Infosys®
Navigate your next

WHITEPAPER

AI AND ML IN CYBERSECURITY RISK MANAGEMENT

The COVID-19 pandemic has exacerbated the threat of cyberattacks as criminals take advantage of workplace changes. Traditional cybersecurity risk management systems have not kept pace with the threat, but artificial intelligence offers new defenses.

Infosys® | Knowledge Institute

The number, types, and extent of cybercrimes increase with each passing year. More recently, firms across the globe have borne the brunt of cybersecurity and ransomware attacks, such as NotPetya and WannaCry. Further research shows that cyberattacks against banks have increased by as much as 238% due to the COVID-19 pandemic.[1]

These attacks include very sophisticated cybercrime methods utilized by criminals, such as:

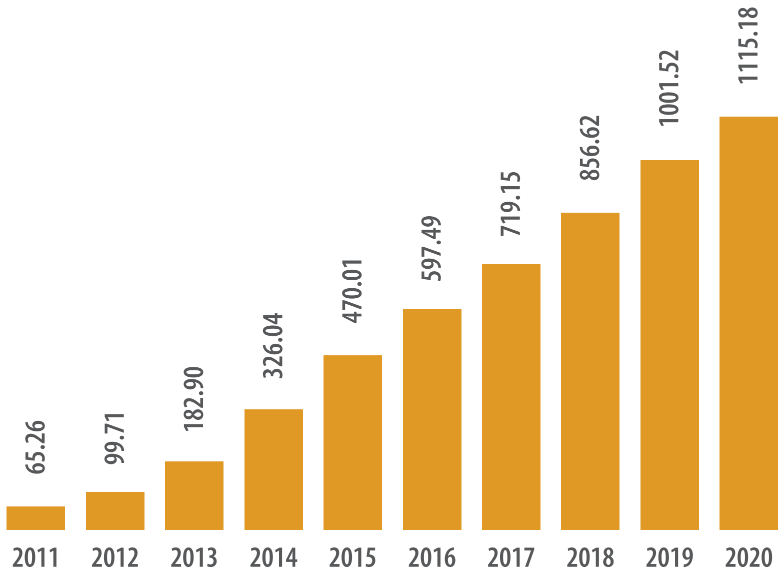
- Malware, including ransomware.
- Distributed denial of service (DDoS) attacks.
- Man-in-the-middle attacks (MITM).
- SQL injection.
- Zero-day exploits.
- Spear-phishing.
- Watering hole.
- Webshell.
- Domain name systems (DNS) poisoning.
- Port scanning.
- Cross-site scripting.
- Rootkits.

According to research firm Cybersecurity Ventures, cybercrime is predicted to cost the world more than $6 trillion annually by 2021, up from $3 trillion in 2015.[3] Unfortunately for organizations, traditionally fragmented and siloed cybersecurity risk management systems have not kept pace with the increasing scale of sophisticated cybercrime. In this landscape, systems are just unable to support real-time monitoring of cyber risks at big data scale.

The need for AI in cybersecurity

The time is ripe to use artificial intelligence (AI) and machine learning (ML) to combat cybercrime. Cybersecurity Ventures estimated that global spending on cybersecurity will exceed $1 trillion cumulatively from 2017 to 2021.[4] A big swath of this spending will go to innovative new AI solutions that tackle cybercrime. Further, a OnePoll survey found that 82% of respondent firms have implemented an ML cybersecurity solution. Of the remaining companies, 53% plan to implement the technology in the next three to five years.[5] And a registered investment advisers survey from TD Ameritrade, a financial services broker, concluded that AI-based cybersecurity investment is greater than investments made in performance reporting and financial planning (Figure 2).

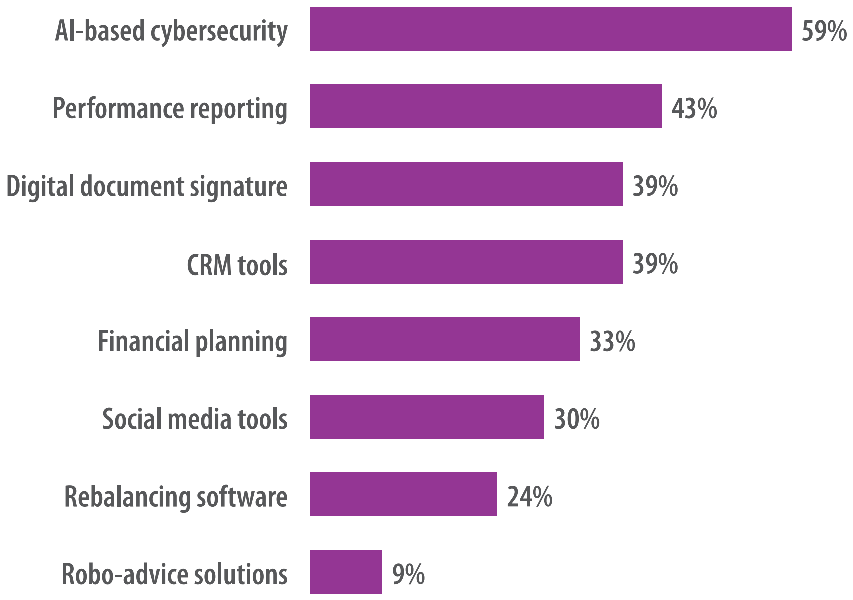
Figure 1. The number of malware is increasing



Source: AV-TEST Institute[2]

— Numbers are in millions
— 2020 data is until November 11, 2020

Figure 2. AI-based cybersecurity was the top technology investment in 2019 for retirement investment advisers



Source: TD Ameritrade[6]

So just why is AI and ML so popular in cybersecurity circles? Put simply, the benefits of this technology to secure vital infrastructure and stop unwanted intrusions is vast. It can be used for:

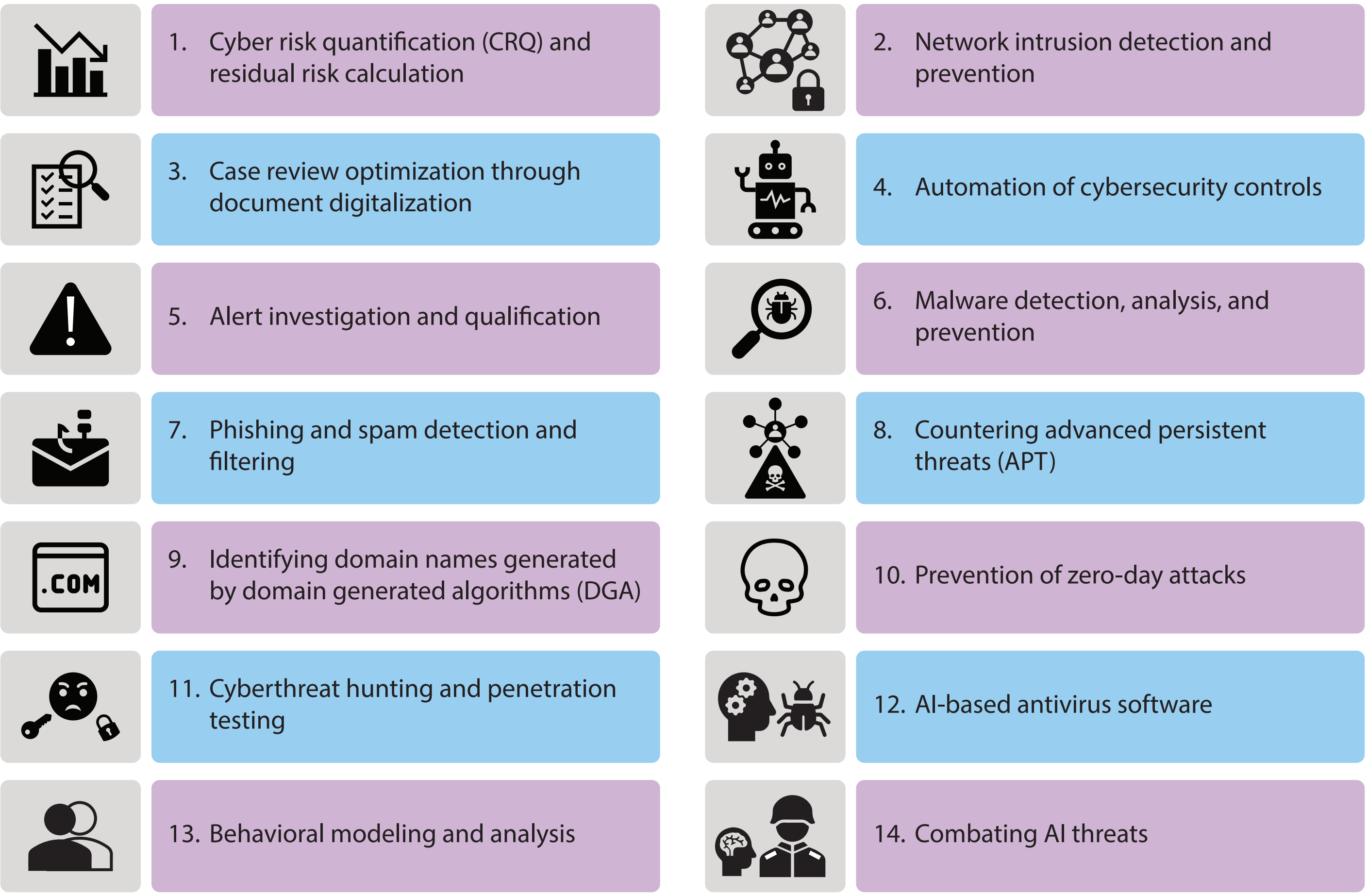
- Holistic cybersecurity risk management.
- Proactive and accurate assessment of cyber risk posture.
- Real-time detection and speedy prevention of cybercrime.
- Enhanced efficiency and effectiveness of cybersecurity controls.
- Combating novel polymorphic, and metamorphic cyberattacks.
- Enhanced productivity of cybersecurity teams.
- Enhanced true positives.
- Improved signal-to-noise ratios, which reduce false alarms.
- Sophisticated cyber risk reporting with customized qualitative and quantitative dashboards.
- Reducing human bias and chances of manual error.
- Reducing cost of cybersecurity risk management.
- Reducing operational and financial risks at the organization level.

Further, a holistic approach to cybersecurity using AI and ML helps build an integrated security immune system that takes into account:

- Networks.
- Endpoints.
- Devices.
- Hosts.
- Apps.
- Data.
- Cloud.
- Internet of things (IoT) devices.
- Identity and access.
- Firewalls.
- Cybersecurity infrastructure.
- Topology.
- Technology stack.
- Regulatory obligations.

In this paper, we examine these elements through 14 AI and ML use cases, including cyber risk quantification (CRQ), prevention of zero-day attacks, and behavioral modeling and analysis (Figure 3).

Figure 3. AI and ML cybersecurity use cases



1. Cyber risk quantification (CRQ) and residual risk calculation
2. Network intrusion detection and prevention
3. Case review optimization through document digitalization
4. Automation of cybersecurity controls
5. Alert investigation and qualification
6. Malware detection, analysis, and prevention
7. Phishing and spam detection and filtering
8. Countering advanced persistent threats (APT)
9. Identifying domain names generated by domain generated algorithms (DGA)
10. Prevention of zero-day attacks
11. Cyberthreat hunting and penetration testing
12. AI-based antivirus software
13. Behavioral modeling and analysis
14. Combating AI threats

CRQ and residual risk calculation

Using this solution, decision-makers can accurately and objectively measure the extent of cyber risk their firms carry in next to real time. Also, the solution enables firms to take a holistic technology and business value-oriented approach to prioritizing cybersecurity investments and assessing return on investment.

In this paradigm, cyber risks can be thwarted at various levels of strategic complexity.

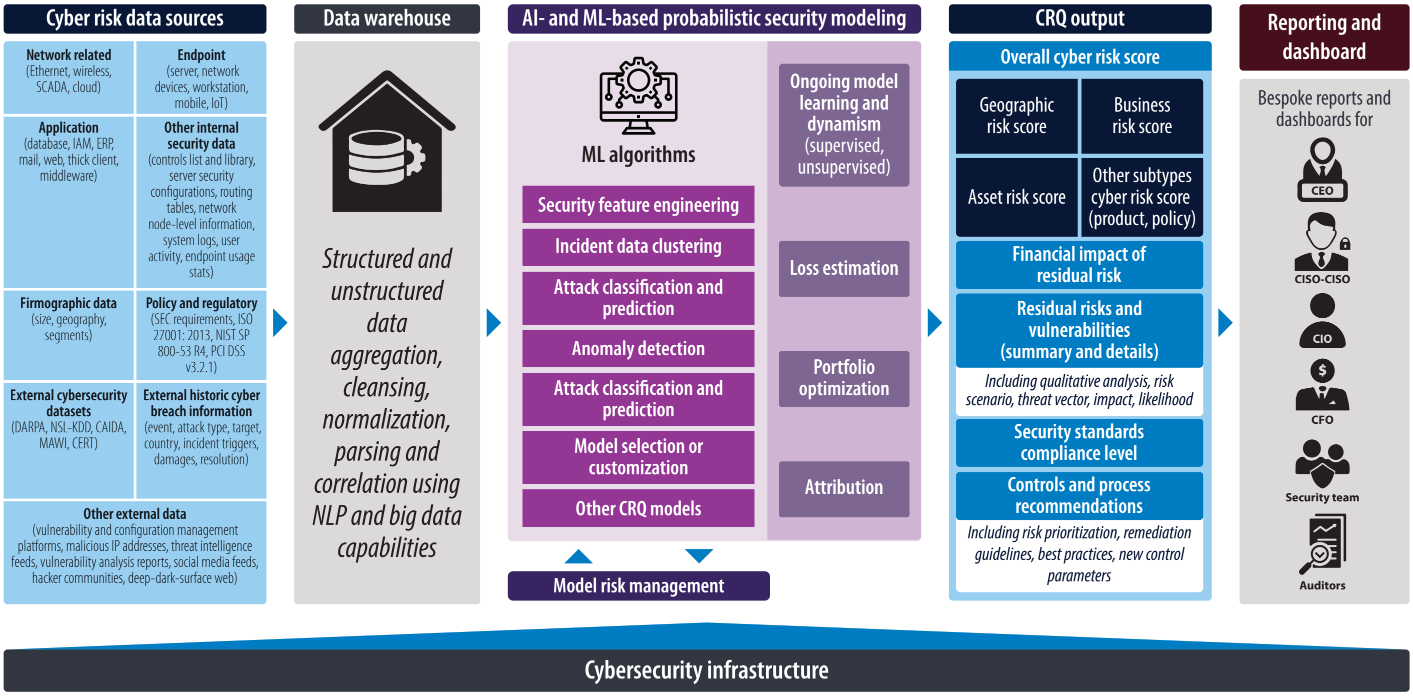
Salient aspects of AI- and ML-based CRQ solutions include:

Sophisticated cyber risk scoring	• Creates robust, empirically derived scores that provide a forward-looking indicator of the security risk. • Provides a single consolidated score for the firm's overall cybersecurity posture. This score applies to the sub-group level (geography, technology), macro level (across all technology devices), and micro level (score per IP address).
Exhaustive assessment	• Enables comprehensive and near-real time security assessment of all significant parameters, including technology stack, risk signals captured at internet scale, topology, threat level, business priorities, regulatory obligations, time-series observations of internet facing assets, and historical insights. This helps arrive at the cyber risk posture.
Advanced modeling techniques	• Leverages industry leading ML-based probabilistic security modeling techniques that utilize multilayered intelligence. These work to derive correlations between a firm's vulnerabilities and its security configurations and behavioral factors. • Uses techniques such as random forest, Naive Bayes, support vector machines (SVM), Hidden Markov models, generalized linear models, deep learning, fuzzy c-means clustering (FCM), artificial neural networks (ANN), k-nearest neighbors algorithm (KNN), recursive neural networks (RNN), and long short-term memory networks (LSTM).
Advanced dashboards and reports	• Enables customized and easy to understand dashboards and reports tailored to technical and nontechnical stakeholders, including the CEO, CISO, CRO, CXO, and security team. • Provides robust stratification, comparison, and benchmarking of cyber risk postures across portfolios and against peers. • Offers additional sophisticated capabilities, such as advanced heat maps and intelligent drilldowns.

Beneficiaries and benefits of AI and ML-based CRQ solution include:

Firms	• Thoroughly assess the efficacy of their own cyber risk programs and prioritize and optimize cyber risk investments. • Optimize cyber insurance coverage. • Effectively assess and mitigate cyber risks across the supply chain, including third and fourth parties, and cyber concentration risks across partners.
M&A entities	• Ascertain the cyber risks and investment demands of potential target firms. These insights are crucial in price negotiations.
Cyber insurers	• Cyber insurance underwriting processes and the management of aggregate portfolio risk.

Figure 4. Functional architecture of CRQ and residual risk calculation solution


Cyber risk data sources
Network related (Ethernet, wireless, SCADA, cloud)
Endpoint (server, network devices, workstation, mobile, IoT)
Application (database, IAM, ERP, mail, web, thick client, middleware)
Other internal security data (controls list and library, server security configurations, routing tables, network node-level information, system logs, user activity, endpoint usage stats)
Firmographic data (size, geography, segments)
Policy and regulatory (SEC requirements, ISO 27001: 2013, NIST SP 800-53 R4, PCI DSS v3.2.1)
External cybersecurity datasets (DARPA, NSL-KDD, CAIDA, MAWI, CERT)
External historic cyber breach information (event, attack type, target, country, incident triggers, damages, resolution)
Other external data (vulnerability and configuration management platforms, malicious IP addresses, threat intelligence feeds, vulnerability analysis reports, social media feeds, hacker communities, deep-dark-surface web)
Data warehouse
Structured and unstructured data aggregation, cleansing, normalization, parsing and correlation using NLP and big data capabilities
AI- and ML-based probabilistic security modeling
ML algorithms
Security feature engineering
Incident data clustering
Attack classification and prediction
Anomaly detection
Attack classification and prediction
Model selection or customization
Other CRQ models
Ongoing model learning and dynamism (supervised, unsupervised)
Loss estimation
Portfolio optimization
Attribution
Model risk management
CRQ output
Overall cyber risk score
Geographic risk score
Business risk score
Asset risk score
Other subtypes cyber risk score (product, policy)
Financial impact of residual risk
Residual risks and vulnerabilities (summary and details)
Including qualitative analysis, risk scenario, threat vector, impact, likelihood
Security standards compliance level
Controls and process recommendations
Including risk prioritization, remediation guidelines, best practices, new control parameters
Reporting and dashboard
Bespoke reports and dashboards for
CEO
CISO-CISO
CIO
CFO
Security team
Auditors
Cybersecurity infrastructure

Network intrusion detection and prevention

Novel and unanticipated intrusions and threats — undetectable by traditional signature-based systems — can be detected using an AI and ML solution. This new approach would:

- Monitor all incoming and outgoing network traffic to identify suspicious activity and classify the type of threat.
- Identify malicious applications in large enterprise networks.
- Enable robust network protection across Ethernet, wireless, supervisory control and data acquisition (SCADA), and Software-defined networks (SDN).
- Utilize ML-based anomaly detection capabilities for enterprise network level threat detection and classification, including the detection of botnets and domain generation algorithms (DGA).
- Use ML-powered network traffic analysis. This can take advantage of supervised and unsupervised learning algorithms to classify and cluster the attacks based on packet header and data flow information, such as protocol, number of bytes, rates, and counters.
- Offer ML techniques to aid in IP traffic classification.

The following AI and ML approaches are currently under consideration for network intrusion detection and prevention:

- Unlabeled samples and supervised learning algorithms used to enhance classifier performance, such as reducing false alarms.
- Combination of extreme learning machines and SVMs, along with modified k-means clustering, as the intrusion detection system (IDS) model.
- Utilization of KDD'99 dataset to enhance accuracy and reduce false alarms.
- IDS based upon sampling with least square SVM.
- Fuzziness-based semi-supervised learning.
- Nonsymmetric deep auto-encoder (NDAE), a new deep learning-based method for network intrusion detection.
- Genetic algorithms (GA) and fuzzy logic for detection of network intrusions. This uses glow analysis to generate a digital signature of a network segment. It can predict network traffic behavior during a specified time interval and for anomaly assessment.
- Ant tree miner classification, a new decision tree method.
- IDS utilizing binary KNN and particle swarm optimization (PSO), which includes feature selection and classification steps.
- PSO fast learning network.

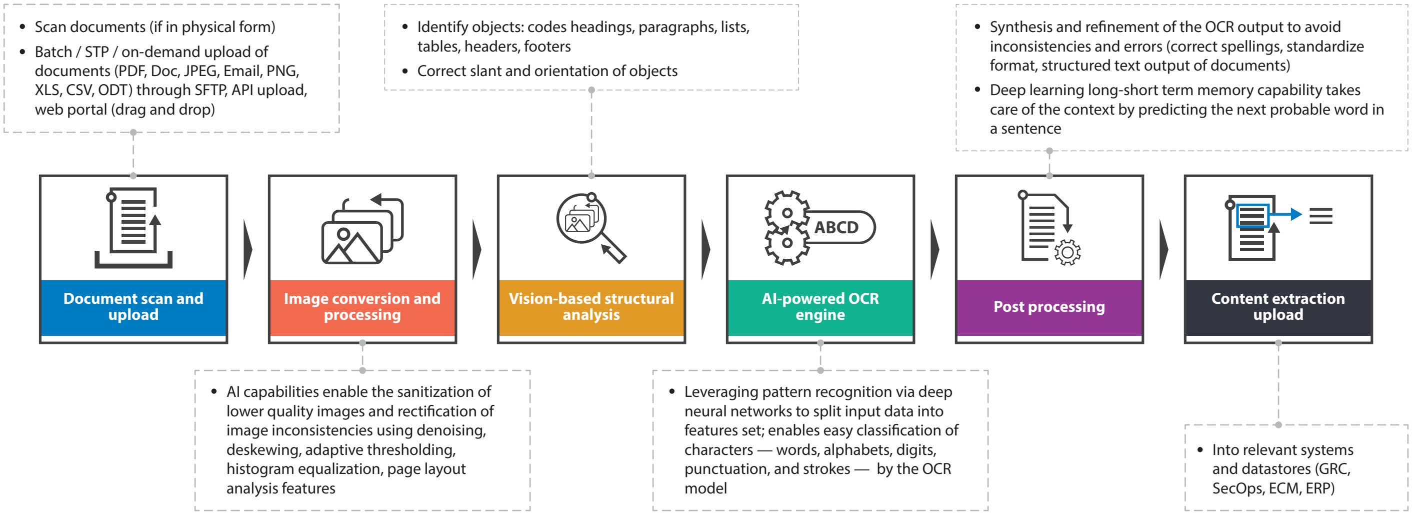
Case review optimization through document digitalization

Digitizing documents using traditional systems require rules-based methods, such as using regular expressions for identifying fields of extracting optical character recognition (OCR) from fixed field positions. These traditional solutions don't always work optimally.

With an increasing number of documents used in cybersecurity risk management (case management, policy, and cyber incident documents), it is important that firms improve process efficiency and effectiveness. Such a robust solution would improve turnaround times by converting such documents into a machine-readable format. An AI or ML solution can help companies improve case review optimization through document digitalization. Such an AI or ML solution would:

- **Optimize document data ingestion** — Automatically convert the physical document into structured and machine-readable data.
- **Automate data extraction** — With a machine-readable document, the solution can use ML and natural language processing (NLP) to automate data analysis. Robotic process automation (RPA) can enter relevant data into data stores.
- **Handle most document types** — NLP, advanced ML models, and ANN can accurately process cursive and handwritten text.
- **Unearth forgery or criminal intent** — Associative rule learning and sentiment analysis can quickly flag potentially criminal activity on payroll statements and ID documents.

Figure 5. High-level workflow for AI-based document digitalization



- Scan documents (if in physical form)
- Batch / STP / on-demand upload of documents (PDF, Doc, JPEG, Email, PNG, XLS, CSV, ODT) through SFTP, API upload, web portal (drag and drop)

- Identify objects: codes headings, paragraphs, lists, tables, headers, footers
- Correct slant and orientation of objects

- Synthesis and refinement of the OCR output to avoid inconsistencies and errors (correct spellings, standardize format, structured text output of documents)
- Deep learning long-short term memory capability takes care of the context by predicting the next probable word in a sentence

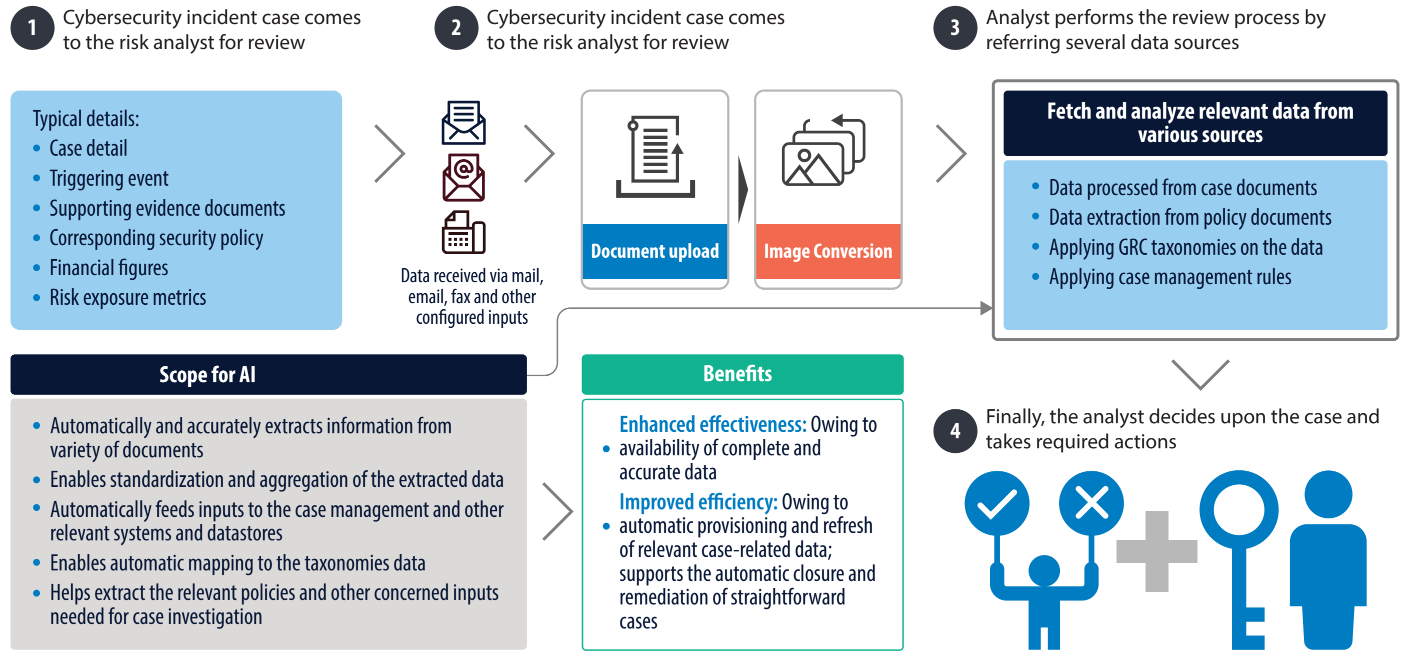
Document scan and upload
Image conversion and processing
Vision-based structural analysis
ABCD
AI-powered OCR engine
Post processing
Content extraction upload

- AI capabilities enable the sanitization of lower quality images and rectification of image inconsistencies using denoising, deskewing, adaptive thresholding, histogram equalization, page layout analysis features

- Leveraging pattern recognition via deep neural networks to split input data into features set; enables easy classification of characters — words, alphabets, digits, punctuation, and strokes — by the OCR model

- Into relevant systems and datastores (GRC, SecOps, ECM, ERP)

Figure 6. AI's role in case review optimization



1 Cybersecurity incident case comes to the risk analyst for review

2 Cybersecurity incident case comes to the risk analyst for review

3 Analyst performs the review process by referring several data sources

Typical details:
- Case detail
- Triggering event
- Supporting evidence documents
- Corresponding security policy
- Financial figures
- Risk exposure metrics

Data received via mail, email, fax and other configured inputs

Fetch and analyze relevant data from various sources

- Data processed from case documents
- Data extraction from policy documents
- Applying GRC taxonomies on the data
- Applying case management rules

Scope for AI

- Automatically and accurately extracts information from variety of documents
- Enables standardization and aggregation of the extracted data
- Automatically feeds inputs to the case management and other relevant systems and datastores
- Enables automatic mapping to the taxonomies data
- Helps extract the relevant policies and other concerned inputs needed for case investigation

Benefits

- Enhanced effectiveness: Owing to availability of complete and accurate data
- Improved efficiency: Owing to automatic provisioning and refresh of relevant case-related data; supports the automatic closure and remediation of straightforward cases

4 Finally, the analyst decides upon the case and takes required actions

Automation of cybersecurity controls

AI capabilities — specifically RPA, ML, and NLP — can help intelligently automate repetitive and manual cybersecurity tasks, including cybersecurity controls and control functions (see Figure 7). Using AI in this way leads to improved efficiency and effectiveness in using cyber controls, along with controls process simplification, enhanced controls visibility, and controls-related cost reduction.

AI- and ML-enabled cybersecurity controls solutions can enable:

- Automatic controls testing and updates.
- Controls framework automation and standardization.
- Automated inspection, scanning, and analysis across network logs, applications, and device inventory.
- Automated controls for data discovery, extraction, classification, and aggregation.
- Automated data loss detection and monitoring.
- Security validation and remediation. For example, RPA can automatically capture information on URLs and code to be tested.
- Automatic rollout of updates and patches.
- Automated backups of core cybersecurity control processes.
- Regulatory compliance assurance with respect to the European Union's General Data Protection Regulation, California Consumer Privacy Act (CCPA), and the Payment Card Industry Data Security Standard.
- Threat intelligence triaging, using automated breach notification.
- Automated gate checks for security activities in the software development life cycle.
- Identity and access fulfilment, including secure role-based access enablement and unauthorized access elimination.

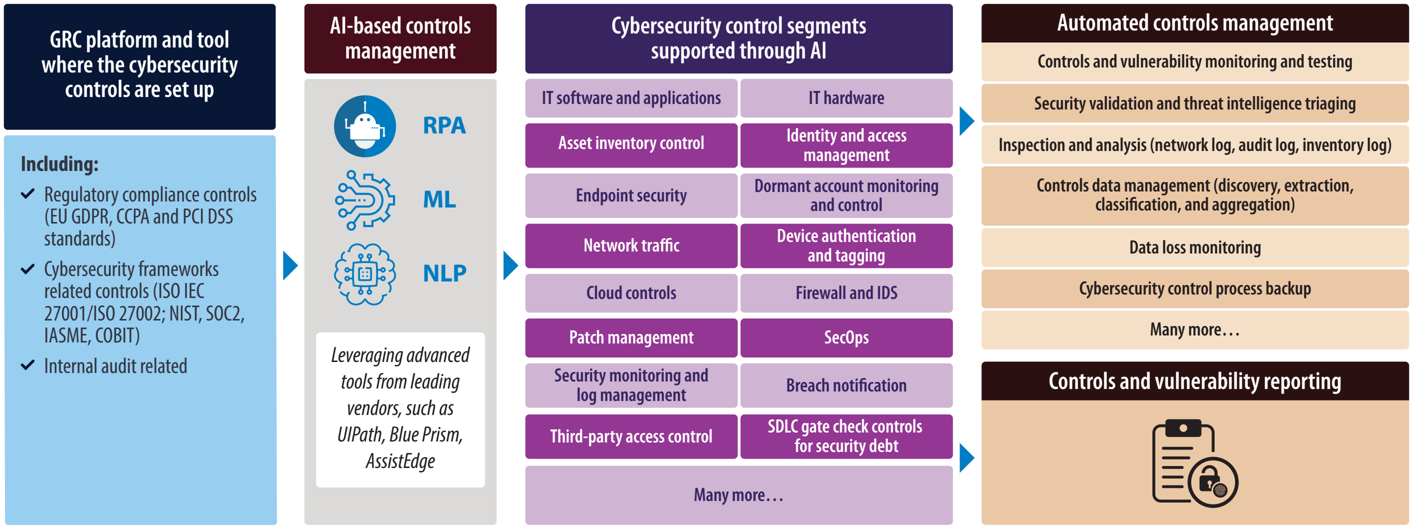
Alert investigation and qualification

An AI- or ML-based solution can help cybersecurity teams enhance the efficiency and effectiveness of their alert investigation and qualification. For example, the Massachusetts Institute of Technology's Computer Science and Artificial Intelligence Laboratory has developed an adaptive ML security platform named AI^2. The platform reviews millions of log lines every day, filters the data, and passes it on to a human analyst. This reduces the number of alerts to roughly 100 per day. Along with a massive reduction in false positives, the platform also helps significantly improve the attack detection rate.[7, 8]

The following elements should be imbedded into an AI or ML alert investigation and qualification solution:

- **Enriched incident context** — Using clustering and classification features on threat indicators to enable improved context for alert prioritization.
- **Sophisticated threat alert research and analysis** — Using NLP for semantic analysis; and deep nets for automatic information and insights gathering on the incident, forensics, behavior, and time-series analysis.
- **False positive and noise reduction** — Using principal component analysis, RNNs, and deep convolutional neural networks (CNN)-based transfer learning methods.
- **Automation of repetitive alert management tasks** — Such as triaging of low-risk alerts or tedious alert data enrichment tasks using RPA, NLP, and ML.

Figure 7. RPA-based automation of cybersecurity controls


GRC platform and tool where the cybersecurity controls are set up
Including:
✓ Regulatory compliance controls (EU GDPR, CCPA and PCI DSS standards)
✓ Cybersecurity frameworks related controls (ISO IEC 27001/ISO 27002; NIST, SOC2, IASME, COBIT)
✓ Internal audit related
AI-based controls management
RPA
ML
NLP
Leveraging advanced tools from leading vendors, such as UIPath, Blue Prism, AssistEdge
Cybersecurity control segments supported through AI
IT software and applications
IT hardware
Asset inventory control
Identity and access management
Endpoint security
Dormant account monitoring and control
Network traffic
Device authentication and tagging
Cloud controls
Firewall and IDS
Patch management
SecOps
Security monitoring and log management
Breach notification
Third-party access control
SDLC gate check controls for security debt
Many more…
Automated controls management
Controls and vulnerability monitoring and testing
Security validation and threat intelligence triaging
Inspection and analysis (network log, audit log, inventory log)
Controls data management (discovery, extraction, classification, and aggregation)
Data loss monitoring
Cybersecurity control process backup
Many more…
Controls and vulnerability reporting

- **Response planning, simulation, and recommendations** — Using decision matrices, observational learning, and association rule learning.

Malware detection and analysis

An AI or ML solution can enable effective malware detection and analysis. Such a solution can:

- Detect, analyze and prevent novel malware variants and evolving and self-changing malware, such as viruses, Trojan horses, worms, exploits, retroviruses, botnets, malvertising, and ransomware.
- Analyze a vast array of features, such as accessed fields on the disk, accessed APIs, consumed bandwidth, consumed processor power, data volume transmitted over the internet, and accessed products such as keyboards and cameras, all in a bid to detect and analyze the malware.
- Leverage inference techniques, using previously identified malware characteristics, to predict future threats that signature-based approaches are unable to detect.
- Use ML models to perform behavior and advanced static analysis and detect and classify malware before they execute.
- Use unsupervised future learning with auto-encoders to discover relevant properties of malware samples.

Some of the AI and ML approaches being used or considered for malware detection and analysis include:

- ML to enable hardware-aided malware discovery utilizing virtual memory access patterns. The machine learning does this through logistic regression, SVM, and random forest classifiers.
- Using operational codes, KNN, and SVM as ML classifiers for malware classification.
- Deep learning for intelligent detection of malware, by utilizing an auto-encoder along with multilayer restricted Boltzmann machines.
- Rotation forest, a novel ML algorithm.
- ANN along with raw sequences of the API method calls for detecting Android malware.
- A hybrid model based upon CNN and deep autoencoder for large-scale Android malware detection.
- Bio-inspired methods for feature optimization, malware classification, and classifiers parameter optimization by using PSO or GA.

Phishing, and spam detection and filtering

Traditional anti-phishing and spamming approaches — involving simple word filtering, IP blacklists, content filtering, and sender reputation mapping — are not always effective. More advanced solutions instead take advantage of sophisticated ML models that offer hundreds of input features, use of NLP to check grammar, and apply visual analytics to automatically and more effectively detect and classify phishing and spam emails. Further, such methods can detect content that organizations want to block.

The following are currently being considered and used across industries:

- Anti-phishing methods that utilize various ML algorithms and features to differentiate phishing websites from genuine ones.
- Reinforcement learning and neural network applications to identify phishing websites. Such methods utilize risk minimization principles and Monte Carlo algorithms.
- Real-time anti-phishing systems that use various classification algorithms and NLP-based features.
- Stacking models that combine XGBoost, gradient boosted decision trees, and LightGBM using HTML and URL features for the classification of phishing webpages.
- Combined Naive Bayes and SVMs to develop spam filtering systems.
- Spam categorization using modified cuckoo search for enhancing spam classification. Step-size cuckoo search is used for feature extraction, and SVM is leveraged for classification.
- Filtering Facebook spam messages using AI and ML techniques. Here, a PSO algorithm is utilized for feature selection, and decision tree SVMs handle classification.
- Hybrid approach for identification of spam profiles on Twitter through bio-inspired computing and social media analytics. Spammer detection uses modified k-means integrated with the Levy-flight firefly algorithm and chaotic maps.
- Email spam detection and identification systems based upon random weight networks and GAs.

Countering advanced persistent threats

APTs are cyberattacks that use sophisticated methods to exploit sensitive data while remaining undetected. APT attackers usually focus on high-value targets, such as governments or a large firm's security division. The goal is often the long-term theft of information.

AI or ML solutions can be used to protect against APT attacks, including the following:

- Decision tree for building IDS to detect the APT attacks from the start and react quickly.

- Frameworks based upon multiple parallel classifiers.
- Deep neural networks (DNN) that use dynamic analysis features for APT attribution.
- Using self-organizing feature map and machine activity metrics for differentiating the legitimate versus malicious software.
- MLAPT, an ML-based approach for identifying and predicting APTs.

Identifying domain names generated by domain generated algorithms

DGAs are algorithms that periodically generate a large number of fake random domain names. These names conceal the operator's command and control server.

AI or ML solutions can identify with high precision the domain names created by DGAs. Such a solution may, for example, deploy ML models to look for DGAs associated with unidentified malware in domain name systems (DNS) logs.

Some of the AI or ML solutions include:

- Adoption of RNN- or CNN-based architecture.
- Using generalized likelihood ratio tests.
- Novel LSTM-based algorithms for handling the multiclass imbalance issue via DGA malware detection.
- ML-based DNS covert channel and DGA detection system. Such a system utilizes a specificity score, improved term frequency-inverse document frequency, and other algorithms for identifying malicious domain names.
- Identification of word-based DGAs by leveraging the words' frequency distribution and ensemble classifier built using extra trees, Naive Bayes, and logistic regression.

Prevention of zero-day attacks

A zero-day weakness is a software security vulnerability that is unknown to, or yet to be addressed by, the parties responsible for fixing the flaw. Until such vulnerabilities are plugged, hackers can misuse these for criminal purposes. Zero-day exploits cannot be detected by conventional means, such as anti-malware or IDS-IPS devices because signatures have not yet been created.

An AI or ML solution can be used here to help close zero-day vulnerabilities. For example, an Arizona State University team used ML to monitor traffic on the dark web and identify data related to zero-day exploits.[9] Armed with such insights, firms can potentially close the software vulnerabilities and patch exploits before these lead to data breaches.

More distinctly, AI- or ML-based solutions can:

- Expedite the sandboxing, or memory dump, approach that experts use to analyze some zero-day threats. Sandboxing involves installing suspicious files or programs in a virtual machine and then observing its behavior to ascertain whether it's good or bad. When done manually, this process can take several minutes, while AI and ML models can provide a judgment in a few milliseconds.
- Using unsupervised learning and behavior-based detection techniques to analyze the users' interactions with the software and all contextual information to predict malicious action.
- Utilizing oriented graph model capabilities, such as Galois lattice for ranking the actions and analysis for tracing the correlation between events.

Cyberthreat hunting and penetration testing

Cyberthreat hunting involves actively and iteratively probing through the networks to find and isolate advanced threats that may evade existing solutions. This is different from the traditional threat management approaches such as firewalls, IDS, and security information and event management systems that usually require investigation of data after a warning has already been raised.

Penetration testing — also known as ethical hacking or pentesting — involves probing a network, web application, or computer system to identify security vulnerabilities that might be misused by attackers.

AI-based threat hunting and pentesting solutions enable firms to effectively learn and reproduce hidden and complex cybersecurity vulnerabilities. These solutions:

- Enable accurate, reliable, and comprehensive coverage and testing of the attack vectors.
- Allow automated, intelligence, and guided hunting of unknown cyberthreats.
- Use advanced ML techniques, such as reinforcement learning and partially observed Markov decision process to identify vulnerabilities.
- Integrate with industrial pentesting frameworks and diverse data sources at internet scale to enable effective vulnerability assessment.
- Take advantage of robust pre-built threat libraries — comprised of models, queries, data features, and playbooks — to support a wide range of threats.
- Use link analysis and chaining capabilities to automatically connect all events linked to an incident and provide full context.
- Can even predict the potential next step of an attack with a given threat scenario — along with information on affected devices and uses — to enable pre-emptive remediation.

AI-based antivirus software

Traditional antivirus software scans files on the company network and determines whether any of them match the signature of known viruses or malware. However, there are significant problems with this traditional defense. While it works well for previously encountered threats that have a public signature, new threats aren't easily detected. These types of software are also slow and don't provide real-time threat detection since updates are required to identify new viruses.

AI-powered antivirus software can help firms overcome these challenges. Instead of matching the signatures, the AI utilizes anomaly detection capabilities to monitor program behavior and identify abnormal actions.

Behavioral modeling and analysis

Certain cybersecurity breaches involve the cyberattacker stealing credentials of a user (without the user being aware) to get access to the enterprise network via technically legitimate means. This kind of attack is therefore difficult to identify and stop.

An AI-powered solution can use behavioral modeling and analysis capabilities to help prevent such attacks. These solutions:

- Gather data from software installed on customer workstations and sensors placed in network segments.
- Feed the above-mentioned data into behavioral analytics and threat intelligence engines that use ML to identify anomalies, and abnormal endpoint and network behavior. The system shuts down these connections when they occur.
- Use ML's regression analysis capabilities to analyze unprocessed network traffic data to identify the baseline behavior for each user and device.
- Utilize ML classification techniques to group different users for peer group analysis and clustering to separate groups of users and detect outliers.
- Identify substantial deviation from baseline behavior, such as logins at an unusual time, and alert the enterprise about potential cyberthreats.

Combating AI threats

There are several ways cybercriminals can use AI- and ML-based technologies for their own purposes. Such threats capitalize on the technologies' common value propositions, such as behavioral analytics, rapid scalability, and personalization. Some ways cybercriminals use AI and ML include:

- Generating new variants of older malware.
- Creating new phishing and spam content based upon training sets from earlier successful campaigns.
- Helping phishers and spammers detect recurring patterns in malicious content.
- Detecting vulnerable points in enterprise networks and using this information to target points of entry for spyware, phishing, or DDoS attacks.
- Building smart malware, or artificial hackers, to execute personalized attacks.
- Improving the targeting of malware by profiling potential victims using publicly available, harvested, or extracted data.
- Finding new zero-day vulnerabilities by feeding the algorithm with unexpected, invalid, or random data as inputs. That allows the ML algorithm to learn the routine required for identifying new vulnerabilities.
- Allowing botnet nodes learn collectively and share the intelligence for identifying the most effective forms of attack.

Firms and cybersecurity vendors can enable AI- or ML-based solutions to fight back and constantly adapt to new scenarios. These solutions use sophisticated ML algorithms to recognize attacks that are performed by other ML algorithms. In near real-time, advanced defenses can detect these cyberattacks and vulnerabilities, and provide recommendations. AI and ML solutions can also help detect odd, inactive, or anomalous machines in botnets.

AI and ML cybersecurity in the real world

The following companies provide real-world AI and ML cybersecurity risk management solutions.

Company	Use case	Details
Absolute	Endpoint resilience	• The company enables adaptive, intelligent, and self-healing endpoint security — along with always-connected visibility into data, devices, applications, and users — regardless of whether the endpoints are on or off. • Absolute Intelligence standardizes data through asset and security advocacy analytics. This enables security managers to ask all pertinent questions.[10, 11]
Blue Hexagon	Network intrusion detection and prevention	• It offers customers real-time network threat protection. The solution works across networks and the cloud and covers multiple types of threats among diverse platforms. • The firm uses AI to create malware based upon dark web and global threat data in order to test its own systems and enhance security capabilities.[12, 13]
Callsign	Identity verification and validation for fraud prevention	• Its Intelligence Driven Authentication solution uses AI and ML capabilities to validate a person's identity based only upon the number of keystrokes, touch-screen swipes, number of locations, and other activities. • Callsign uses multifactor authentication and fraud analytics — powered by deep learning technology — to combat identity fraud, SMS phishing, and other cybercrimes. • The solution captures thousands of data points — including behavioral, location, device, and telecom data — to correlate the identity traits. It then blends this insight with threat analysis information. • Data are analyzed in real-time utilizing advanced ML to deliver a user authenticity confidence score for a transaction.

		• The solution's intelligence engine works from the very first interaction and gets richer with each subsequent interaction. This ultimately builds a unique identity profile for each user.[14, 15]
CrowdStrike	Threat hunting	• CrowdStrike's Falcon platform uses AI to provide clients with visibility and protection on their enterprise networks. The platform is focused on averting endpoint attacks, including ransomware threats. • The solution offers actionable threat intelligence, real-time protection, and 24/7 managed threat hunting.[16, 17]
Cyberwrite	CRQ and residual risk mitigation platform	• Cyberwrite's proprietary ML-based solution enables real-time and on-demand cybersecurity risk analysis and assessment of financial impact. The advanced algorithms and an easy-to-understand reporting system are accessible for businesses of any size. • The solution supports cyber profiling. It also assesses cybersecurity threats and exposure to first- and third-party cyber risks, while proactively making data-driven cybersecurity improvements. • The solution automatically gathers internet data related to the dark web, attack surfaces, and proprietary cybersecurity risk, and also digital risk-based data connected to each entity. • Such data are then utilized as classifiers in the solution's exclusive machine learning models and transformed into benchmarked risk scores that can be compared to industry peers. This allows visibility of the firm's risk levels for each type of risk. • Beyond customer-specific data, which is monitored and collected in real-time, the solution's cyber risk models also take into consideration the inherent and external risk factors of a firm, including its sector, geography, and operational risks. • The solution also leverages data related to current regulatory fines, historical cyberattack damages, and risks that firms need to manage. That data allows companies to construct comprehensive cyber risk benchmarking reports used for supply chain vendor risk management, cyber insurance, and cyber risk financial analysis.[18, 19]
Cylance	Antivirus	• Cylance's smart antivirus product uses AI to predict, identify, and respond to threats. The solution learns to identify patterns that indicate malicious programs.[20, 21]
Darktrace	Network intrusion detection and prevention	• Darktrace has used AI and ML capabilities in its Enterprise Immune System and Darktrace Antigena platforms to identify a diverse range of cyberthreats in their initial stages. These work across various digital environments, including cloud, virtualized networks, IoT, and industrial control systems (ICS). • The solutions can be integrated into financial institutions' networks and offers the Darktrace Threat Visualizer, a dashboard for monitoring cyberthreats in real time.[22, 23]

Deep Instinct	Prevent zero-day threats and APT attacks	• Deep Instinct protects enterprise endpoints and mobile devices against cybersecurity threats on any infrastructure. • Its on-device solution applies deep learning to safeguard against zero-day threats and APT attacks. It enables cyberattacks to be detected and blocked in real-time.[24, 25, 26]
FICO	CRQ and residual risk mitigation platform	• FICO released its ML-based Cyber Risk Score on AWS Marketplace. The solution's scoring algorithm utilizes new globally gathered micro signal data that enhances the capability to quantify an organization's cyber risk for the next 12 months. • The solution also provides supplementary security risk indicators that are particularly valuable for small and medium-sized enterprises. • The solution provides sophisticated workflows and dashboards to compare, stratify, and manage the aggregate cybersecurity risk. • The three-digit score allows companies to measure the breach exposure and security posture across the supply chain. • The score is delivered via a suite of applications that are tailored to various use cases, including self-assessment, vendor risk management, and cyber insurance underwriting.[27, 28, 29]
Kount	Online fraud prevention	• Kount's next generation adaptive AI solution uses ML capabilities, both supervised and unsupervised, to prevent transaction fraud. • The solution can quickly and correctly detect existing or emerging, complex, and automated fraud. • The platform empowers digital businesses, online merchants, and payment service providers to protect against payment, new account creation, and account takeover frauds.[30, 31]
SECURITI.ai	PrivacyOps	• SECURITI.ai is a leader in AI-powered PrivacyOps. Its platform operationalizes and simplifies privacy-related compliance using an RPA and NLP interface. • The platform allows firms to provide rights to users for their data, be responsible guardians of people-related data, and comply with CCPA and other global privacy regulations.[32, 33]
ShieldX Networks	Security policy identification	• This cloud-native security platform constantly ascertains workloads, identifies risk, and imposes security policies in a multicloud environment. • ShieldX uses AI to expedite the process of determining which cybersecurity policies are applicable for each application. • The solution can also analyze each application's network communications data and provide security policy recommendations for that application.[34, 35]

Tessian	Email monitoring for phishing	• Tessian offers an AI-based email monitoring solution that helps financial institutions prevent phishing attacks, misdirected emails, and data breaches. • The solution utilizes anomaly detection models and NLP at various stages to recognize emails that pose cybersecurity threats.[36, 37]
Vade Secure	Email security	• Vade Secure is one of the world's leading email defense companies. It deploys AI and ML to protect more than 600 million mailboxes in 76 countries from cyberthreats, including ransomware, spear phishing, and malware.[38, 39]
Versive	Network intrusion detection and prevention	• The eSentire-owned Versive offers an AI-based enterprise cybersecurity solution, VSE Versive Security Engine, that uses dissonant detection to find network security vulnerabilities. • The solution uses ML capabilities to help banks and financial institutions monitor networks and enables adversary detection and management of cybersecurity threats. • The engine utilizes DNS, proxy data, and the banks' NetFlow — the network protocol for gathering IP traffic information and for monitoring network traffic.[40, 41, 42]
Zero Networks	Zero trust security	• The company's solution, Zero Networks Access Orchestrator, uses AI to enable a zero-trust network model. • The platform watches how users and machines usually communicate, and automatically defines and enforces a zero-trust network model across an enterprise. • The solution allows customers to create rare or new connections and automatically updates policies to enable genuine users' uninterrupted access.[43, 44]

AI technologies have many high-impact use cases in cybersecurity risk management. Firms are already using AI to effectively manage cybersecurity risks. And many others are planning to implement use cases in the near future. As AI and machine learning technologies gain greater maturity, the benefits that firms will reap from these use cases will undoubtedly multiply. The results will help ensure that cyber operations support real-time monitoring of risks at big data scale and across business ecosystems.

Acronyms

Acronym	Name	Acronym	Name
AI	Artificial intelligence	LS-SVM	Least squares support-vector machine
APTs	Advanced persistent threats	LSTM	Long short-term memory
ANN	Artificial neural networks	M&A	Mergers and acquisitions
ATM	Ant tree miner	MITM	Man-in-the-middle attacks
CCPA	California Consumer Privacy Act	ML	Machine learning
CISO	Chief information security officer	MoG-DNN	Mixture of gaussians-deep neural network
CNN	Convolutional neural network	NDAE	Nonsymmetric deep autoencoder
CRO	Chief risk officer	NLP	Natural language processing
CRQ	Cyber risk quantification	NTA	Network traffic analytics
DDoS	Distributed denial of service	OCR	Optical character recognition
DGAs	Domain generated algorithms	POMDP	Partially observed Markov decision process
DNN	Deep neural network	PSO-FLN	Particle swarm optimization — fast learning network
DNS	Domain name systems	RIA	Registered investment adviser
FCM	Fuzzy c-means clustering	RNN	Recurrent neural network
GA	Genetic algorithm	RPA	Robotic process automation
GBDT	Gradient boosting decision tree	RWN	Random Weight Network
GLRT	Generalized likelihood ratio test	SCADA	Supervisory control and data acquisition
HMM	Hidden Markov model	SDN	Software-defined networking
IDS	Intrusion detection system	SIEM	Security information and event management
IOC	Indicators of compromise	VM	Virtual machine
IP	Internet protocol	SVM	Support vector machine
KDD	Knowledge discovery in databases	XSS	Cross-site scripting
KNN	K-nearest neighbors algorithm		
LFA	Levy-flight firefly algorithm		
LightGBM	Light gradient boosted machine		

References

1. COVID-19 blamed for 238% surge in cyberattacks against banks, Charlie Osborne, May 2020, ZDNet
2. Malware, AVtest
3. 2019 Official Annual Cybercrime Report, Steve Morgan, Cybersecurity Ventures
4. 2019 Official Annual Cybercrime Report, Steve Morgan, Cybersecurity Ventures
5. Machine Learning Era in Cybersecurity: A Step Toward a Safer World of the Brink of Chaos?, February 2019, Eset
6. TD Ameritrade Institutional 2019 RIA Sentiment Survey, January 2019
7. MIT's Teaching AI How to Help Stop Cyberattacks, Brian Barrett, April 2016, Wired
8. System predicts 85 percent of cyber-attacks using input from human experts, Adam Conner-Simons, April 2016, MIT News
9. Machine Learning Goes Dark And Deep To Find Zero-Day Exploits Before Day Zero, Kevin Murnane, August 2016, Forbes
10. Absolute Extends Power of Resilience To Expanded Ecosystem Of Leading Endpoint Security Applications, February 2020, AiThority
11. https://www.absolute.com/
12. The Leading AI Cyber Security Firms (Part 1), June 2020, Cyber Security Intelligence
13. https://bluehexagon.ai/
14. Eight leading AI/ML cybersecurity companies in 2020, March 2020, Jonathan Greig, ZDNet
15. https://www.callsign.com/product/
16. CrowdStrike Introduces Enhanced Endpoint Machine Learning Capabilities and Advanced Endpoint Protection Modules, February 2017, CrowdStrike
17. https://www.crowdstrike.com/
18. Cyberwrite Awarded Most Innovative Cyber Risk Modeling Technology Firm by Frost & Sullivan for Its AI-powered Cyber Risk Technology, August 2020, Frost & Sullivan
19. https://www.cyberwrite.com/
20. Cylance Unveils "Cylance Smart Antivirus;" AI-Powered Antivirus for Consumers, July 2018, Business Wire
21. https://www.blackberry.com/us/en/products#ai
22. The Leading AI Cyber Security Firms (Part 1), June 2020, Cyber Security Intelligence
23. https://www.darktrace.com/en/cyber-ai-platform/
24. Deep Instinct Launches First Commercially Available, Real-Time Cybersecurity Solution Based on Deep Learning, November 2015, GlobeNewswire
25. Deep Instinct Delivers Integrated Protection Through Integration with Micro Focus ArcSight, January 2018, Business Wire
26. https://www.deepinstinct.com/
27. FICO Cyber Risk Score Is First on AWS Marketplace, December 2019, FICO
28. FICO Enterprise Security Score Gives Long-Term View of Cyber Risk Exposure, August 2016, FICO
29. https://www.fico.com/
30. Kount Launches Next-Generation AI, Changing How Payments Fraud Prevention is Delivered, June 2019, Kount
31. https://kount.com/
32. SECURITI.ai Unveils PRIVACI.ai, the First-Ever 'PrivacyOps' Platform that Automates Data Privacy Compliance, August 2019, SECURITI.ai
33. https://securiti.ai/
34. Artificial Intelligence in Cybersecurity – Current Use-Cases and Capabilities, Raghav Bharadwaj, July 2019, Emerj Artificial Intelligence Research
35. https://www.shieldx.com/
36. AI for Cybersecurity in Banking – Where Banks Are Investing Today, Raghav Bharadwaj, August 2019, Emerj Artificial Intelligence Research
37. https://www.tessian.com/
38. Eight leading AI/ML cybersecurity companies in 2020, March 2020, Jonathan Greig, ZDNet
39. https://www.vadesecure.com/en/
40. AI for Cybersecurity in Banking – Where Banks Are Investing Today, Raghav Bharadwaj, August 2019, Emerj Artificial Intelligence Research
41. https://www.welcome.ai/tech/security/versive
42. https://www.esentire.com/
43. Eight leading AI/ML cybersecurity companies in 2020, March 2020, Jonathan Greig, ZDNet
44. https://zeronetworks.com/product/

Authors

Amit Khullar

Senior Industry Principal – Infosys
amit_khullar@infosys.com

Anjani Kumar

Principal Consultant – Infosys
anjani_kumar@infosys.com

Producers

Jeff Mosier

Senior Consultant – Infosys
jeff.mosier@infosys.com

Harry Keir Hughes

Senior Consultant – Infosys
harrykeir.hughes@infosys.com

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.
To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

For more information, contact askus@infosys.com

Infosys®
Navigate your next