Solution Brief

Groundbreaking Threat Intelligence Advancements from McAfee Labs

Gain the advantage over adversaries

Enterprise security professionals are well aware that attackers are rapidly gaining an advantage. Security teams are constantly scrambling to stay ahead of the next complex, large-scale campaign often targeted at specific organizations. Adversaries have fine-tuned their tools to such an extent that only 12 to 15 toolkits are responsible for generating millions of unique malware samples. And 70% to 90% of malware samples are unique to a single organization.[1] Sophisticated and continually evolving cyberattack techniques, like botnets, ransomware, and advanced persistent threats (APTs), evade security solutions and are increasingly difficult to detect, thwart, remediate, and prevent in the future. A sense of urgency dominates every decision and every action. Organizations are coming to the realization that a collaborative, proactive threat defense is absolutely essential for an effective defense. Security operations and threat/incident management starts with a solid understanding of who the adversaries are, what tactics they use, indicators of compromise (IoCs), which surfaces are at risk, and, potentially, motivations behind the attack. And that's where high-quality, actionable threat intelligence comes into play for protection, detection, analysis, and containment.

Threat intelligence is gaining ground in today's security organizations. A recent SANS Institute survey reveals that 69% of respondents are using threat intelligence to some extent, and 37.6% of those using threat intelligence are seeing a 50% improvement in their organization's response to events in terms of context, accuracy, and/or speed.[2]

Threat Intelligence Obstacles

But getting visibility to today's threat landscape can be a complex proposition. It's easy, for example, for security teams to drown in the volume of threat intelligence data produced by sensors and other threat intelligence sources. The endless variety of threat intelligence data and the relevance of this data require understanding and advanced analytics to extract value and high-quality insights to help solve cybersecurity problems.

There's also the issue of freshness. As attackers evolve their techniques and strategies, a certain amount of threat intelligence loses relevance quickly. By the same token, having a historical perspective can help researchers understand context and help them get a better handle on trends. Data consumption and analysis need to occur at light speed so that hackers lose their edge.

intel Security

Finally, turning threat intelligence into tactical and operational wisdom requires more than just transformation. It also calls for cross-correlation from multiple sources. The bottom line is that not all threat intelligence is created equal, nor should it be used in the same way.

The question also arises as to whether organizations have the wherewithal to have their own in-house threat intelligence teams. The main obstacles are the shortage of threat analysts and their high salaries, which are beyond the budgetary reach of most enterprises.

McAfee Labs Today: Proactive, Predictive, and Prescriptive Threat Intelligence

A better approach is to engage with a leading-edge threat intelligence provider. Based on solid threat visibility, CISOs and security operations teams can now make decisions with greater confidence—without the expense of hiring an internal team. McAfee® Labs has evolved into an innovative provider of proactive, predictive, and prescriptive global threat intelligence with a proven reputation that spans more than two decades. Combining in-depth threat knowledge with a broad set of advanced identification methodologies and automation tools, McAfee Labs enriches products and enables them to protect, detect, and correct faster and more accurately.

McAfee Labs offers a unique approach to threat intelligence grounded in research, threat analytics, and knowledge. Its latest advancements include three key functional components:

- A cloud infrastructure connected to millions of global sensors.
- Automation and machine learning to collect and transform data sourced from sensors, third-party sharing communities, historical repositories, and customers.
- A broad variety of analytics and human interpretations from a variety of data sets. The analysis process encompasses both real-time interpretation and historic data mining based on two decades of research and is facilitated by a large cloud compute surface.

The Cloud Infrastructure and Big Data

With threat coverage across historical and geographical parameters and multiple threat vectors, the McAfee Labs cloud infrastructure expands the size, dimension, and collection/ingestion speed of threat intelligence. Data is gathered from millions of endpoints, gateways, and mobile devices and a broad sweep of IT environments, geographies, and threat actors. McAfee Labs is able to respond to millions of requests around the world via nine data centers, whose data is refreshed every five minutes.

This is further enhanced by 25 years' worth of accumulated data to provide enterprises with knowledge for deep analytics and trend mapping. This broad set of data types is stored in the McAfee Labs proprietary classification system and covers one petabyte of data—which is equivalent 13.3 years of HDTV content (approximately 58,292 movies).

Shared third-party threat information via the Cyber Threat Alliance further enriches this knowledge base. The Cyber Threat Alliance is a consortium of 174 different threat intelligence and threat feed providers that crowdsource and share threat intelligence. Cyber Threat Alliance processes more than 500,000 file samples and 350,000 URLs daily. The goal is to both strengthen vendors' capabilities against adversaries and constantly improve their customers' defenses across all sectors.

McAfee Labs

- 250 researchers across 13 countries.
- Portfolio of approximately 300 patents since 1990 and almost 100 in the last six years.
- A network of millions of sensors spanning the Internet and distributed globally.
- More than 300 new threats tallied every minute, or more than five every seconds.
- Services are consumed by multiple types of security tools: web protection, firewall and intrusion prevention systems, endpoint defenses, sandbox technologies, and integrated third-party products.

Automation

Advanced McAfee Labs automation technologies improve the volume and speed of threat intelligence delivery. These automated capabilities, enhanced by human assistance, collect and transform threat insights, such as file types, indicators of compromise (IoCs), reputation lists, and exploits into knowledge within minutes, rather than hours. Suspicious files are consumed and processed at a capacity of one million files per day. Innovations in automation have resulted in a 20% improvement in URL cloud publication intervals. The window of threat exposure is narrowed, thanks to reputation refresh intervals every five minutes. Ultimately, automation helps transform product telemetry and threat intelligence data into countermeasures and containment procedures across Intel Security and third-party solutions.

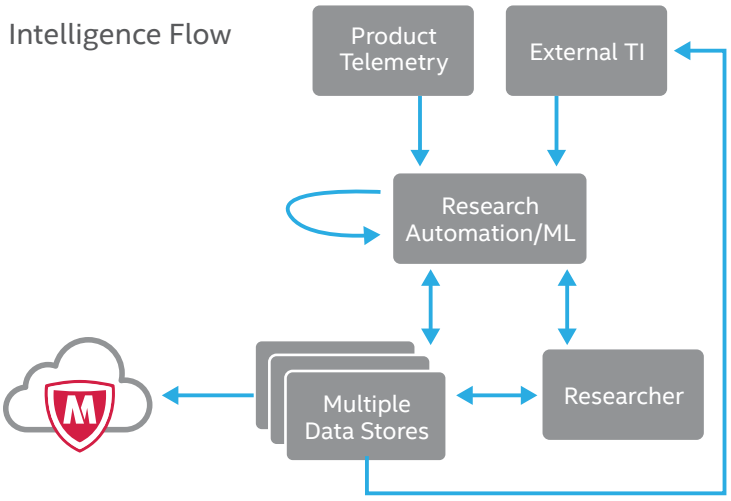

Figure 1. The flow of threat intelligence across McAfee Labs.

Based on telemetry from millions of endpoints plus external threat intelligence submissions, McAfee Labs generates more than 10,000 new and updated protection drivers daily. Average processing time is 12 minutes. Additionally, automated machine learning feeds via data mining; proactive, in-depth threat surface inspection; and expert analysis conducted by our researchers—all processed in a multisequenced, automated manner—provide users with swift protection and detection and a 99.98% accuracy rating.

As described in Figure 1 above, the combination of continuous product telemetry, human analytics, machine learning, and existing heuristics increases detection accuracy and containment quality. Our team of data scientists monitors data 24/7 for quality, with an internal baseline standard of 0.01% false positives. For example, over the past several years, external tests placed McAfee Endpoint Security among the top security solutions with low false positive rates. In early 2016, Intel Security received the **AV TEST usability award** for its McAfee Endpoint Security client solution. To test its ability to protect users, this client solution was required to visit websites, evaluate installations, and scan millions of files without triggering any false positives.

Analytics and deep learning

To get to results, threat insights are gleaned from machine learning, as well as from automated, behavioral-based classification in the cloud to detect zero-day malware on endpoints. Machine learning, which drives the proactive threat intelligence model, is derived from the combined capabilities of a number of key elements: applications, analytics and collaborative data science, data handling, and the cloud infrastructure.

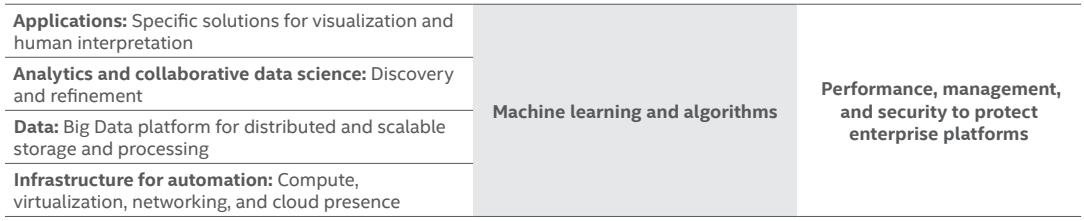

Figure 2. McAfee Labs cloud infrastructure.

Human analysts work hand in hand in a closed loop with machine learning tools to adjust the learning and analytic models. For example, exclusive McAfee Labs automation technology gathers intelligence from live malware samples though its extensive network of millions of global sensors. The automation technology executes multiple analytics against these samples to determine whether the files are malicious or not. The output is often a file hash (=id) with a classification that can be used by human investigators.

Data points provided by the automation tools help threat researchers find similar samples so that they can create generic signatures or drivers. Analysts then write these drivers and add them to beta endpoint signature updates consumed by the automation technology, which tests the success of the signature and determine whether there are false positives. When a new generic driver is developed, all the malware samples that were used to create the signature are reprocessed in order to ensure detection effectiveness. In addition, samples submitted by humans can be pushed through dynamic analysis, reducing the time spent by researchers on malware analysis.

Use Cases

Use case 1: Predictive attack campaign detection via McAfee Global Threat Intelligence (McAfee GTI) usage statistics

Usage: McAfee Labs frequently publishes insights on new and popular emerging threat campaigns in the McAfee Labs Threats Reports and on its dashboards. Additionally, McAfee Labs updates individual product security control protections based on data mining and learnings derived from McAfee GTI usage statistics.

Benefits: Readers of the McAfee Labs Threats Reports and threat center statistics get fast and easy visibility into strategic threat intelligence and global emerging threats. In addition, security controls receive automated, preventive updates on new threats before they start proliferating.

Cloud Intelligence Components, Data and Methods	
Big Data	• 125 terabytes of threat reputation data servicing 188 million sensors and producing 44 billion file, web, certificate, and IP reputations queries daily. • Continuous threat feeds via the Cyber Threat Alliance.
Automation	• Continuous monitoring of sensors, providing 420 billion lines of telemetry data per month. • 1.5 million files analyzed per day, with average processing time of less than 12 minutes, continually producing new reputation data.
Analytics and Deep Learning	• Supervised learning detects quickly emerging threat campaigns by correlating existing known malware against new geographical and URL variants. • Discovers 245 new threats vectors per minute.

Use case 2: Zero-day malware protection with Real Protect

Usage: Real Protect analyzes file behavior and translates the results into static and dynamic classifiers. By comparing the classifiers against known good and bad behavior, the Real Protect client proactively stops high-risk executables.

Benefits: Real Protect stops threats before they cause harm—and, even more significantly, this occurs at lightning speed and with minimal human involvement.

Functional Components and Data Elements	
Big Data	• Usage of millions of static and dynamic file classifiers from Real Protect clients.
Automation	• Continuously updates endpoint with known good and bad static classifiers. • Automated forwarding of dynamic classifiers into the cloud to detect unknown behavior.
Analytics and Deep Learning	• Compares dynamic classifiers via unsupervised Euclidian distance learning to detect and block new malware variants.

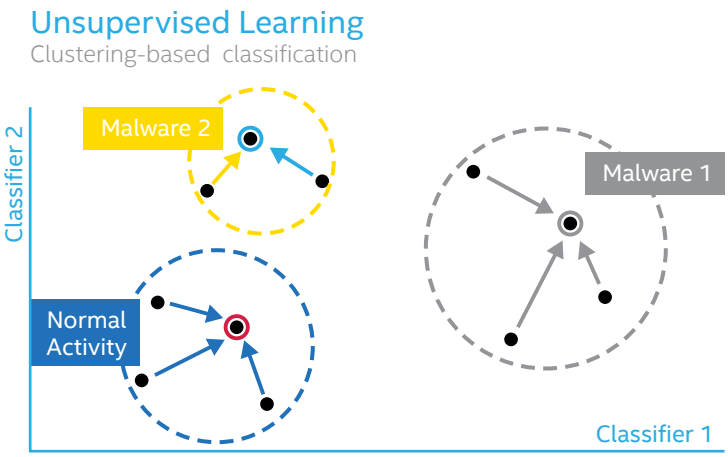

Figure 3. Unsupervised machine learning in Real Protect.

Euclidian Distance Learning
Also called "similarity learning," Euclidian distance learning is a form of machine learning, with the ability to learn from similar, already known examples. It measures how similar or related two objects are and is often used for applications in ranking, recommendation systems, profiling (identity tracking), and voice

Use case 3: Rapid containment with McAfee Cloud Threat Detection

Usage: McAfee Cloud Threat Detection offers organizations a convenient new cloud-based service that plugs into our existing solutions (McAfee Network Security Platform, McAfee Web Gateway, and McAfee® ePO™ Cloud) to help contain zero-day advanced malware and expose evasive threats.

Benefits: The cloud service enables organizations to easily take advantage of significant compute horsepower to operate an array of the latest analysis techniques that enhance detection and optimize existing security investments. McAfee Cloud Threat Detection can be integrated with existing enterprise infrastructures for more effective countermeasures, management, and orchestration.

Functional Components and Data Elements	
Big Data	• Massive footprint allows usage of a broad and rich set of file classifiers that encompass behavior, genealogy, network usage, and McAfee Web Gateway.
Automation	• Automated and integrated with existing Intel Security Infrastructures. • Perpetually updated with intelligence from a broad ecosystem.
Analytics and Deep Learning	• Validates classifiers for prevalence. • Correlates against gray data and field metadata.

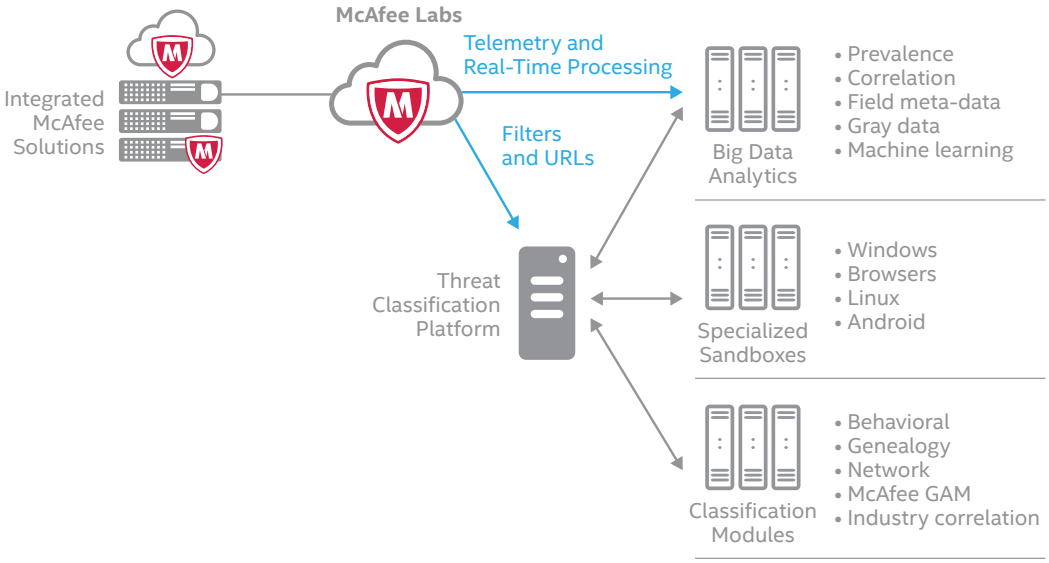

Figure 4. McAfee Cloud Threat Detection cloud-based service.

Summary: The Benefits of Cloud Intelligence

- **Broad set of threat visibility**: McAfee Labs Cloud Intelligence delivers a broad set of threat insights, including emerging threat trends (McAfee Threats Report), tactical file analysis via McAfee Cloud Threat Detection, and operational, behavioral-based protection data via McAfee Real Protect. McAfee Labs Cloud Intelligence provides a broad set of actionable data to combat adversaries on multiple fronts.
- **Integrated timely response**: By connecting Intel Security products into cloud intelligence platforms, organizations can get a jump on adversaries via proactive threat intelligence based on known patterns. McAfee Labs can even predict new forms of campaign outbreaks via Bayesian networks, as well as proactively deliver a new set of detection and protection updates to customer-deployed products.
- **Affordable and accessible intelligence**: McAfee Cloud Threat intelligence is deployed across multiple regions and data centers—all within easy reach via a redundant cloud model that even syncs up with the controls when temporarily unconnected. This cloud service allows organizations to easily take advantage of significant compute horsepower without the capital expenditure or the effort and cost of provisioning and maintaining an on-premises appliance.

Learn More

To learn more about cloud intelligence output and supported products, visit the links below.

Threat Center: **http://www.mcafee.com/us/threat-center.aspx**

Advanced Threat Analysis: **http://www.mcafee.com/us/products/advanced-threat-analysis/index.aspx**

McAfee Endpoint Security: **http://www.mcafee.com/us/products/endpoint-protection/endpoint-security.aspx**

McAfee Global Threat Intelligence: **http://www.mcafee.com/us/threat-center/technology/global-threat-intelligence-technology.aspx**

1. **http://www.mcafee.com/us/resources/white-papers/wp-understanding-ransomware-strategies-defeat.pdf**
2. **https://www.sans.org/reading-room/whitepapers/analyst/who-039-s-cyberthreat-intelligence-how-35767**

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com