DARKTRACE

WHITE PAPER

Complying with New York DFS Cybersecurity Regulations

New Cyber Defense Strategies in the Wake of 23 NYCRR 500

Overview

With the new cyber security regulations issued by the New York State Department of Financial Services (DFS) in place, financial institutions and third-parties providing services to those institutions are forced to adopt stringent measures to enhance their security posture.

23 NYCRR 500 obliges covered entities to assess their risk profile and establish a cyber security program that "addresses its risks in a robust fashion." The program includes a host of requirements which span from annual penetration testing through to regular training sessions, hiring a qualified CISO, and more. While some of these requirements are relatively straightforward, the DFS has also introduced strict measures which pose a significant challenge to organizations forced to comply.

Most notably, the regulation mandates that covered institutions report "Cybersecurity Events" within 72 hours of determining that an incident has a "reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity." While it is not yet clear how the DFS will ultimately define "material harm," most industry insiders agree that the financial consequences of not complying with this measure will be considerable.

As the threat landscape continues to evolve, the challenge of complying with the 72-hour rule and similarly demanding measures will be virtually impossible without the right technology in place. Modern corporate networks and supply-chains have become increasingly complex, and the rapid adoption of vulnerable IoT devices and cloud technologies has multiplied attack vectors across the digital enterprise. Against this turbulent background, legacy tools based on signatures of past attacks have proven ill-equipped to defend against quiet or novel threats, malicious insiders, and machine-speed attacks like ransomware.

As a world leader in machine learning for cyber defense, Darktrace works with organizations in all industry sectors, including hundreds of financial services firms, to help defend against cyber-threats that would otherwise go unnoticed by traditional security defenses. Powered by machine learning and AI algorithms, Darktrace's Enterprise Immune System software is easy to implement and critical for helping organizations comply with these new requirements in an evolving threat landscape.

This paper focuses on the most stringent of the DFS's new requirements, particularly the necessity to report security events that are currently not discoverable using traditional methods. By unpacking each of these in turn, we will demonstrate how Darktrace's Enterprise Immune System technology is vital to finding anomalous behaviors and events quickly, and delivering a robust and adaptive cyber security program suited for this new era of evolving cyber-threats.

> “New Yorkers must be confident that banks, insurance companies, and other financial institutions ensure the security and privacy of their sensitive personal information.”
>
> **Maria T. Vullo, New York State Department of Financial Services Superintendent**

What is the Enterprise Immune System?

Applying the principles of a human immune system, Darktrace's Enterprise Immune System is the world's most advanced machine learning technology for cyber defense. Powered by machine learning and AI algorithms, the Enterprise Immune System iteratively learns the 'pattern of life' for every user and device on the network, using this understanding of 'normal' as a baseline to detect and respond to never-before-seen threats in real time.

Crucially, the Enterprise Immune System is self-learning, so it doesn't rely on human input or training data and can be installed in under an hour. This self-learning approach enables the platform to identify novel threats, including zero-days, insiders, and sophisticated 'low-and-slow' attacks.

> “Darktrace shines a light onto our systems, giving us a visual overview of what's really happening 'under the hood' – instead of relying on guesswork.”
>
> **Conor Claxton, COO, Macrosynergy Partners**

Identifying internal and external security risks

One of the regulation's core requirements involves identifying and assessing all internal and external cyber security risks that may threaten the security or integrity of non-public information stored on an organization's IT systems, see Section 500.02(b)(1).

As networks expand into cloud and virtual environments and take on mobile and IoT devices at an alarming rate, modern digital architectures are becoming increasingly complex and difficult to secure. While many organizations have standard risk assessment procedures in place, they often struggle with network visibility and are unable to accurately identify and assess genuine cyber security risks. Indeed, CISOs typically underestimate the number of devices connected to their networks by a margin of 35%. In order to identify vulnerabilities and curb cyber-threats, security teams need to gain a comprehensive view of the entire corporate network.

> **CISOs typically underestimate the number of devices connected to their networks by a margin of 35%.**

The Enterprise Immune System is able to model the normal behavior of all users and devices across all network types, in order to establish a 'pattern of life' specific to an organization's environment. The platform maps this 'pattern of life' onto its 3D Threat Visualizer, a graphical and interactive interface from which the user can monitor and investigate every user and device, as well as any anomalous activity in an organization's network. These anomalies are probabilistically judged in Darktrace's Threat Classifier, ensuring that only the most serious anomalies are presented to the security team for consideration.

Darktrace's ability to learn on the job and understand an organization's normal 'pattern of life' allows for real-time identification of network vulnerabilities and emerging threats which would have otherwise gone unnoticed, providing users with a comprehensive overview of their organization's evolving risk profile.

Detecting previously unidentified threats – in real time

A crucial function of the required cyber security program is the effective detection of "any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System" in an organization's network, see Section 500.01(d)(1). In the current threat landscape, where attackers are innovating faster than our defenses, real-time threat detection has become more significant and challenging than ever.

Darktrace's distinctive approach to threat detection, grounded as it is in a rich understanding of normal network behavior, enables the Enterprise Immune System to spot never-before-seen threats that other tools miss. Additionally, the ability to investigate alerts in an intuitive and digestible way lies at the heart of Darktrace's user interface. Darktrace's interactive Threat Visualizer not only provides a high-level oversight of threat levels, but also allows you to dive deep into granular details, such as specific connections of particular devices, or the pace of data transfers outside the organization.

> **The ability to investigate alerts in an intuitive and digestible way lies at the heart of Darktrace's user interface.**

Darktrace combines this depth of detail with features that enhance ergonomics and facilitate investigation for security teams of all maturity levels. The Dynamic Threat Dashboard allows threat analysts to rapidly triage alerts, with the platform automatically presenting relevant information for decision-making in one click. Equally, the Threat Visualizer's 'Ask the Expert' feature allows users to instantly send anomalous network events to Darktrace analysts for timely assistance.

> “With the Enterprise Immune System, the machine learning technology allows our security team to focus on the real threats, without having to tune or tweak the software.”
>
> **Laura Whitt-Winyard, Director of Information Security, Billtrust**

To date, Darktrace has uncovered over 63,500 in-progress attacks. In one case, a bank in Italy experienced a malware attack in which cyber-criminals covertly hijacked the bank's servers in order to launch an extensive bitcoin mining operation. The Enterprise Immune System detected anomalous behavior and discovered the hijacked servers in real time, enabling the bank's security team to dispose of the mining operation within less than an hour of the initial compromise – a prime example of an attack that Darktrace was able to detect which otherwise would have gone unnoticed.

> In the past six months, Darktrace has detected over 1,000 cryptocurrency mining operations worldwide.

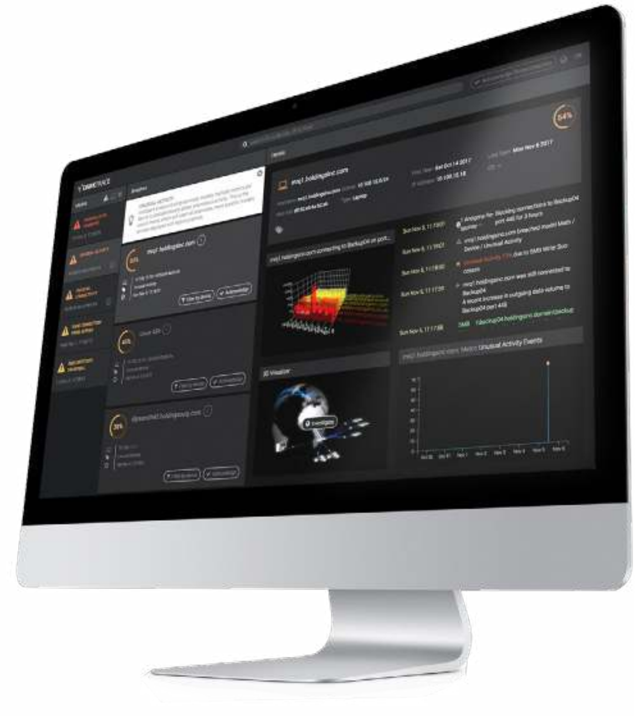

Figure 1. Darktrace's Dynamic Threat Dashboard provides a real-time view of high-priority threats and suspicious activities inside the network.

Responding to cyber-threats

Once a cyber security threat or event has been detected, regulated organizations must be able to effectively neutralize the threat before it turns into a crisis, see Section 500.02(b)(4).

This requirement poses a tough challenge given the increasing speed with which today's threats operate. Security teams often struggle to respond to serious threats before they escalate and do damage. As attackers continue to innovate and gain in sophistication, the problem is getting harder, with the latest strains of ransomware ushering in a new phase of automated attacks.

Security teams alone, even those with 24/7 support, cannot keep pace, and most IT research analysts agree that autonomous response is becoming a requirement to keep up. As Scott Crawford, Research Director of Information Security at 451 Research, has said, "People cannot possibly keep up with the increasing complexity of security, which means that unsupervised machine learning must be equipped to take action against threats as they emerge."

Toward that end, Darktrace's autonomous response solution, Antigena, works by enforcing an organization's evolving 'pattern of life', taking surgical, proportionate action in response to in-progress threats by slowing down or stopping specific connections and giving security teams time to catch up.

Antigena is fully configurable, allowing for varying degrees of automation according to the organization's needs. For example, Antigena typically starts in 'Human Confirmation Mode' so users can validate Antigena's actions before they are put into effect, letting security teams gain confidence in Antigena's invariably measured responses before enabling full-on 'Active Mode'.

In one customer's environment, Darktrace detected an automated strain of ransomware activated by an employee who had accessed a phishing email on her personal account. Seconds later, the device began connecting to an external server on the Tor network and commencing SMB encryption activities. Although the security team had gone home for the weekend, Antigena swiftly interrupted all attempts to write encrypted files to network file shares and stopped the attack within seconds. Here as elsewhere, Antigena has become an indispensable tool for proactively neutralizing threats and buying security teams valuable time, without disrupting normal business operations.

> "Darktrace Antigena is the only automated cyber defense technology on the market that is capable of fighting the most important battles for us."
>
> **Michael Sherwood, CIO, City of Las Vegas**

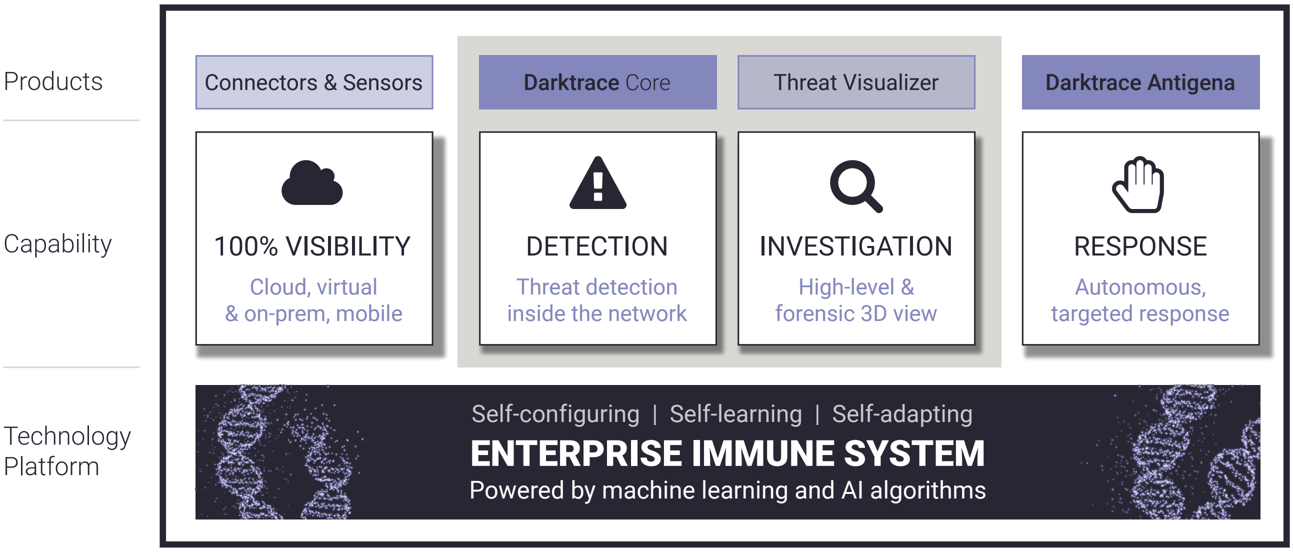
Products
Capability
Technology Platform
Connectors & Sensors
Darktrace Core
Threat Visualizer
Darktrace Antigena
100% VISIBILITY
Cloud, virtual & on-prem, mobile
DETECTION
Threat detection inside the network
INVESTIGATION
High-level & forensic 3D view
RESPONSE
Autonomous, targeted response
Self-configuring | Self-learning | Self-adapting
ENTERPRISE IMMUNE SYSTEM
Powered by machine learning and AI algorithms

Figure 2. The Enterprise Immune System is a self-learning technology that protects your entire digital infrastructure.

Reporting obligations & the 72-hour rule

Regulated organizations are required to track and report cyber security events to the DFS. Most notably, Section 500.17 requires that organizations inform the DFS as soon as possible but no later than 72 hours after the organization has determined that a significant cyber security event has occurred. Crucially, Darktrace helps organizations avoid this time-frame by detecting and responding to cyber-threats in real time, before they have time to gain access to critical data and cause material harm.

Together, Darktrace's core technology and investigation tools have helped hundreds of customers detect emerging threats and respond fast enough to avoid a reportable breach. Unlike conventional defenses, Darktrace can detect anomalous and potentially damaging activity at the first signs of compromise, including zero-day threats and quiet, stealthy attacks that take months to unfold, and which are typically missed by traditional tools that rely on matching an attack to a signature.

> **Darktrace's core technology and investigation tools have helped hundreds of customers detect emerging threats and respond fast enough to avoid a reportable breach.**

In addition, per Section 500.06, organizations must be able to furnish a detailed audit trail outlining specific security and risk-related events that occur on the network. Darktrace also helps support this reporting function, as event logs are stored on the appliance for up to a year, and can be retrieved and stored elsewhere, if required. Darktrace's graphical Threat Visualizer also allows users to replay activity that can be used for reporting purposes in an audit trail, and Darktrace's one-click Executive Threat Report automatically generates a summary of high-priority threats and activities over a selected period of time, providing a high-level overview of results and trends.

> “Darktrace has reduced the mean time to detect intrusions by 40%.”
>
> **Vari Bindra, Head of Cyber Defense Center, Blackhawk Network**

Managing third-party risk

Third-party risk remains a key preoccupation for firms that thrive on interconnectivity, yet are increasingly exposed to vulnerabilities introduced by their suppliers, contractors and even clients. Indeed, the entire supply chain has to be considered, comprising a complex web of related parties that can quickly spin out of an organization's direct control. To minimize the risks inherent in far-reaching digital ecosystems, regulated organizations are now required to demonstrate that third-party service providers have adequate cyber defenses, controls, and governance in place, see Section 500.11.

Darktrace detects anomalous behaviors wherever they touch the network, allowing the technology to monitor all associated third-parties in real time. This includes interactions between the business and third-party environments as well as the entire supply chain, with the option of implementing privacy controls to keep sensitive data confidential. This coverage extends across virtual networks, the cloud, and non-traditional IT, thus providing complete visibility of the entire digital business.

> “Darktrace provides huge value – we can visualize our network, and the behavior between hosts, so that we can protect our critical assets properly.”
>
> **Guillermo Guerra, Vice President and CISO, Jackson National Life Insurance**

Conclusion

Cyber security is the biggest risk factor facing the global financial system today. For the organizations regulated – and for those who might expect to be regulated in the future – now is the time to act. If followed properly, 23 NYCRR 500 will help ensure that financial institutions have the technologies and procedures in place to protect vital assets in the face of an unfamiliar and fast-evolving threat landscape.

As networks have grown in scope and complexity, the opportunities for attackers to exploit the gaps have increased. Perimeter defenses are no longer enough to protect the content of systems, rules cannot pre-emptively defend against all possible attack vectors, and signature-based detection methods fail repeatedly. Cyber-attacks are advanced, unpredictable, and subtle, and only real-time threat detection and autonomous response based on machine learning and AI can keep up.

The Enterprise Immune System's self-learning technology has helped financial institutions stay ahead of malicious anomalies for years, detecting and responding to advanced, never-before-seen threats in real time, before they have time to encrypt, exfiltrate, or manipulate critical data. No rules or signatures are needed. Instead, Darktrace's evolving sense of 'self' lets it dynamically spot anomalies as they emerge and take measured actions to curb in-progress threats.

About Darktrace

Darktrace is the world's leading AI company for cyber defense. With over 7,000 deployments worldwide, the Enterprise Immune System is relied on to detect and fight back against cyber-attacks in real time. The self-learning AI protects the cloud, SaaS, corporate networks, IoT and industrial systems against the full range of cyber-threats and vulnerabilities, from insider threats and ransomware, to stealthy and silent attacks. Darktrace has 800 employees and 39 offices worldwide. It is headquartered in San Francisco, and Cambridge, UK.

Contact Us

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

Disclaimer: This white paper is for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue or problem.

.