DARKTRACE

WHITE PAPER

The Enterprise Immune System

Embracing Probability to Deliver
Next-Generation Cyber Defense

Executive Summary

Darktrace takes a fresh approach to the challenge of countering sophisticated attackers coming from the outside or the inside of an organization, based on advanced machine learning and mathematics.

If we look back to medieval times, the concept of a walled hill town was common, whereby the people inside the town walls were trusted and the people on the outside were not. This model was reassuring and worked well, until the interests of growth and trade made it necessary for all sorts of individuals to interact with each other. The modern city thus came into being based on dynamic collaboration and interaction – and no city walls in sight. The most modern and successful cities in the world are complex places and continue mile after mile.

The benefits of collaboration and interaction are clearly fundamental to progress, and we have seen this in the cyber security area too. Where walls are put up, they will often be overcome, not only by malicious attackers but also by company employees who choose to bypass security controls in order to do their jobs efficiently. As we consider risk assessment, it is important to remember that your employees will not always take the path that you have chosen for them.

Data is not only at risk of being illegally taken out of the organization, but also being unknowingly changed. Whereas data loss or theft loss is undesirable, it is usually obvious when it has happened. Much more difficult is the challenge of knowing when the integrity of data has been compromised. A high premium is put on the confidence that we place in our critical data, so what happens when 10,000 bank account balances are changed, but the bank is unable to identify which ones?

A new approach that pays attention to very subtle actions that happen very quietly will be critical to winning the battle against cyber attackers. It is a battle that has been played out in the biological world too for billions of years. Our DNA represents information that is constantly under attack from a variety of viruses. Whilst we cannot live in plastic bubbles and avoid these viral attacks, we have an immune system that understands what 'self' is, knowing what is part of 'us' and therefore identifying what is abnormal and not 'us'.

Dealing with the unexpected in this way is crucial in our ability, as human beings, to protect against major threats to our health while interacting and collaborating with each other. Darktrace helps companies strike this balance by delivering an immune system for the enterprise that calculates probabilities of threats in the light of evidence. Based on proven machine learning and mathematics, it allows organizations to stay close to their employees, supply chain and customers, whilst protecting against serious, sophisticated threats. This self-learning technology offers the first practical way to deal with our new cyber reality, when we don't always know when there is a fire to fight.

The Threat Is Inside

While the traditional approach to security relies on a distinction between inside and outside, the reality is that boundaries are virtually impossible to define within modern infrastructures, and threat actors are already on the inside. Today's information systems and networks are global, complex and porous – they need to be in order to work and prosper in the modern world. But this makes them vulnerable to exploitation too.

Today, all companies face risk from within their own walls from a variety of individuals and groups, including their employees and contractors, supply chain and customers, as well as malicious parties that have infiltrated the organization. Ongoing attacks that transpire week by week, often hitting the headlines and entailing serious damage to the victim company's reputation and revenues, show that traditional methods are not working.

It is no good building a wall around a system that is already infiltrated and inherently at risk. Such walls are also largely inhibitive to the efficiency and speed with which the modern business is expected to act. Companies are in danger of suffering from the double negative impact of damaging their competitiveness and productivity, due to overzealous data restrictions, and at the same time remaining extremely vulnerable to both insider threats and sophisticated external attackers.

The real 'cyber security' challenge is not about 'securing' our information systems – it is about accepting probability and understanding what is really going on from the inside of complex information environments. It is an illusion to think that if we have a lock and a key, we can achieve perfect security. In reality, we know that locks break and keys can be copied – and there is no perfect answer. The best solution must allow companies to continue to expose themselves to all sorts of risks, in the interests of running global, connected and competitive businesses.

> "Good cyber security is not just about a really strong wall on the outside, but some kind of an immune system within."
>
> Lord Evans of Weardale, former Director General, MI5

Wrong Assumptions: Why the Traditional Approach Is Failing

There are three key reasons why the traditional IT security approach to cyber security has failed.

1. You can't keep threat out
The traditional approach to security assumes that you can keep attackers on the outside of your networks, by strengthening your boundaries. Organizations have invested large amounts of time and money into perimeter controls and network reconfiguration with the goal of keeping their information systems free from infiltration.

Unfortunately, the majority of corporate networks have been infiltrated in some way already. Threat actors have proven themselves capable of overcoming perimeter controls, and employees and other insiders with access to the network pose a significant risk too. We have to work on the basis that we are constantly at risk and that many threats, and certainly the most insidious, will get into an organization with relative ease.

2. You can't define what is illegitimate
Creating definitions and policing information according to those definitions lies at the heart of traditional information technology. This core IT principle, widely used for all manner of automated applications, has duly been transmuted to the cyber security field. Indeed, there is a wide range of solutions that aim to create definitions of what 'bad' looks like, and proceed to protect you against that type of 'bad', if and when it is encountered again, in exactly the same way.

Whilst this approach may protect against unsophisticated attackers that use the same toolkit and tactics repeatedly, it is widely known that the most serious attackers are very good at what they do – they change their strategies all the time and use bespoke malware designed to conquer a specific target.

Furthermore, for this rules-based approach to work to any level of accuracy, constant software updates are required, although inevitably fail to keep up with the pace of constantly-evolving attack tactics. It is reactive and incapable of defending against fresh, ever-changing threats as they happen.

3. The threat is not purely technical
It can be easy to forget the human at the end of every cyber mission, in a world of botnets, Trojans and Remote Access Tools. It is important to remember that serious cyber threats are directed by skilled people who move deftly and subtly around the network. The traditional black and white approach described above is incapable of dealing with the complexity and delicacy that such attackers bring to their missions.

Both external and insider parties usually exhibit identifiable characteristics or warning signs before engaging in malicious acts. A contractor logging into the network at an unusual time of day, groups of files being aggregated, the set-up of a new employee account or the volume of email traffic through a particular server – these are all signs that are often insignificant individually but form a compelling picture when correlated.

In addition to the human nature of the attack mission, we should remember that the human vulnerability of employees and insiders is often used and exploited by attackers. Socially-engineered attacks are on the up, and aim to dupe innocent-minded insiders into taking a certain action. Whilst training can help reduce this, it is impossible to stop all your employees taking the wrong decision every time.

The challenge of cyber and IT security executives is to embrace probability, taking into account the subtleties of human behaviors. This requires seeing and understanding subtle, weak indicators that point to human intent and activity from within the network, in order to detect the emerging threat behaviors of the astute individuals behind every potential threat.

Protecting Data Integrity – It's Not Just About Data Loss

The nature of risk has changed, broadening to encompass a whole range of ways in which damage can be inflicted. One major concern is around data leakage, loss and theft, with the proliferation of individuals and groups of individuals who want to take data because of its inherent financial value (such as credit card details), its economic value (such as manufacturing designs) or its political insights (such as government documents).

This is a worrying phenomenon, but perhaps more concerning still is that today's information environments allow for data to be changed, without this being detected. Whether you are an insider or an external hacker, once you are on the inside, your access to data and your ability to change that data, or parts of it, is very difficult to stop. With a little malicious intent, very serious problems can arise. Imagine a situation where even your back-up is corrupted.

Ensuring data integrity is absolutely central for most businesses in order to operate in the public market. For a healthcare organization handling patient blood types or a bank managing its customers' bank balances, the prospect that critical data could be compromised in some way has the potential to destroy public confidence in their products or services and put them out of business.

When we think about how to solve the problem of cyber-attacks, we need to think beyond isolated data leaks or website hacks and take in the bigger implications of large infrastructures being compromised and confidence destroyed. Edward Snowden proved that even the best-defended and most security-conscious organizations are vulnerable to subtle, lone attackers who move silently within their systems and have the ready means to disproportionately undermine their entire operation.

> "A key element of improvement involves acknowledging the importance of human behavior when designing, building and using cyber security technology."
>
> Institute for Information Infrastructure Protection, 2013

Insider threat

The threat from people inside the organization is massively underestimated – perhaps because it is an extremely difficult problem to solve. We need to entrust our employees and partners with certain access rights to allow them to do their jobs, and yet at the same time, we cannot trust all of them to take the right decision, all of the time. Some may fall victim to phishing attacks and unwittingly help an attacker get in; others may have a grudge or other motivations that drive them to abuse their privileges with malicious intent.

Insider threat does not only come from our employees, but anyone with access to the network, corporate data or company premises, which makes policing insiders challenging. Modern enterprises thrive on the interconnectedness between them and their supply chain, customer base, contractual workers and other partner organizations and individuals. Today's corporations have expanded their networks accordingly, opening up their organizations to increased risk for the sake of fluid, efficient and competitive business operations.

There is a wide range of reasons why an insider could be inspired to act, either unwittingly or with deliberate intent, including financial gain, ideology, desire for recognition, loyalty to family or friends and general disaffection. With a range of personalities and motivations involved, it is impossible to identify high-risk users in advance.

Rather than analyze 'who did it' or try to second guess 'who might do it', the real challenge is to identify such attacks and understand how they develop in real time – by analyzing and correlating the subtle signs of compromise that each insider makes as they move within the network.

Insider incidents do not need to be at the scale of Edward Snowden or Bradley Manning to do significant damage to your reputation or business. In spite of the improvements to internal security in the majority of enterprises, we know that insider attacks are still feasible to carry out in spite of legacy security tools and good practise. Indeed, as network boundaries become more and more porous, the definition of those inside and outside the organization has lost its relevance. One way or another, today's threats are carrying out the bulk of their missions from within the firewall. We need to learn and interpret the behaviors of all users, devices and networks in order to spot real adversaries in a world in which everyone is – or can become – an insider.

Introducing the Enterprise Immune System

Darktrace has pioneered a fundamentally new approach to the cyber challenge, known as the Enterprise Immune System, which is based on the assumption that organizations face a constant level of threat from within. This emerging category represents cutting-edge technology that is capable of learning 'self' within an organization on an adaptive, real-time basis – thereby understanding when abnormal behavior starts to manifest itself.

Like viral DNA, which constantly mutates and evolves to ensure its survival within the human body, cyber attackers are sophisticated and constantly change and tweak their behaviors in order to avoid detection. Fortunately for us, the immune system is just as clever as viral DNA – it is continually learning and understanding what constitutes a threat. It's not a perfect system – sometimes we catch the odd cold – but generally it does a great job at protecting us from serious illnesses. In doing so, it allows humans to interact with each other and expose themselves to risk on a day-to-day basis. Because human beings thrive on social interaction and collaboration, living in a sterile glass box is not an option for us – and it is not an option for modern enterprises either.

Darktrace's innovative approach is based on complex mathematics that calculates probabilities in the light of evidence. This probabilistic method of detecting anomalies is the most pragmatic and accurate way of protecting against unknown attack vectors operating within complex network environments. Enterprise Immune System technology iteratively learns a pattern of life for every network, device and individual user, correlating this information in order to establish an overview pattern of life and thereby spot deviations that indicate live, in-progress threats.

This new approach does not require prior knowledge of threats, looking instead for any behaviors that are probabilistically determined to be anomalous and therefore worthy of investigation. An Enterprise Immune System therefore gives organizations the ability to get ahead of threat for the first time, and remediate emerging suspicious activity before major damage is done. It also allows threat analysts to focus on truly concerning incidents that are likely to be seriously threatening, rather than producing floods of undifferentiated alerts.

This ability to self-learn and adapt to changing environments in real time represents a step change for organizations around the world, enabling them to reconcile their need for an interconnected workforce, customer base and supply chain, whilst ensuring that they protect against serious, existential threats to their businesses in the most effective way possible.

> "The key is detecting that you have been breached as quickly as possible and having the systems in place to protect your vital assets."
>
> John Colley, International Information Systems Security Certification Consortium, 2013

Mathematics and Machine Learning 'Done Right'

The core of Darktrace's innovative approach lies in a breakthrough in probabilistic mathematics made at the University of Cambridge. Bayesian theory is known for its ability to draw meaning from large sets of data, and a new branch of this field of mathematics, named Recursive Bayesian Estimation (RBE), is central to the development of Darktrace's founding technological innovation.

By mathematically characterizing what constitutes 'normal' behavior, based on the analysis of multiple data sources, RBE mathematics succeeds in identifying changing attack behaviors where conventional signature-based methods fall down. Powered by RBE, Darktrace's mathematical models are constantly adapting themselves in real time, according to the new information that it processes, and continually providing calculations of threat levels.

Darktrace also uses 'Sequential Monte Carlo' or particle filter techniques to maintain a distribution over the probability state variable. This distribution is built from a complex set of low-level host, network and traffic observations or 'features'. These features are recorded iteratively and processed in real time on the platform.
A plausible representation of the relational information among entities in dynamic systems in general, such as an enterprise network, a living cell or a social community, or indeed the entire internet, is a stochastic network, which is topologically rewiring and semantically evolving over time.

In many high-dimensional structured I/O problems, such as the observation of packet traffic and host activity within an enterprise LAN or WAN, where both input and output can contain tens of thousands, sometimes even millions of inter-related features (data transport, host-web-client dialogue, log change and rule trigger, etc.), learning a sparse and consistent structured predictive function is challenged by a lack of normal distribution.

In this context, Darktrace has pioneered the most advanced, large-scale computational approach to learn sparse structured I/O models by extending the L1-regularized regression model (the lasso method) to a family of sparse 'structured' regression models. This allows for the discovery of true associations between linked malware and C2 events (inputs) and data egress (outputs), which can be cast as efficiently solvable convex optimization problems and yield parsimonious models.

Acute methods for estimating and analyzing varying coefficient models with structural changes occurring at unknown times or locations are required for Enterprise Immune System technology. Instances of such models are frequently encountered in social and biological problems, where data is structured and longitudinal, and the IID assumptions on samples being generated from an invariant underlying model no longer hold.

For example, at a given time point, the observations (such as a snapshot of the social state of all actors) are distributed according to a model (such as a network) specific to that time, and therefore cannot be directly used for estimating models corresponding to other time points.

Darktrace has pioneered Bayesian methods for tracking the changing model structures and parameters, incorporating structural changes, the change times and unknown variables. These methods are essential when observing subtle variations in machine events to determine pivotal features within a behavioral history that may determine compromise.

In addition, the new mathematics provides Darktrace with a non-frequentist architecture for inferring and testing causal links between explanatory variables, observations and feature sets. Granger causality, Bayesian belief networks and the new approaches based upon Convergent Cross Mapping (CCM) permit high-degree confidence in causal linkage to be drawn, without the need for protracted and repeated observation.
The core of Darktrace's mathematical processing is the determination of normative behavior using the methods described above, pivoting on Recursive Bayesian Estimation, Particle Filters and Sequential Monte Carlo techniques. This core incorporates a series of adaptive change point detectors (Mean and Variance, Sequential Point Estimation and General Linear Change Point Detector) to resolve a probable threat sequence.

> "Darktrace is interesting because of its back-to-front approach to security... [it] profiles not possible attack vectors, but the network itself, as well as the devices that connect to the network and the network's users."
>
> David Meyer, Gigaom, 2014

Conclusion

In an era of pervasive internal threat, a new approach is necessary that does not rely on legacy distinctions of 'inside' and 'outside' but instead is capable of understanding what is happening from within an organization and dealing with the unexpected.

Modern organizations are not like medieval walled cities – interaction and collaboration across geographical and virtual boundaries is vital to their ability to survive. The new model of security must allow and encourage this flexibility, accepting that threat is present by default and that the battle against it will be constant.
The Enterprise Immune System movement allows organizations to understand threat holistically and defend against it, based on new machine learning and mathematical breakthroughs. The system is continually learning, meaning that it can deal with the unpredictability of sophisticated threats and move in step with both a changing organizational environment and evolving threat landscape.

Organizations that have implemented an Enterprise Immune System into the core of their information systems are now benefitting from the world's leading advances in machine learning and mathematics to protect against insidious and persistent threats from within their networks, while maintaining the flexibility and interconnection that we all thrive on. An Enterprise Immune System sits at the heart of a new approach that accepts the complexity of our systems and the threats within them. You may still catch the odd cold but in this game of probability, it'll be a price well worth paying.

> "Tackling cyber security properly will require a leap of faith into the more uncertain world of probability – we need to start picking our battles and deal with the important stuff that might kill us first."
>
> Dr Mike Lynch OBE, founder of Autonomy and Invoke Capital, 2014

About Darktrace

Winner of the Queen's Award for Enterprise in Innovation 2016, Darktrace is one of the world's leading cyber threat defense companies. Its Enterprise Immune System technology detects and responds to previously unidentified threats, powered by machine learning and mathematics developed by specialists from the University of Cambridge. Without using rules or signatures, Darktrace is uniquely capable of understanding the 'pattern of life' of every device, user and network within an organization, and defends against evolving threats that bypass all other systems. Some of the world's largest corporations rely on Darktrace's self-learning technology in sectors including energy and utilities, financial services, telecommunications, healthcare, manufacturing, retail and transportation. Darktrace is headquartered in Cambridge, UK and San Francisco, with 20 global offices including Auckland, Johannesburg, Lima, London, Milan, Mumbai, Paris, Seoul, Singapore, Sydney, Tokyo, Toronto and Washington D.C.

Contact Us

US: +1 (415) 243 3940
Europe: +44 (0) 1223 324 114
APAC: +65 6248 4516

Email: info@darktrace.com

www.darktrace.com