SOLUTION BRIEF

Financial Services
Artificial Intelligence

Accelerate Threat Detection with *n*Lighten*, Cybraics' Advanced Security Analytics and Artificial Intelligence Platform

Advanced security analytics and artificial intelligence powered by Intel® technology can transform information security—quickly detecting not only known threats but also unknown and insider threats

This solution brief describes how to solve business challenges through investment in innovative technologies.

If you are responsible for...

- **Business strategy:** You will better understand how a threat detection solution will enable you to successfully meet your business outcomes.
- **Technology decisions:** You will learn how a threat detection solution works to deliver IT and business value.

CYBRAICS

Executive Summary

The average consolidated total cost of a data breach is USD 4 million.[1] While more difficult to measure, the impact on a company's brand, lost revenue opportunities, and lost growth potential can be equally disastrous. On average, threats go undetected for over 200 days before a recognized breach occurs.[2] This dwell time is a critical metric to consider. The longer it takes to discover a breach, the greater the extent of the damage. The discovery-to-remediation cycle must be shortened to have a measurable financial impact for breach prevention.

Cybraics* dramatically shortens dwell time, and presents an opportunity to deal proactively with malicious activity. Cybraics brings cutting-edge innovation drawn from years of top-secret machine learning and artificial intelligence (AI) designs. The solution uses modern methods of intelligent threat detection that go far beyond traditional cybersecurity tools. Legacy tools are limited to non-corollary signature-based detection, which means they can find only known patterns of threat. In contrast, Cybraics' *n*Lighten* platform uses a combination of different machine learning techniques, in conjunction with a sophisticated AI engine, to discover known and unknown threats, as well as insider threats and targeted attacks. Cybraics' AI-based solution, combined with domain experts and advanced high-performance technology from Intel®, create a proactive and comprehensive state-of-the-art threat detection solution.

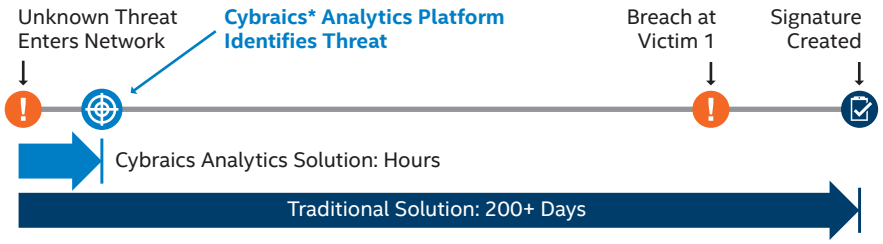


Figure 1. Nondeterministic methods using artificial intelligence enable the Cybraics* cyber analytics platform to detect previously unknown threats in hours, not days or months. The potential savings in both dollars and reputation are significant.

Solution Providers

Cybraics*. Provides advanced, accelerated threat detection using advanced security analytics and artificial intelligence as part of their analytics as a service platform, *n*Lighten*.

Cloudera*. Provides data processing and management based on Apache Hadoop* through the Cloudera Enterprise* data hub.

CyrusOne*, Switch*, QTS*, and ByteGrid*. Cloud service providers who partner with Cybraics for private cloud hosting of the Cybraics *n*Lighten platform.

Business Challenge: Adversaries Constantly Learning New Tricks

New technologies such as cloud computing and mobile devices introduce new threat vectors for hackers to exploit. Firmware and sub OS-level vulnerabilities are on the rise, as are Internet of Things (IoT) attacks. Hackers quietly use zero-day vulnerabilities before they are closed. Historically, businesses have found it difficult to be as agile as their attackers, always being victimized by lengthy dwell times (the length of time it takes to detect an attack) and stealthy malware activity.

The traditional approach to cybersecurity involves gathering data about intrusion prevention and intrusion detection system alerts, malware endpoint detection, data loss prevention rules, email filtering, phishing campaigns, white listing and black listing, patch levels, configuration variances, and other risk-based security baselines. Security information and event management (SIEM) systems use these rules to build a digital baseline to determine whether a cyberattack has been detected. The SIEM tools compare these signatures against corporate network data, and create alerts of known threats from the company's monitoring rules. Many tools are designed to protect only specific assets or against specific threat types. While SIEM systems are helpful, they do not offer a level of protection commensurate with the amount of damage they are designed to prevent. The aggregate sum of SIEM events is rarely cross-correlated to form an intelligent 360-degree view, and is unable to detect unknown attack patterns. The advent of point-and-click exploit kits, which enable attackers to create a unique signature for each attack, render signature-based tools ineffective at best. Conversely, malicious insiders with administrator privileges can be seen only using advanced correlation of a user ID's access and activity patterns over time.

In an attempt to manage these risks, organizations often turn to point solutions to address specific issues and protect specific high-value assets. The result is a large, unmanageable, and growing footprint of security tools, and yet the breaches continue:[3]

- Five of the United States' 20 largest banks suffered data breaches in the first half of 2016.
- In 2015, at least 87 breaches were reported in the financial services sector, up from 45 in 2014.
- Over 60 organizations suffered recurring breaches in the last decade, including most major banks. This indicates root-cause analysis was poor or non-existent, allowing the same attack to be successful more than once.

Increasingly, cyberattacks are not levied by amateurs, but instead by organized crime and state-backed hackers, who often direct highly sophisticated attacks against specific targets. More than 50 percent of data breaches remain undiscovered for months,[4] as hackers use innovative malware, botnets, and other advanced techniques to compromise a target, gain access to the environment, and patiently gather intelligence as they plan the next stage of their attack.

The threat space is growing and unmanageable. The tools at attackers' disposal seem endless—web application attacks, point-of-sale breaches, insider and privilege misuse, ransomware, Wi-Fi exploits, distributed denial of service (DDoS) attacks, botnet activity, and purpose-built malware all have kill-chain patterns that are varied and are often missed by traditional security tools. As if that was not enough of a challenge, the massive amounts of data (security logs, SIEM reports, network traffic flows, and so on) and security alerts make it next to impossible for a security team to identify, prioritize, and respond to threats. It is not uncommon for a security team to have over 10,000 new alarms to deal with each month. With a false positive rate of over 52 percent, most of their time is spent triaging, and this makes it impossible for them to prioritize the real threats.[5] Businesses require a real-time, proactive approach to threat detection (see Figure 2).

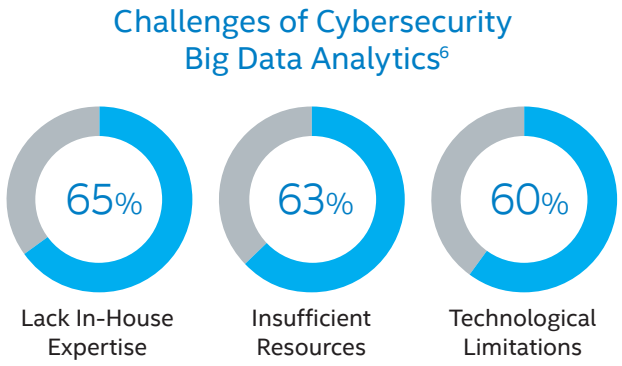
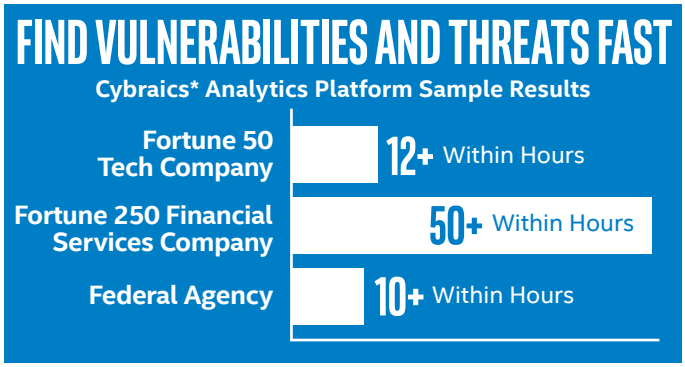


Figure 2. Traditional signature-based cybersecurity tools and approaches are not stemming the rising tide of cyberattacks.



Find Threats Before They Do Damage

As shown by the following use cases, the Cybraics* *n*Lighten* platform is flexible and powerful enough to detect a wide range of cyber threats—even when they have never occurred before.

- **Botnet on financial servers.** Cybraics analyzed hundreds of terabytes of data and identified several anomalies that had gone undetected by the customers' existing security tools. Cybraics' multiple analytics were able to correlate disparate behaviors and identify the presence of a widespread, active botnet that was not registered on any of the threat intelligence feeds. The customer was able to identify and remediate the infection before the adversary was able to exfiltrate any data or cause any damage.
- **Advanced malware.** Cybraics detected a weak attack signal within a customer's domain name server logs, indicating a potential active threat. This customer runs a large network of interconnected locations; a compromise at one location could potentially allow the attacker access to their entire environment. The organization failed to identify the threat because the impacted host was a vendor-provided device that was not managed by their existing end-point tools, and the domains attempting to be resolved did not exist on any of their blacklists. Further investigation confirmed an unknown strain of malware on the device and led to the vendor replacing the device and updating their security architecture for the customer.
- **Low-and-slow intrusion attempt.** Cybraics detected an intruder attempting to connect to an employee email server. The attacker was using a sophisticated surveillance tactic that systematically progresses through a list of user accounts, attempting to authenticate a few times every hour with the same account. By avoiding lockout policies, the attacker was able to start building a list of valid accounts on the server. Cybraics' detection and elimination of this threat prevented further malicious intelligence gathering.
- **Unknown backup failure.** Cybraics identified authentication failures that were happening at the same time each day. The number of incorrect login attempts was below the threshold of the monitoring system so the customer was not alerted. Investigation revealed that the customer had recently made broad password changes, and the credentials for a specific backup server had not been updated, causing the backups to fail. Though not a malicious threat, the failed backups put the company's data at risk and could have cost the organization significant time, resources, and money to recover or rebuild the data.
- **Ransomware in medical scanners.** Cybraics alerted a customer to anomalous behavior not matching the expected activity of internal users. The network management server responsible for monitoring and managing bedside devices was infected with malware. Had the infected device successfully connected with its command and control (located outside the customer's network), it could have locked the hospital out of all patient and financial information and cost the customer significantly in lost revenues, ransom fees, and remediation, not to mention threatening patient treatment and safety.

Solution Value: Affordable Volume, Velocity, and Veracity

Cybraics' artificial intelligence (AI)-based cyber analytics solution uses proven, deep inspection of anomalous and malicious threat detection patterns. The faster a threat is detected, the less damage it can do—potentially saving a company millions of dollars, irreparable harm to reputation, or business failure.

The core of Cybraics' analytics engine leverages unsupervised machine learning, which enables the platform to move beyond rules, signatures, and black lists to identify unknown threats. The analytics engine was developed by data scientists with the sole purpose of monitoring network, user, and entity behaviors in a given network. Cybraics' unique approach to algorithm development has yielded extremely sophisticated and scalable algorithms that can identify threats other approaches miss.

Unlike most analysis companies that have only a couple generic algorithms or focus on specific data sources, the Cybraics platform uses analytic pluralism. Cybraics has developed over 30 unique analytics and adapted them to run against virtually any data source. The result is that they are able to cover the entire threat space and protect all types of assets.

The solution can detect threats occurring in real time as well as vulnerabilities such as misconfigurations that could result in attacks. The platform can also perform historical correlation of massive data stores that show new patterns of attack or malicious user activity that have never been seen before.

The *n*Lighten platform is delivered as a service, so customers' total cost of ownership (TCO) is dramatically lower than if they were to build a comparable analytics solution themselves. In a preliminary internal study, Cybraics estimates that the monthly cost for the *n*Lighten platform is one-tenth of the monthly cost of a customer-built solution.[7]

"The combination of Intel's CPUs, SSDs, and network interface cards are the best option for running Cybraics software."

— Travis Collins, Vice President of Engineering, Cybraics

Solution Architecture: Cyber Analytics as a Service

The Cybraics *n*Lighten platform (see Figure 3) is a fully managed platform that can be deployed in an offsite private cloud or on-premises. It includes all the necessary hardware and software to provide a highly reliable, scalable, and end-to-end solution that delivers actionable cyber intelligence. The primary building blocks of the solution are as follows:

- **Data ingestion and management.** Built to handle terabytes of data per day from multiple sources, the data management platform provides automated, repeatable, reliable data management.
- **Big data platform.** *n*Lighten is deployed on the Cloudera Enterprise* data hub, which consists of Apache Hadoop* clusters powered by Intel® technology. Tightly integrated pods of compute, network, and storage resources provide rapid scaling, automated job scheduling, and built-in high availability.
- **Cyber analytics.** Unique and novel algorithms combine unsupervised, supervised, and semi-supervised learning techniques. Using a mix of automated batch and real-time analysis, over 30 customized analytics are run against multiple data sources to provide broad and deep threat detection.
- **Janus*.** A revolutionary AI-based machine analyst uses a combination of self-learning and active learning to quickly learn the environment and apply context from threats it has seen elsewhere. It accurately determines what anomalies are indicative of threats, reducing false positives.
- **Managed security operations center.** Access to Cybraics' expert cybersecurity analysts is built directly into the user interface, giving security teams the ability to scale on demand by allowing them to quickly request more context, or to simply engage them to assist with investigations.
- **User interface.** Through a rich user interface, the security team is presented with a curated list of actionable cases that include full context, and instant access to the tools needed for further investigation. Feedback automatically gathered from the user interface is directly integrated into the platform to help Janus learn and adapt to a customer's ever-changing environment.

Grow the Solution with Intel® Technology

While Intel® Xeon® processor-based servers provide high performance, some customers with more advanced workloads can tailor their Cybraics system by using more powerful Intel® technology specifically designed for analytics workloads.

- **Intel® Xeon Phi™ processor** helps eliminate node bottlenecks, simplify code modernization, and increase power efficiency. The bootable host processor offers an integrated architecture for powerful, highly parallel performance that paves the path to deeper insight, innovation for today's most demanding high-performance computing applications, including machine learning. Supported by a comprehensive technology roadmap and robust ecosystem, the Intel Xeon Phi processor is a future-ready solution that maximizes return on investment by using open standards code that is flexible, portable, and reusable.
- **Intel® FPGA** accelerates CPU cores to meet market needs for performance of diverse workloads in the data center. This platform will offer a simplified programming model, new classes of algorithms for acceleration, and integration with software-defined infrastructure (SDI) and Intel® Rack Scale Design (Intel® RSD).
- **Intel® Data Analytics Acceleration Library (Intel® DAAL)** helps speed big data analytics by providing highly optimized algorithmic building blocks for all data analysis stages (pre-processing, transformation, analysis, modeling, validation, and decision making) for offline, streaming, and distributed analytics usages. It is designed for use with popular data platforms including Hadoop*, Spark*, R*, and MATLAB* for highly efficient data access.

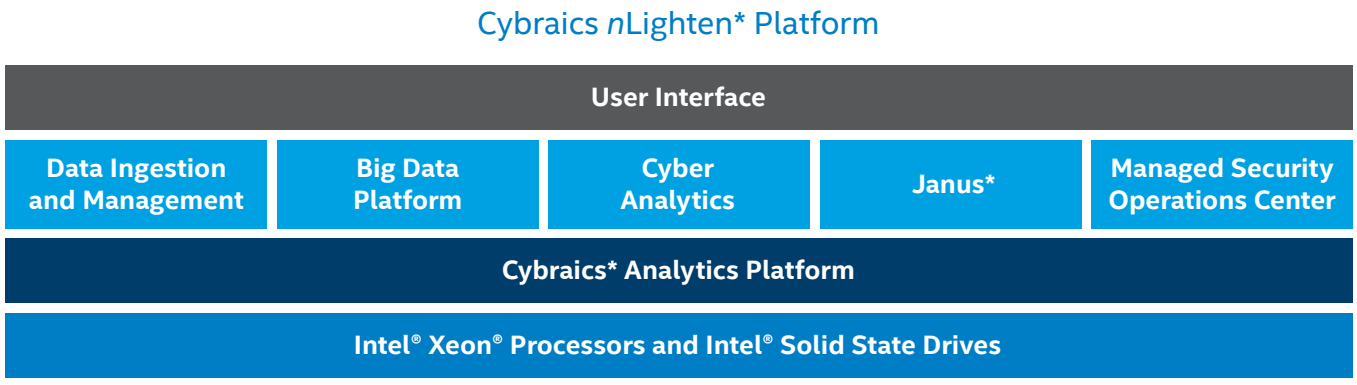


Figure 3. The Cybraics *n*Lighten* platform tightly integrates data, analytics, and domain expertise to quickly find threats—even those previously unknown.

An AI-based platform like *n*Lighten must be able to scale to the huge storage, memory, and computation requirements represented by terabytes, or even petabytes of information and real-time data streaming. Intel® Xeon® processor-based servers, combined with Intel® Solid State Drives (Intel® SSDs) with Non-Volatile Memory Express* support complex and real-time analytics operation. The Cybraics solution takes advantage of the built-in hardware-based security of Intel Xeon processors as well as accelerated technology for AI.

Both Intel and Cybraics have been active in the development of leading-edge advanced analytics technology, such as Apache Spot*. Together, the firms can serve as trusted advisors to help organizations develop the best possible cybersecurity platform.

Conclusion

The growing sophistication of organized crime and state-backed cyber threats means that a company's approach to protection must evolve and change as rapidly as the threat landscape. Businesses can no longer afford to wait months before a threat becomes obvious—protection must now be measured in hours. The Cybraics *n*Lighten platform can quickly discover new and unforeseen threats and patterns of malicious behavior.

Combining a unique blend of artificial intelligence, big data analytics, and human expertise, the Cybraics solution provides a world-class approach to detecting threats and vulnerabilities, and protecting organizations' assets and customer data. This end-to-end platform finds both known and unknown threats in a fraction of the time that other legacy tools take. The platform includes leading-edge technology from Cloudera* and Intel that powers actionable cybersecurity insights. By fusing the industry knowledge of Cybraics and Intel, the Cybraics *n*Lighten platform transforms and accelerates threat detection, potentially saving businesses millions of dollars in lost data, damaged reputations, and other costs that can occur from a single breach.

Find the solution that is right for your organization.
Contact your Intel representative or visit **intel.com/FSI**.

Solution Provided By:

CYBRAICS

intel

Focus on Cybraics

Cybraics is a security analytics and artificial intelligence company, focused on solving the hardest problems in cybersecurity. We are a collection of like-minded citizens passionate about ensuring that our nation's organizations and consumers can live free of cybercrime. We have created one of the world's first security analytics and AI platforms, *n*Lighten, delivered as a service. *n*Lighten uniquely combines multiple modes of machine learning with an advanced AI engine to find unknown, advanced and insider threats as well as targeted attacks, and fundamentally change the economics of cybersecurity.

Learn More

You may also find the following resources useful:

- Cybraics Website
- Apache Spot (Open Network Insight) Website
- Apache Spot Video: Leading a New Era of Cybersecurity

[1] "2016 Ponemon Institute Cost of a Data Breach Study," Larry Ponemon, June 2016, tinyurl.com/pc3hfro

[2] "Hackers Spend 200+ Days Inside Systems Before Discovery," Phil Muncaster, February 2015, infosecurity-magazine.com/news/hackers-spend-over-200-days-inside/

[3] Aggregated from the following sources: "ITRC Data Breach Reports," Identity Theft Resource Center, December 2015, idtheftcenter.org/images/breach/DataBreachReports_2015.pdf; Privacy Rights Clearinghouse, privacyrights.org/; "Maryland Information Security Breach Notices," Maryland Attorney General, Brian E. Frosh, oag.state.md.us/idtheft/breachNotices2015.htm; Office of the Indiana Attorney General, 2015_04_01_ITU_Breach, in.gov/attorneygeneral/files/2015_04_01_ITU_Breach(3).pdf; "2016 Cost of Data Breach Study: United States," Ponemon Institute LLC, June 2016, ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094USEN

[4] "2016 Data Breach Investigations Report," Verizon, regmedia.co.uk/2016/05/12/dbir_2016.pdf

[5] "Solving Alert Fatigue in Cyber Security," Nathan Burke, April 2016, slideshare.net/nathanwburke/solving-alert-fatigue-in-cyber-security

[6] "Big Data Cybersecurity Analytics Research Report," Ponemon Institute, September 2016, go.cloudera.com/ponemon#_ga=1.121747787.1395852778.1480629889

[7] Cybraics Internal Measurements, 2017.

0517/JWIL/KC/PDF ♻ Please Recycle 335246-001US