ARCTIC WOLF

END CYBER RISK

WHITE PAPER

Hybrid AI Offers the Cybersecurity Industry's Most Effective Defense

Today's threat landscape is vastly complex and constantly evolving, which currently makes it impossible for AI-based solutions to eliminate humans in the loop while maintaining a strong security posture.

Artificial intelligence (AI) and machine learning (ML) technologies are used increasingly to develop the next generation of cybersecurity solutions. These solutions make it easier for organizations to identify advanced cyberattacks while reducing your cost to manage such solutions. Unfortunately, many have a misconception about AI. People often imagine there is a human-like brain inside the machine that is capable of handling complex tasks and reducing their need to hire any security experts to manage such solutions. This is not the case. Today's threat landscape is vastly complex and constantly evolving, which currently makes it impossible for AI-based solutions to eliminate humans in the loop while maintaining a strong security posture.

This white paper walks through the cybersecurity challenges facing the market and the limitations of AI and machine-learning solutions when applied to cybersecurity. It discusses why human-augmented machine learning is necessary to address these challenges and describes how Arctic Wolf uses Hybrid AI and other supporting capabilities in our cloud-based security operations platform to provide the industry's most effective cybersecurity defense and incident response.

Cybersecurity Challenges Facing the Market

Security breaches make news headlines on an almost daily basis. One example many are familiar with is Equifax, the credit reporting company whose breach revealed the private information of 143 million people (half of the US population). Ransomware attacks such as WannaCry and Petya have impacted hundreds of hospitals and clinics, manufacturing plants, and point-of-sale terminals across the globe. No one is immune to such cyberattacks, and many organizations are facing the same challenges:

Too many alerts, too much data:

Many organizations have invested in perimeter and endpoint security products to protect themselves from common cyberthreats, but lack a solution to gain centralized visibility across all products. Each of these point products produces hundreds of log records per day, resulting in alert fatigue for limited IT staff.

Cybersecurity skills shortage:

As the volume of cyberattacks increase, so does the demand for security talent. With a huge shortage of security skills in the industry, many companies find it impossible to hire and retain security experts. Hence, existing IT staff are spread too thin and lack the security skills required to hunt down and triage advanced threats and mitigate risks.

Lack of actionable information:

When it comes to cybersecurity, there is no lack of data in log records, but there is a huge shortage of contextual intelligence on who, what, when, and where the attack originated or what it targeted, as well as what actions to take to mitigate the risk. This is where having the latest threat intelligence and human expertise makes a big difference.

With humans in the loop (HITL), a security expert can use machine learning with threat intelligence to detect both well-known malware strains and zero-day exploits depending on the model. For the newer strains, the security analyst should examine behaviors through the entire kill chain and discover additional threat intelligence parameters to accurately classify this new strain of malware. The analyst can then tweak the machine-learning model to automatically detect this new strain of malware anytime in the future.

Arctic Wolf Security Operations with Hybrid AI

As the leader in security operations, Arctic Wolf recognizes limitations of AI's application in cybersecurity and leverages Hybrid AI to deliver the best of both worlds.

Hybrid AI combines human intelligence with machine-scale performance to deliver exponentially better threat detection, greatly reduce false positives, and speed up time between detection and response. It applies the Concierge Security® Team's experience and intuition from handling real-life security incidents to machine learning to enhance and refine its detection capabilities.

The Role of AI in Cybersecurity

The analytics capacity required to handle massive amounts of data from thousands of sources is far beyond the cognitive capabilities of a human being. Leveraging the superior computing capabilities of machines is one way to address this issue, and that is driving the need for AI across any cybersecurity solution. However, AI has yet to reach the performance of human intelligence and intuition, and CISOs must factor that in when considering it as part of their security operations infrastructure.

These are the two major types of machine-learning styles used in all AI systems, with some using just one or a blend of both depending on how they are designed.

- **Supervised machine learning:** We consider this the approach where a machine learning model is refined based on the reinforcement of positive outcomes. Here detections are based on a good amount of "known" threat data that is labeled and supplied to the model as examples. This helps the model classify threats and identify attacks accurately. A good analogy is predicting the predisposition of a disease like diabetes in a new set of patients, using parameters like height, weight, age, and blood sugar levels associated with "known" diabetes patients.
- **Unsupervised machine learning:** For these models, detections are based on anomalous patterns automatically extracted from large sets of data that are unlabeled. Consider situations where you do not know what threat parameters to look for, these models have the ability of identify patterns that may have been undetectable by humans. This tends to result in a lot more false-positives and alerts during the learning phase and could, result in alert fatigue and operational inefficiencies. It is analogous to identifying a new strain of virus (similar to a zero-day attack), where the causes of the disease are not yet known.

Like any advanced technology, both supervised and unsupervised machine learning are not something that can be set once and forgotten. Cybercriminals continuously modify their approach and invent new delivery methods to bypass existing cyber defenses that may use machine learning techniques. Therefore, human expertise is required to filter-out false positives and fine-tune the algorithms by using good threat data and threat intelligence.

Hybrid AI – Harnessing the Potential of AI in Cybersecurity

Let's see why a Hybrid AI approach with a human in the loop (HITL) is essential to harness the full potential of AI and accurately detect new strains of ransomware.

Environments that choose to implement machine learning solutions without adequate human involvement may find these tools are actually more detrimental to their security posture than not having them at all. Implementing machine learning without proper management could result in the models either generating a high rate of false positives and harmful noise or outright missing detections. It's not unlike installing a security camera without ensuring that it is in focus or pointing in the correct direction. Without the correct tuning and management, the only thing it provides is a false sense of security.

Arctic Wolf Concierge Security® Team (CST)

The CST is the primary contact for every Arctic Wolf customer. The CST becomes an extension of your internal team, who understands your network infrastructure and business risks, and has the security expertise to hunt down advanced threats and recommend response actions.

The CST is the primary contact for every Arctic Wolf customer. The CST becomes an extension of your internal team, who understands your network infrastructure and business risks, and has the security expertise to hunt down advanced threats and recommend response actions. The CST acts as your trusted advisor, regularly reports on the effectiveness of your security posture, and conducts business reviews to provide strategic insights into your cybersecurity investments.

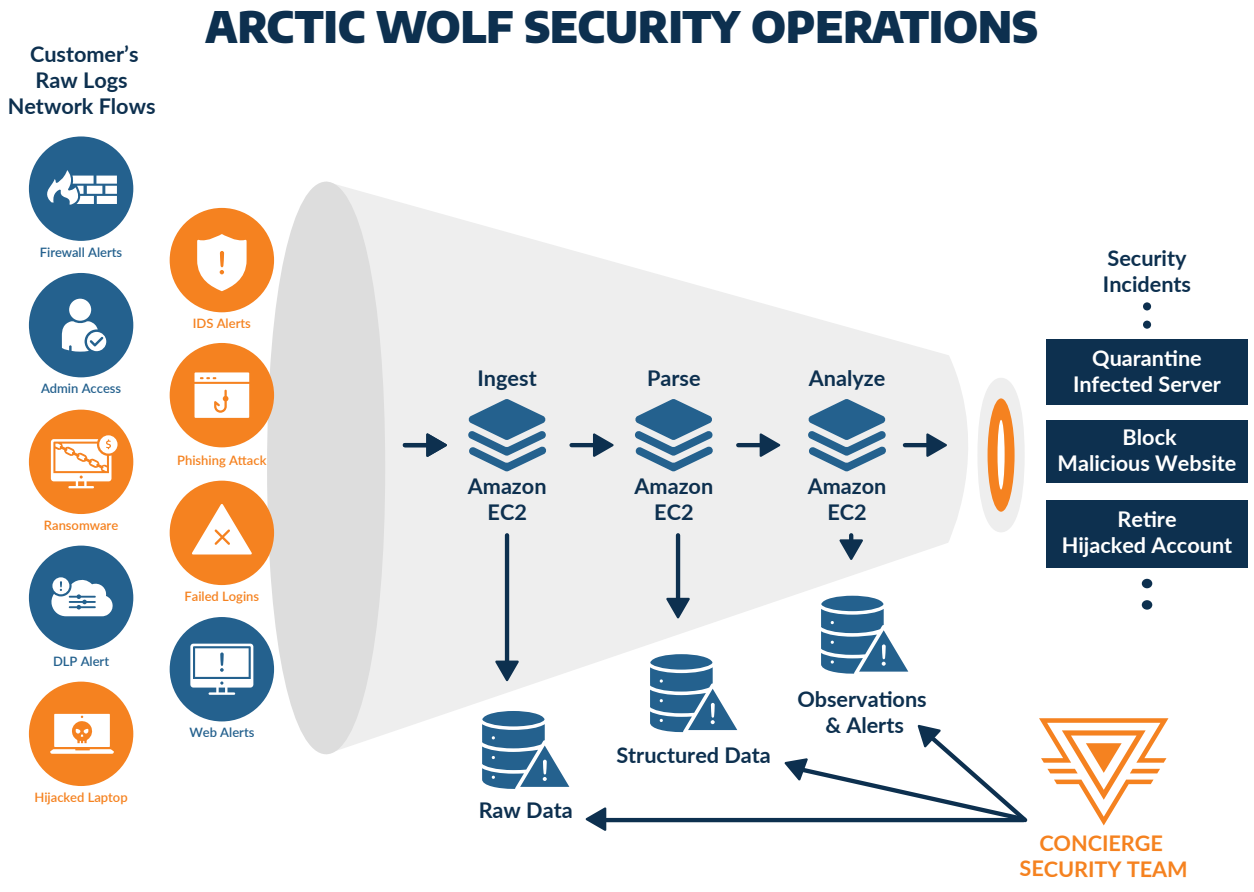
The CST uses the following unique capabilities in the Arctic Wolf Security Operations Platform to incorporate new data, handle unexpected events, and apply additional context to provide the best protection in the industry.

Security Optimized Data Architecture

The Arctic Wolf security operations platform is cloud-based and built on a highly scalable multi-tenant architecture that is optimized for handling security events. It ingests over 65 billion events per day, which it parses and then aggregates into structured observations.

The data is then analyzed in context using behavior analytics and cyber threat intelligence to escalate only the most severe incidents across all customers. This leads to a 99.9997% reduction in the volume of incidents requiring customer action, which amounts, on average, to less than one security incident per week per customer.

As shown in the diagram below, the Arctic Wolf® Platform leverages Amazon Web Services (AWS) cloud infrastructure to dynamically scale computing and storage resources using AWS Elastic Computing (EC2) and simple storage services (S3). This allows Arctic Wolf to ingest, parse, and analyze unlimited amounts of raw logs from multiple customers and still give the CST quick access to security-related data in any level—raw, structured, or observations/alerts.



Multiple Machine Learning Loops

The Hybrid AI approach can provide 10X better accuracy than standard AI-based technology because it uses multiple learning loops to refine security incidents and filter out the noise at each stage of the ingesting, parsing, and analysis process.

Human-to-human learning loop:

The CST interacts with the customer during onboarding, understands customer business risks, and develops a baseline of normal operation. This allows for detection of anomalies within customer telemetry. The CST provides regular updates and reports on a customer's security posture, and escalates security incidents only when action is needed to mitigate/remediate business-critical issues.

Human-to-machine learning loop:

The CST sets customizable security policies in the Arctic Wolf Platform to fine-tune our Customizable Rules Engine (CRulE) to eliminate any noise (false positives) and detect advanced threats using configurable policies. These configurable policies can be broadly applied to all customers, and yet customized to a specific customer's special needs.

Machine-to-machine learning loop:

The platform uses threat intelligence and behavior analytics information in correlation with rules to accurately identify the latest threats. It leverages a diverse set of threat intelligence data, such as software vulnerabilities, advanced malware, emerging network threats, and web-based threats.

Customizable Security Policies

The CST uses the Customizable Rules Engine (CRulE) to define customized security policies and:

Eliminate noise:

These custom rules selectively filter out noisy events that represent no real security risk unique to the customer and allows for the elimination of false positives.

Detect known threats:

These rules identify cyberattacks originating from known malicious IP addresses and websites/URLs, or suspected ransomware attacks, which use known command-and-control servers for exchanging encryption keys.

Detect unknown threats:

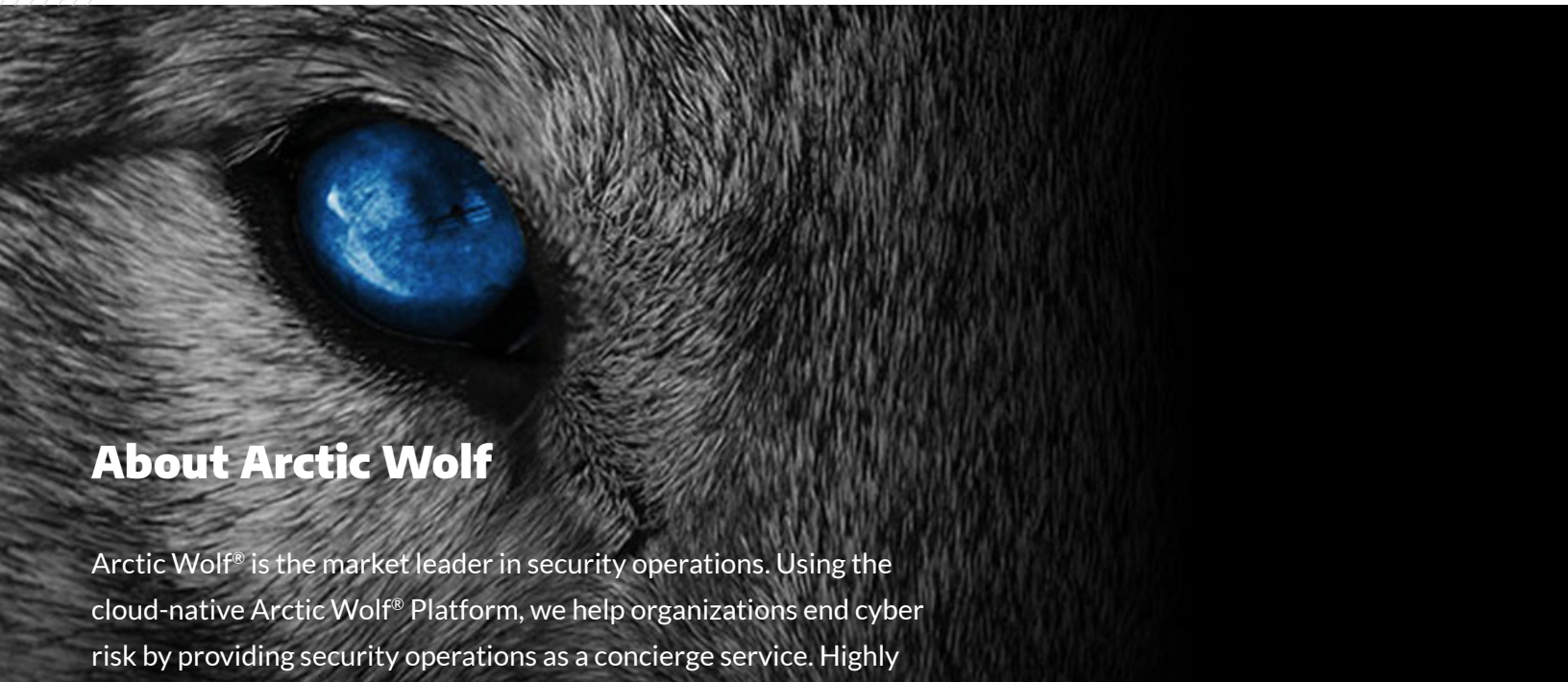
These rules detect evolving and difficult-to-identify attacks—such as new phishing attempts or credential compromise—when the Arctic Wolf Platform detects anomalous behavior. This could include unusual, privileged user activity or frequent failed login attempts on Active Directory.

The Best of Both Worlds

Keeping humans in the loop can greatly improve the results of AI and machine learning.

Machines and algorithms are great for automating known quantities, but new threat data often requires human intervention to properly categorize it. Using machine learning to classify malicious and benign activity, while humans focus on the grey areas, is the most effective combination to tackle today's threat landscape of constantly evolving cyberattacks.

Arctic Wolf security operations with Hybrid AI combines the best of AI with the CST's expertise, so our customers get the best of both worlds. Combining human intelligence with machine scale capabilities creates a winning combination that allows CISOs to leverage AI for world-class security operations.



About Arctic Wolf

Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf® Platform, we help organizations end cyber risk by providing security operations as a concierge service. Highly trained Concierge Security® experts work as an extension of your team to provide 24x7 monitoring, detection, and response, as well as ongoing risk management to proactively protect systems and data while continually strengthening your security posture. And we now provide managed security awareness training to better inform and prepare your employees about security best practices and how to effectively respond against social engineering attacks.

For more information about Arctic Wolf, visit arcticwolf.com

Contact Us

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com