# Hot news

## Enterprise Immune System Protect Enterprise from Cyber Attacks

Today's attackers are silent and stealthy, motivated to not only steal data and deface websites, but damage infrastructure and undermine data integrity, potentially ruining reputations in the process. iCON business systems Limited, will introduce the latest technologies which can protect enterprise from these attacks.

DARKTRACE

**Q Linuxpilot A iCON Business Systems Limited**

**Q What is the biggest challenge of nowadays network security?**

**A** Cyber security has become an AI arms race. We are already seeing artificial intelligence being used in cyber attacks. For example, polymorphic malware that changes its attributes mid-attack to evade detection. We've also seen the targeting of non-standard devices like interconnected biometric sensors, coffee machines, video conferencing devices and printers.

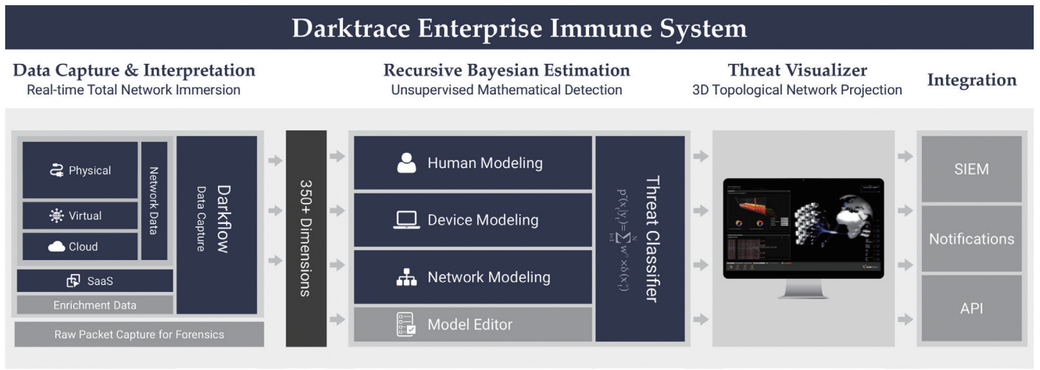
**Q How can Darktrace overcome these challenges?**

**A** As cyber criminals launch increasingly sophisticated, fast and automated attacks, defenders will have to respond with smart technology that automatically recognize threats and deals with them. With AI algorithms that learn about every user and device, organizations develop a sense of their 'self'. In this way, they can detect abnormal behaviors as they occur and respond automatically, buying security teams precious time to catch up. 85% of networks are already infiltrated in some way, so we must assume that the threat is already inside. This is Darktrace's approach. The Enterprise Immune System uses genuine machine learning technology and AI to effectively 'self-learn' normal behaviors and identify abnormal activity, without relying on the rules and signatures of pre-categorized threats.

**Q How does Darktrace work?**

**A** Every day our bodies are exposed to new bacteria and viruses and whilst our skin stops most from getting in, some will inevitably get through and infect us. This is where the human immune system comes into play by identifying and killing dangerous pathogens. Darktrace's Enterprise Immune System is modelled on the human immune system and uses advanced mathematics and unsupervised machine learning i.e. machine learning that does not require any human pre-programming, to defend organizations big and small.


Compromise of Biometric Control System.




Darktrace Enterprise Immune System.

Our approach is capable of mapping all digital activity across the network and creates a baseline of what is the 'pattern of life' for every user, device and network as a whole. In this way, organizations can understand what 'normal' looks like for their unique infrastructure and can identify and respond to abnormal behavior, before damage is done. Darktrace enables humans to prioritise real threats and takes measured action to quickly neutralise in-progress threats, before the security team has arrived on the scene.

**Q How are these machine learning and probabilistic mathematics being developed?**

**A** These technologies are driven by world-leading mathematicians. The foundations of Darktrace's unique approach lie in cutting-edge machine learning and mathematics developed at the University of Cambridge. The founders of Darktrace include senior members of the UK government's cyber community from MI5 and GCHQ, and they have former Director of MI5 sits on the advisory board. Darktrace's team has now expanded to include experts from intelligence communities globally, such as the NSA and CIA, with backgrounds ranging from threat analysis to senior intelligence positions.

**Q What kind of attack can be stopped by Darktrace?**

**A** By applying its unique, unsupervised machine learning, Darktrace has identified 30,000 previously unknown threats in over 3,000 networks ranging from more traditional types to novel zero-day attacks, insider threats, ransomware and 'trust attacks' to name a few.

**Q Are there any successful cases? What kind of attack has been stopped?**

**A** Darktrace has been deployed in a number of organizations in Hong Kong. One example of a real-world attack in Asia-Pacific is the infiltration of a biometric scanner on the secure facility at a manufacturing company.

When we installed Darktrace, we started to see unusual Telnet connections to and from a particular device – that device turned out to be the biometric scanner, which was hooked up to the corporate network.

When we investigated, we saw that an external party had compromised the scanner through software vulnerabilities on the main network, and had started to replace legitimate biometric data with different data, quite possibly the attacker's own fingerprints.

This was very serious because it meant that the attackers were well on their way to gaining physical access to the plant, through this digital compromise. No signature existed for that type of threat and it would have gone unchecked by legacy controls. Fortunately, we were able to flag it to the organization in time to avoid a physical intrusion and potentially catastrophic damage.

Darktrace has been deployed in a number of organizations in Hong Kong. One example of a real-world attack in Asia-Pacific is the infiltration of a biometric scanner on the secure facility at a manufacturing company.

Darktrace Threat Visualizer.

**Q What is the pricing model? Is it affordable for SMEs?**

**A** Darktrace is deployed in organizations big and small, from a top 5 FCMG company to a small bakery in Singapore. Pricing is bespoke to the organization's individual network.

**Q Is it going to be a trend of using machine learning at security industry?**

**A** It is very difficult to get machine learning working in practice, on real networks with live data. The network is one of the most difficult concepts to learn about as it is incredibly complex and dynamic. Darktrace's machine learning is incredibly powerful – it leverages the interplay of supervised and unsupervised machine learning and a layer of Bayesian probabilistic mathematics to detect threats and decide what the best action is. Ultimately, machine learning – when done right – turns traditional approaches on their head. Rather than trying to predefine and predict the future, machine learning is about embracing uncertainty.

**Q How can enterprises prove Darktrace works for them, and the value can be justified and measured?**

**A** We can arrange a product demonstration for potential customers. Darktrace is delivered as a physical appliance, which is easily and rapidly installed within an hour, at a SPAN or TAP port within the customer network. The appliance passively monitors raw network data in real time, without disrupting business operations, and provides instant visibility into all network activity, notifying security teams of in-progress attacks or emerging anomalies. Customers only need to tell us which subnet Darktrace should be installed, and customer will be able to obtain the details about their network activities after 1-2 weeks.

**iCON Business Systems Limited**
Website: https://www.icon-info.com.hk/
Tel: 852 2748 3698