BforeAI

www.bfore.ai

The Future of Predictive Security: A Manifesto

Enabling Preemptive Cyber Defense (PCD) and Preemptive Fraud Detection (PFD)

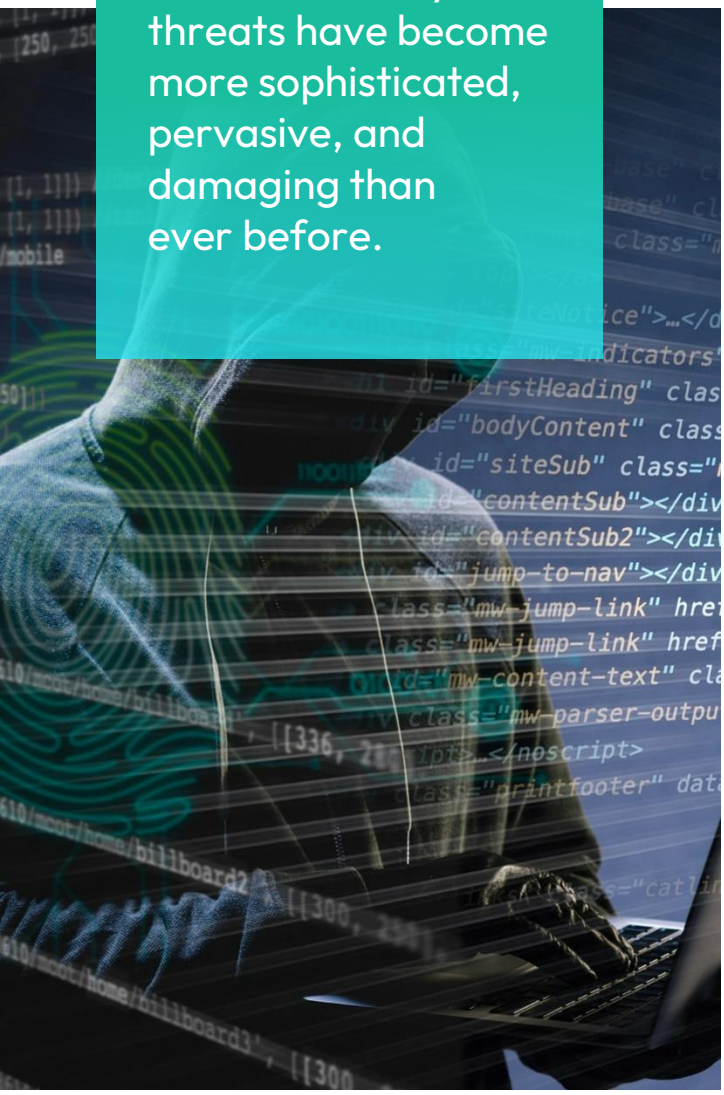
2025 JAN

Table of content

In this report:

Yesterday's cybersecurity can't stop tomorrow's attacks

In today's digital environment, cyber threats have become more sophisticated, pervasive, and damaging than ever before.



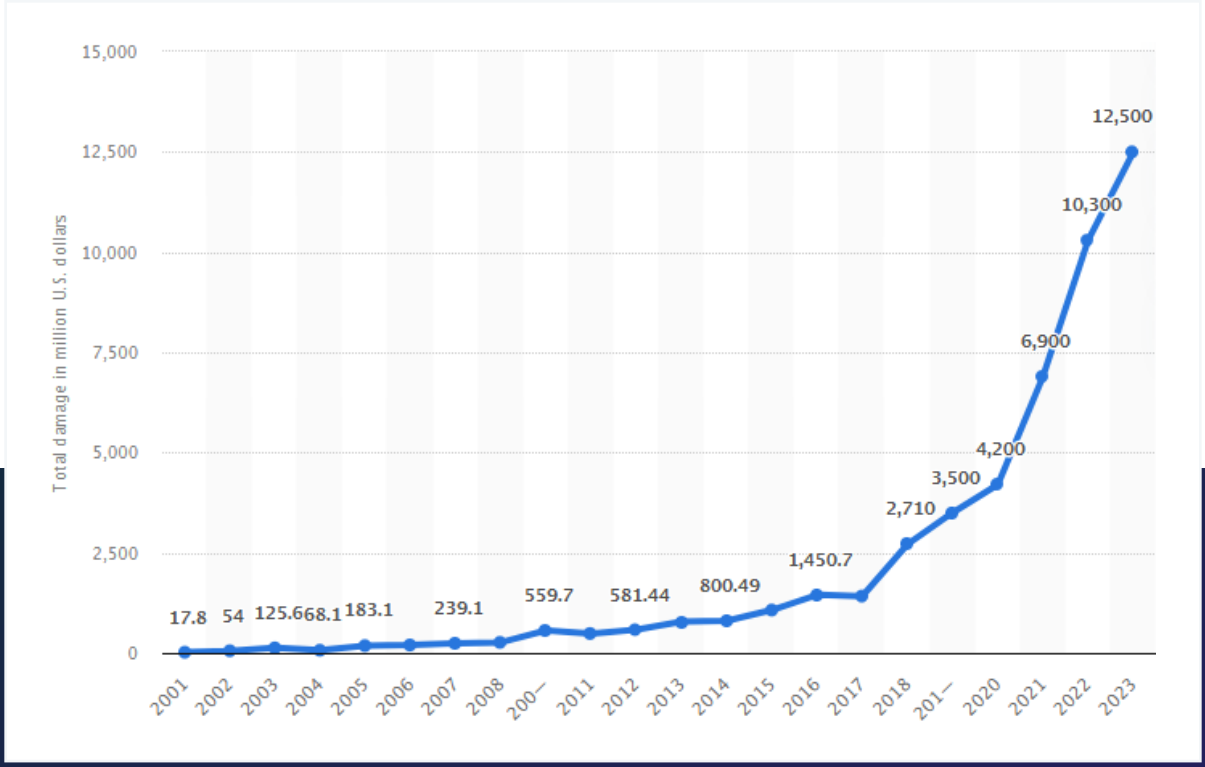
With the rapid adoption of remote work and increasingly interconnected systems, attack surfaces have expanded. While cloud computing, open networks, and the Internet of Things(IoT) create incredible convenience and opportunities for innovation, they also present more opportunities for threat actors to exploit vulnerabilities.

These attackers are not only leveraging traditional techniques but are also employing new tactics. Advanced malware can change its code to avoid detection, and complex social engineering methods can trick even the most attentive employees into exposing company data. This evolving threat landscape is outpacing conventional cybersecurity defenses, which commonly rely on inadequate methods such as signature-based detection—meaning, only previously known attackers are flagged, and new malicious infrastructure goes unnoticed. **As a result, the need for innovative technologies in cybersecurity has never been more urgent.**

The prevailing belief in cybersecurity is that the only response to any cyberattack is reactive. In other words, organizations wait to become a victim of a phishing attack, a ransomware event, a data breach, or a DDoS attack. Only after an attack is launched can they start responding. But what if technology could proactively predict the next cyberattack and disrupt a malicious infrastructure even before the attack has been launched?

With attackers constantly refining their methods and exploiting new technological vulnerabilities, the cybersecurity industry must also reinvent its defense systems to stay ahead of the criminals' methods. Today, predictive technologies enable organizations to shift from a reactive stance to a proactive defense model by identifying and disrupting risks before they evolve into full-scale attacks.

In a world where data breaches and cyberattacks can result in severe financial, operational, reputational, and social harm, having the ability to anticipate and mitigate threats has become a crucial aspect of a comprehensive cybersecurity posture. Cybersecurity experts call this new category of solutions Preemptive Cyber Defense (PCD).These technologies are designed to prevent, stop, or deter cyberattacks from achieving their objectives[1].



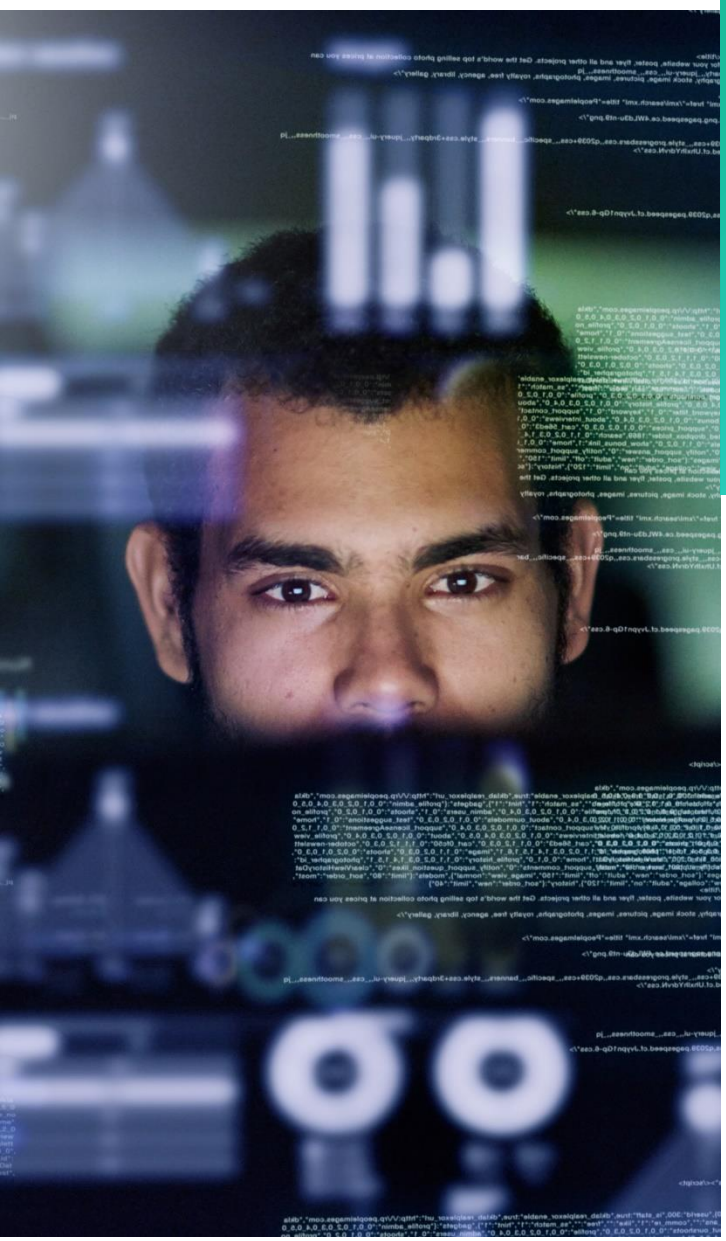
Annual amount of monetary damage caused by reported cybercrime in the United States from 2001 to 2023(in million U.S. dollars) - Statista

[1] https://www.gartner.com/en/documents/5916175

Unlike traditional systems, which often rely on historical data and known signatures to detect threats, PCD approaches use advanced algorithms and machine learning to analyze patterns, forecast potential risks, and proactively adapt to emerging threats. By leveraging the latest advancements in behavioral artificial intelligence and machine learning, these systems can analyze vast amounts of data, uncover subtle indicators of potential attacks, and provide actionable insights in real-time. This shift from a passive and reactive stance to anticipating cyberattacks and taking steps to prevent them from happening in the first place is essential in addressing modern threats and building resilient digital defenses.

> With a commitment to addressing modern cybersecurity challenges, amplifying the role of AI in their development, and driving how these advancements are shaping the future of digital security, BforeAI has become a pioneer in predictive technologies in cybersecurity.

Real-World Intelligence and Its Role in National Security



For governments, intelligence is the process of gathering, analyzing, and interpreting data about potential threats to a nation's security. Governments worldwide rely on intelligence to anticipate and understand real-life threats – such as military invasions, terrorist plots, and large-scale criminal activities – often well before they reach a critical point. This information is derived from various sources, including human intelligence (HUMINT), signals intelligence(SIGINT), imagery intelligence (IMINT), and open-source intelligence (OSINT). The goal is to develop a clear picture of an adversary's intent, capabilities, and potential actions, enabling informed decisions to protect national interests.

Through intelligence, governments can detect threats by identifying unusual patterns, emerging plans, and hostile preparations. Intelligence teams work to piece together information from different sources, creating a comprehensive understanding of adversarial behavior. For instance, human informants may reveal terrorist cell activities, while communications monitoring might intercept encrypted messages hinting at an impending attack. Detection and correlation of these signs allow governments to deploy early countermeasures, from raising public alerts to strengthening critical defenses, ultimately preventing the threat from fully materializing.

From Detection to Preemption

Once a threat is detected, governments may choose to act preemptively to neutralize it before it unfolds. Preemptive action involves a range of tactics, such as targeted strikes, arrests, or cyber operations that aim to disrupt an enemy's plans.

In a military context, preemptive strikes are a classic example. If intelligence reveals an imminent threat, such as troop mobilization or weapons deployments, a nation may strike first to prevent or weaken the coming attack. This doctrine of preemption is rooted in the idea of preventing potential harm before it reaches a critical stage, reducing the likelihood of a full-scale conflict and minimizing casualties.

Leveraging Deterrence to Prevent Attacks

Deterrence complements intelligence and preemption by creating a defensive posture so strong that adversaries are discouraged from even considering an attack. In the military sphere, deterrence is often discussed in terms of nuclear capabilities, where the mere possession of devastating weapons acts as a powerful deterrent against adversaries.

By showcasing robust defensive capabilities, such as advanced weaponry, well-trained forces, or cyber resilience, a nation signals to its enemies that an attack would not succeed or would incur unacceptable costs.

But how can technology mimic in the digital space what happens in the physical world?

The Role of AI in Cybersecurity

Artificial Intelligence (AI) is transforming cybersecurity by significantly enhancing our ability to detect and respond to cyber threats. Specifically, AI can drastically reduce reaction times —making the difference between stopping an attack in its tracks and suffering devastating consequences. In today's fast-paced cyber threat landscape, where the element of surprise is often on the side of attackers, AI helps level the playing field.

The Growing Need for AI in Cybersecurity

The pace of cyberattacks underscores the urgency of leveraging AI for protection. Consider these alarming statistics[2]:

Ransomware attacks:

Hackers can penetrate a business network in as little as 45minutes, with ransomware attacks occurring every 11 seconds on average.

Speed of data theft:

The average hacker needs only 9.5 hours to steal valuable data, while organizations take an average of 197 days to detect a breach and an additional67 days to contain it.

Phishing emails:

Nearly 30% of phishing emails are opened, and these emails account for 91% of all cyberattacks.

Malware deployment:

Malicious actors deploy malware at a staggering rate of 11.5 attacks per minute.

AI is critical in mitigating these threats by providing continuous monitoring, analyzing vastamounts of data in real time, and identifying anomalies that human brains might miss.

[2] *https://venturebeat.com/security/the-ai-edge-in-cybersecurity-predictive-tools-aim-to-slash-response-times/*

Key Benefits of AI in Cybersecurity

Advanced Threat Detection

AI can process enormous amounts of data almost instantaneously, identifying even the subtlest anomalies in network traffic, user behavior, and system logs. It can flag deviations from predicted patterns in real-time, ensuring that threats — whether from malware or sophisticated cybercriminals — are predicted before they can cause harm. For instance, behavioral AI can predict and block ransomware attempts well before the typical 45-minute window attackers need to execute their plans.

Behavioral Analytics

AI-powered behavioral analytics offer unmatched precision. Machine learning (ML), a subset of AI, learns normal user behavior patterns, such as consistent login credentials, application usage, and file access. Hackers, by contrast, display distinctly irregular behavior by seeking out sensitive data or exploiting system vulnerabilities. AI detects these deviations and triggers immediate alerts, minimizing the opportunity for attackers to operate undetected.

Reduction of False Alarms

Without AI, cybersecurity teams must spend excessive time responding to false positives —similar to firefighters answering false alarms triggered by overly sensitive smoke detectors.
AI reduces this inefficiency by learning to differentiate between benign anomalies and genuine threats, allowing security teams to focus on critical issues rather than wasting hours on false alerts.

Continuous Monitoring and Adaptation

Unlike human staff or traditional security systems, AI works tirelessly around the clock, identifying and analyzing behavioral patterns in real time. It constantly monitors changes in the open internet infrastructure, gathering actionable insights to refine its threat-detection capabilities. For many organizations, achieving such comprehensive, non-stop monitoring without AI would require prohibitively large teams and resources.

One of AI's most impactful contributions to cybersecurity is its ability to automate a preemptive response. While some business leaders may feel uneasy about relinquishing control to automated systems, AI-driven responses can be configured to align with specific comfort levels. Typically, AI manages low-level threats autonomously while escalating complex incidents for human review. The benefits of automated response include:

- **Speed and efficiency:**
  Pre-programmed responses to emerging threats occur instantly, minimizing damage and mitigating risks in real time.
- **Reduction of human error:**
  Most successful breaches are linked to human mistakes. AI, however, follows predefined protocols, eliminating vulnerabilities that could be exploited due to oversight or error.
- **Scalable solutions:**
  AI can handle the workload of entire teams, adapting to large-scale networks and architectures.

AI not only reacts to threats; it also predicts and prevents them. By analyzing historical data and identifying patterns, AI anticipates potential attack vectors and proactively strengthens defenses. For example, it can predict phishing attempts based on communication trends or detect potential insider threats by monitoring user activity anomalies.

Traditional methods of detecting cyber threats and their limitations

The increasing sophistication of cyber attacks necessitates more advanced detection mechanisms. Traditional methods often rely on signature-based detection. Signature-based detection works by identifying unique patterns (signatures) in the code or behavior of known malware. However, these methods have limitations when dealing with previously unknown threats. Advanced malware is often “polymorphic” or “metamorphic,” meaning it’s designed to constantly change and thereby avoid detection.

Signature-based detection is reactive, not proactive. It relies on patterns or specific indicators that have been previously identified as malicious. This means that for a threat to be detected, it must match a known, pre-existing pattern. If the malware’s code changes, the signature will not match, and the detection may fail. In other words, it works well for known threats but struggles with unknown ones, as signatures are only created once a threat has already been discovered and analyzed. Attackers exploit this limitation by creating malware that does not yet have a signature or modifies itself to avoid detection.

Polymorphic Malware and Constant Code Changes

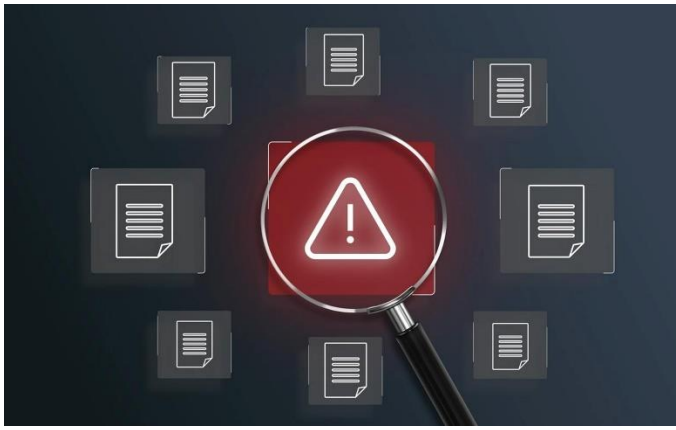
Polymorphic malware is designed to change its code structure or appearance with each infection, making it look different every time it spreads. In many ways, this is analogous toa virus mutating so human antibodies are no longer effective. Polymorphic malware often uses encryption to obscure its code. Each time the malware runs, it decrypts itself to execute the payload, then re-encrypts with a different key or pattern before infecting another system. Signature-based systems cannot detect the encrypted code if they don't have a matching signature for each unique version. This allows the malware to avoid detection by appearing as a "new" program each time it runs, even though the core functionality remains the same.

Metamorphic Malware and Full Code Restructuring

Unlike polymorphic malware, which merely changes appearance, metamorphic malware completely rewrites its code each time it propagates. This advanced level of modification makes it even harder to detect because no part of the malware remains static. Metamorphic malware analyzes its own code and re-codes itself to remove any recognizable patterns or characteristics. It may rearrange instructions, insert irrelevant operations (no-ops), or replace functions with equivalent alternatives, resulting in a unique binary each time. Some metamorphic threats go even further by changing how they perform basic functions, like using different algorithms or operational approaches to avoid behavioral patterns typically used in signatures.

Advanced Evasion Techniques

Many advanced threats use anti-analysis techniques that detect when they're being examined in a sandbox or virtual machine and modify their behavior accordingly. For example, some malware will "sleep" or remain dormant if it senses a virtual environment, avoiding detection by signature-based systems that rely on capturing malicious behavior during analysis. Some malware is designed to deliver its payload in stages, where the initial stage appears benign and thus goes undetected. Once inside a network, it downloads or assembles the actual malicious code, which may have a unique signature that the detection system has not seen before. This technique is called multi-stage delivery.



Fileless Malware and Memory-Based Attacks

Traditional signature-based detection relies heavily on scanning files on disk. Fileless malware, which resides in memory or abuses legitimate system tools, bypasses these scans by not creating files on the hard drive. Fileless malware can inject malicious code directly into the memory of legitimate processes. Because this code never touches the disk, traditional systems may miss it, especially if the injected code has no static signature that a signature-based system would recognize.

In any case, all traditional detection tools are effective after an organization has been attacked, or right of the boom. It is often too late. The organization can only react to what happened.

> Organizations cannot afford to discover an attack after it's occurred. Cybersecurity must be preemptive — acting before there's a breach.

The Power of Graph Inference

Given the current cybersecurity challenges, modern cybersecurity approaches increasingly turn to behavioral analysis and machine learning for detection. These methods look for suspicious activities, such as unusual system calls, network traffic, or behavioral anomalies, rather than relying on static patterns.

Parallel Doctrines in Cybersecurity: Intelligence, Detection, Preemption, and Deterrence

In the field of cybersecurity, the doctrines of intelligence, detection, preemption, and deterrence are equally relevant and can be applied with parallel strategies to counter digital threats.

The development of predictive cybersecurity technologies is deeply rooted in the latest advancements in AI, including machine learning, natural language processing, and deep learning. Machine learning models can now process massive data streams, identifying hidden patterns and potential threats far earlier than traditional methods. Natural language processing allows predictive technologies to understand and analyze threat intelligence reports, picking upon early indicators of threat activity. Furthermore, deep learning techniques are enhancing the ability of predictive systems to detect even the most subtle anomalies, continuously improving accuracy and resilience against a wide array of attack vectors.

Rather than merely reacting to attacks after they occur, deterrence preemptively removes the incentive for threat actors to target an organization in the first place. Think of it like a bank putting money in a time-lock safe - it's a deterrent that makes it much harder for criminals to obtain access.

By leveraging advanced AI-driven threat intelligence, BforeAI preempts malicious activity long before it escalates into an attack. This predictive approach neutralizes threats early, diminishing the potential for damage and signaling to attackers that targeting the protected environment is both futile and costly.

In this context, BforeAI has developed PreCrime™, an advanced technology designed to predict and preempt cyber threats by leveraging graph inference techniques.

PreCrime™ is built on the methodologies outlined in two pivotal research papers: Following Passive DNS Traces to Detect Stealthy Malicious Domains Via Graph Inference[3] and A Domain is Only as Good as its Buddies: Detecting Stealthy Malicious Domains via Graph Inference[4].

[3] *https://www.researchgate.net/publication/342723340_Following_Passive_DNS_Traces_to_Detect_Stealthy_Malicious_Domains_Via_Graph_Inference*
[4] *https://www.researchgate.net/publication/323393061_A_Domain_is_only_as_Good_as_its_Buddies_Detecting_Stealthy_Malicious_Domains_via_Graph_Inference*

What is Graph Inference?

> Graph inference is a method of deriving new information about entities by analyzing the relationships and structures within a graph.

To perform graph inference, data is first organized into a graph structure. For cybersecurity applications, graphs will analyze various digital entities – such as user accounts, network devices, IP addresses, domains, or files – and their relationships, such as shared IP addresses or similar behavior patterns. By analyzing the structure and properties of these graphs, it is possible to infer the likelihood of certain entities being malicious.

Graphs often start with a few known data points or “seed” nodes. These known nodes might have labels indicating benign or malicious status, for example, based on prior threat intelligence. From these seeds, relationships and properties propagate to connected nodes in the graph, gradually building an understanding of other nodes.

How does the Inference Process work?

One of the most common graph inference methods, label propagation involves starting with some known labels or properties of nodes (such as reliable or unreliable) and spreading this information through the network to predict labels for unclassified nodes. For instance, if a node is strongly connected to a majority of reliable nodes, it might infer a similar property.

Graph inference often includes pattern recognition and identifying clusters, or groups of nodes with stronger internal connections than external ones. This helps infer that nodes within a cluster likely share similar characteristics or behaviors.

Inference processes can also use random walks and connectivity-based methods, which involve tracing paths through the graph by randomly selecting edges to follow, which can reveal clusters, identify communities, or estimate the likelihood of relationships. Nodes that are "closer" to each other in terms of graph connectivity might be inferred to have stronger relationships.

Graph Inference Techniques

Graph inference techniques are applied to analyze the constructed graphs. These techniques include:

Anomaly detection:

By understanding what normal relationships in a graph look like, graph inference can detect anomalies, such as unusual connections or isolated nodes that do not fit the standard pattern.

Link prediction:

Another key application is predicting which new edges, or connections, are likely to form. This helps in identifying domains that are likely to become malicious based on their current associations.

Community detection:

This consists of identifying clusters or communities within the graph that exhibit similar behavior. Malicious domains often cluster together due to shared infrastructure or coordinated activities.

Predictive analytics:

Graph inference is used to make predictions, such as which infrastructure is the most likely to prepare a cyberattack against a certain infrastructure.

How PreCrime™ works

PreCrime™ leverages the methodologies outlined above to detect stealthy malicious domains. Here is a step-by-step breakdown of how PreCrime operates:

Data Collection and Preprocessing

PreCrime™ begins by collecting multiple network data points from thousands of sensors deployed across the Internet. The tool observes more than 1 billion infrastructures and 500million domains on a continuous basis – of them, 500,000 are created every day. Data is collected between 5 to 10 times per hour which enables observing any changes on a continuous and precise basis. This data is then preprocessed to remove noise and irrelevant information, ensuring that only meaningful interactions are considered. In total, PreCrime collects several terabytes of data on a daily basis.

Graph Construction and Feature Extraction

Next, PreCrime™ constructs a graph from the preprocessed data. Features such as query frequency, temporal patterns, and resolution paths are extracted and incorporated into the graph. Over 400 billion behaviors and edges are mapped in the graph database. These features provide a detailed view of domain interactions, which is crucial for accurate inference.

Application of Graph Inference Techniques

PreCrime™ applies various graph inference techniques to analyze the constructed graph. Four billion malicious behaviors are mapped in PreCrime. Community detection algorithms identify clusters of domains that exhibit similar behavior, while anomaly detection algorithms highlight nodes with abnormal patterns. Link prediction algorithms are used to forecast potential future connections, helping to identify emerging threats.

Detection and Mitigation: Disruption and Takedown

PreCrime™ re-scores over 20 million suspicious infrastructures on a daily average out of which it predicts 100,000 future attack infrastructures. Based on the results of the graph inference analysis, PreCrime detects infrastructures that exhibit characteristics of malicious behavior. They are flagged for further investigation and mitigation. PreCrime's preemptive approach ensures that potential threats are identified and neutralized before they can cause harm.

Predictive Threat Intelligence: PreCrime™ Intelligence

PreCrime™ Intelligence leverages predictive attack intelligence to upgrade network security solutions to become predictive and avoid cyber attacks before they hit their target IT infrastructure. Network security teams augment their existing network security solutions by integrating the feed received from PreCrime Intelligence through an API integration with their SIEM, SOAR, or XRD/EDR, Protective DNS, network blocking using firewalls and web filters/anti-phishing filters. PreCrime does not send Indicators of Compromise (IoC's), as these indicators are the sign of an already existing compromise, but sends Indicators of Future Attack (IoFAs) instead as a prediction, with a median identification of 18 days ahead of IoCs sent by classical threat intelligence tools. The false positive rate of 0.05% avoids distribution to business while reducing risk associated with network intrusion, and encrypted or stolen data.

By implementing preemptive blocking, network assets and company resources are protected before an attack starts. PreCrime Intelligence addresses risks associated with techniques involving external network communications. For internal or off-the-network techniques (e.g.,rogue employee, social engineering) alternative detect and respond solutions should remain in place.

Preemptive blocking can be the cause of concerns as false positives might cause business disruption. In order to avoid this type of incident, PreCrime Intelligence regularly re-scores IoFAs and self-corrects in nearly every case well before any activity could be disrupted.

The advantage of prediction is indeed the head-up provided both for attack blocking, and also to avoid operational network disruption.

BforeAI

Fraud prevention for Digital Risk Protection Services (DRPS): PreCrime™ Brand

PreCrime™ Brand is a proactive impersonation protection solution that can prevent account takeover and credit card or credential stealing from customers' customers, or protect our customers' suppliers from being attacked in email compromises. This mitigates fraud, reputational harm risk from negative brand damage, or customer credential stealing.

PreCrime Brand identifies a malicious infrastructure only minutes after its creation, puts a network disruption in place within in minutes after identification, and requests action to various takedown operators, who subsequently disturb DNS resolution or content removal, resulting in infrastructure takedown. Our privileged access to the takedown operators (including domain and DNS, content, industry alliances for abuse and malware prevention, law enforcement agencies, and independent response bodies) ensures malicious infrastructure is promptly removed. Our predictive technology is so effective that more than 80% of our takedowns are completed before there's content on the infrastructure.

In parallel, information is shared with BforeAI's disruption partners – e.g., VirusTotal, Quad9,Spamhaus, and Google Safe Browsing – who subsequently put the malicious identified domain in a DNS resolution blocklist. Within 10 minutes on average, up to 75% of the traffic to the malicious infrastructure is already blocked.

How Do Takedowns Work?

Once a malicious infrastructure has been identified and a prediction of an attack has been carried out, PreCrime™ automatically engages with relevant infrastructure service providers involved, such as Hoster, Mail provider, Registrar, Registry, Content Delivery Network (CDN),National CERT/CSIRT, or ICANN.

By providing detailed information on the observed behaviors, PreCrime™ input assists the operator in qualifying the intent of their user as future malicious and carries an account suspension or infrastructure takedown.

Prediction is generated from the behavior, whether the infrastructure already includes active content or not. PreCrime™ may also engage with mail providers to remove A and MX records to quickly disable the infrastructure from being accessible to the threat actor.

Depending on the nature of the takedown, BforeAI engages with law enforcement, cybersecurity industry alliances for abuse and malware prevention, and independent response bodies to further disable infrastructure and threat actors. On a case-by-case basis, the process continues based on the domain and operators' requests and processes.

Advantages of using PreCrime™ and challenges to overcome

PreCrime's ability to detect threats before they manifest ensures a more robust defense against cyber attacks. The use of various internet data sources allows for scalable monitoring of large networks. Advanced graph inference techniques help in minimizing false positives, focusing on genuinely suspicious activities.

However, using AI requires high-quality data, significant computational resources and expertise, and ensuring that BforeAI can respond to attackers who may develop evasion tactics to circumvent graph-based detection methods.

How does PreCrime™ collect data?

The effectiveness of PreCrime™ depends heavily on the quality and completeness of Internet metadata. BforeAI has created its own network of sensors that collect data continuously from across the internet. This enables us to maintain high-quality standards, leading to rapid detection and accurate predictions, with minimized false positives and false negatives.

How does PreCrime™ navigate complexity?

Implementing and maintaining graph inference systems requires significant computational resources and expertise. BforeAI has developed proprietary techniques to exploit graphs in a fast and performant way.

Predictive AI will be the foundation of modern cybersecurity

Security is no longer confined to organizations — it now extends to protecting their customers as well.

PreCrime™ represents a significant advancement in the field of cybersecurity, leveraging graph inference techniques to detect and prevent stealthy malicious activities. By analyzing internet data and constructing detailed graphs, PreCrime can identify suspicious patterns and associations that traditional methods miss. As cyber threats continue to evolve, technologies like PreCrime will undeniably play a crucial role in maintaining robust cybersecurity defenses.

Integrating AI into cybersecurity is one of the most cost-effective ways to enhance an organization's defenses. AI provides efficiency by performing the work of dozens of security analysts tirelessly, adaptability by continuously learning from evolving threats, and comprehensive protection by preventing breaches and identifying insider threats — offering vigilance and staying ahead of attackers in ways manual processes cannot. For any organization serious about protecting its digital assets, integrating AI is not just an option; it is a necessity.

By applying the doctrines of intelligence, detection, preemption, and deterrence to cybersecurity, organizations can adopt a proactive and comprehensive approach to digital defense. This strategic parallel helps build a cyber defense that not only protects assets but also discourages attackers, ultimately fostering a safer digital environment. As with national security, this layered approach is essential for addressing the complex and dynamic nature of modern cyber threats.

About BforeAI

BforeAI is a pioneer in Predictive Attack Intelligence, Preemptive Cyber Defense and Digital Risk Detection. Our PreCrime™ platform uses behavioral AI to predict and automatically preempt malicious campaigns, resulting in the fastest, most accurate solution to stop attacks weeks before they happen. To learn more, visit bfore.ai