDR accessible to all security teams and SOCs

Darktrace / CLOUD™ is a real time CDR solution built with advanced AI. By using multiple machine learning techniques, Darktrace brings unprecedented visibility, threat detection, investigation, and incident response to hybrid and multi-cloud environments.

In addition to autonomous detection and response, Darktrace / CLOUD accelerates the investigation process with Cyber AI Analyst™, which examines all relevant events in the cloud to analyze alerts, correlate incidents across different domains, and produce investigation summaries to reduce your security team's time to meaning.

Darktrace / CLOUD typically provides SOCs with up to 50,000 additional hours of Level 2 analysis and written reporting annually, enriching security operations by producing high level incident alerts with full details so that human analysts can focus on Level 3 tasks.

Darktrace / CLOUD is part of the greater Darktrace ActiveAI Security Platform™, the industry's widest domain coverage that correlates real-time information from across the organization to provide unparalleled visibility into multi-domain attacks. It covers cloud, network, email, identities, endpoints, and Operational Technology (OT).

Darktrace's cloud offerings have been bolstered with the acquisition of Cado Security Ltd., which enables security teams to gain immediate access to forensic-level data in multi-cloud, container, serverless, SaaS, and on-premises environments.

Conclusion:
The future of cloud security

As cloud adoption continues to accelerate, the importance of robust CDR capabilities will only grow. Organizations must adapt their security strategies to address the unique challenges posed by cloud environments, embracing cloud-native technologies and automation to stay ahead of evolving threats.

Learn more about Darktrace / CLOUD for

AWS ↗

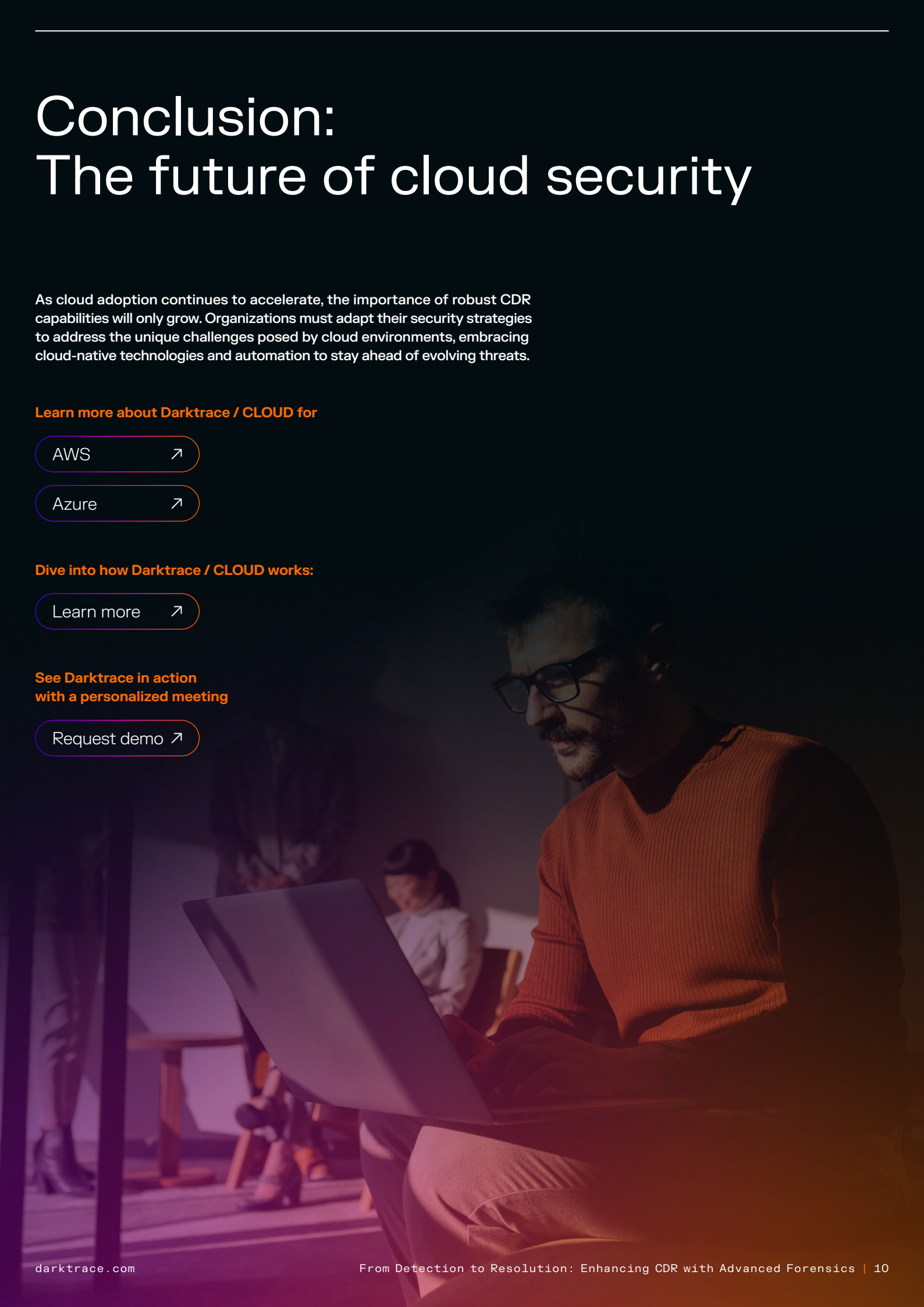
Azure ↗

Dive into how Darktrace / CLOUD works:

Learn more ↗

See Darktrace in action with a personalized meeting

Request demo ↗



About Darktrace

Darktrace is a global leader in AI cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace's platform and services are supported by 2,700+ employees who protect nearly 10,000 customers globally. To learn more, visit www.darktrace.com.

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

darktrace.com | info@darktrace.com