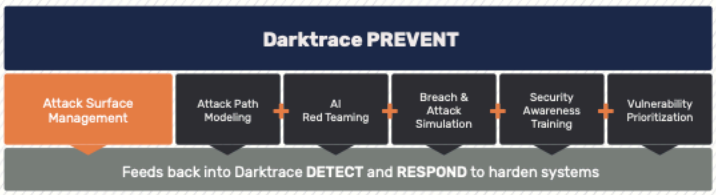
Darktrace PREVENT empowers security teams to reduce the cyber risk to their organizations by prioritizing vulnerabilities and hardening defenses – continuously improving an organization's security posture. Powered by Self-Learning AI, which delivers visibility into every digital asset, employee, and device, PREVENT identifies and fortifies areas of high risk internally and externally, making it possible to anticipate and avert attacks. At the same time, PREVENT also enables the CISO and security staff to prioritize vulnerabilities and autonomously strengthen defenses by providing feedback to Darktrace DETECT and RESPOND.

THE IMPORTANCE OF HARDENING YOUR DEFENSES

Attackers today are using more automation, targeting supply chains and shadow IT, and leveraging new techniques in their attack campaigns. As the threats change, security approaches and operations need to evolve to manage cyber risks to prevent downtime, compromises, or incidents. It's also a matter of efficiency as many organizations find themselves expanding their use of infrequent, manual expert testing to try to identify vulnerabilities that require yet more manual effort from IT teams to patch systems.

While there are point products that aim to address different aspects of the problem, most are siloed and single point-in-time. And in the case of pen tests, most become tick-box exercises for companies to remain in compliance - but do not support action. Security teams can be left with a mountain of vulnerability information to work through, much of it irrelevant to the security risks the executives care about.

INTRODUCING THE DARKTRACE PREVENT PRODUCT FAMILY



In response Darktrace PREVENT delivers the first end-to-end solution with a comprehensive set of capabilities designed to strengthen the security posture internally and on the attack surface. It empowers the CISO and security staff to become an AI-powered Red Team, simulating attacks, identifying critical assets and testing pathways of vulnerability, then shoring up defenses to prevent attackers from reaching vital systems and data. The product suite also includes Attack Surface Management to reduce cyber risk originating outside the organization

PREVENT capabilities automate and uplevel these processes within the Darktrace Cyber AI Loop, which orchestrates a set of dynamically related, cyber threat capabilities that function continuously by preventing, detecting, responding, and healing from cyber disruption.

DARKTRACE PREVENT

As cyber-attacks become more complex, often pivoting through multiple fields of operation, it gets harder to anticipate where the next attack will come from and where to utilize your resources.

Darktrace PREVENT assesses the strategic risks facing your organization, giving you the ability to prepare for attacks before they happen. It runs millions of wargame scenarios to identify the attack paths most likely to be exploited and which would achieve maximum damage to your organization. The end-to-end solution delivers a range of functions, working autonomously, including Attack Surface Management, Attack Path Modeling, AI Red Teaming, Breach & Attack Simulation, Security Awareness Training, and Vulnerability Prioritization.

KEY ASSET IDENTIFICATION

Works out the potential impact of compromising any given target – whether the target is an individual user, a collection of assets, or an operational workload.

INTELLIGENT PRIORITIZATION

Looks at every possible sequence of cyber-attacks, assessing which are most likely and which can cause the most damage. Reveals which pre-emptive security areas will optimize damage and risk mitigation to the greatest extent. It shows you which areas of improvement should be tackled, in which order.

OPERATIONAL RISKS

Contains pre-built templates for commonly identified risks such as ransomware and tracks changes to these risk levels.

ATTACK PROJECTION

Tests the initial foothold of each attack path to ensure its viability with simulated attack campaigns. These attacks are intelligently targeted, trying the best attack on the users who could cause the greatest potential damage to the organization if they were compromised.

HARDENS DEFENSES

Feeds data into Darktrace's continuous Cyber AI Loop, bringing more context to what it already knows, and hardening your defenses.

DARKTRACE PREVENT/ATTACK SURFACE MANAGEMENT

Darktrace Attack Surface Management (ASM) gives you unparalleled visibility into the parts of your organization that are exposed to the outside world – allowing your security team to proactively identify risks before an attack takes place. The solution continuously monitors the external attack surface, assessing all your assets for risks, high-impact vulnerabilities, and external threats.

Darktrace ASM is used by businesses to reveal shadow IT, supply chain risks, potential phishing domains, vulnerabilities and misconfigurations, and risks arising from mergers and acquisitions.

ABOUT DARKTRACE

Darktrace (DARK:L), a global leader in cyber security AI, delivers world-class technology that protects over 6,800 customers worldwide from advanced threats, including ransomware and cloud and SaaS attacks. Darktrace's fundamentally different approach applies Self-Learning AI to enable machines to understand the business in order to autonomously defend it. Headquartered in Cambridge, UK, Darktrace has more than 2,000 employees worldwide. Darktrace was named one of TIME magazine's 'Most Influential Companies' for 2021.

CONTACT US

North America: +1 (415) 229 9100
Europe: +44 (0) 1223 394 100
Asia-Pacific: +65 6804 5010
Latin America: +55 11 97242 2011
info@darktrace.com | darktrace.com
@darktrace