radware

AUTOMATION vs. AUTOMATION

BATTLING CYBERATTACKS WITH MACHINE LEARNING AND AI

ORGANIZATIONS ARE LOSING THE CYBERSECURITY RACE

Cyberthreats are evolving faster than security teams can adapt. The proliferation of data from dozens of security products is outpacing the ability of security teams to process it. And budget and talent shortfalls limit the ability of security teams to expand rapidly.

The question is how does a network security team improve the ability to scale and minimize data breaches when all the while dealing with increasingly complex attack vectors? The answer is automation.

THE ROLE OF AUTOMATION IN SECURITY

Four of five organizations reported facing some form of network- or application-based cyberattack in 2017, according to Radware's *2017–2018 Global Application & Network Security Report*. Zero-day malware, botnets and Burst attacks — all sterling examples of automated attack vectors — saw significant increases in usage in 2017, according to the same report.

The numbers don't lie. Cybercriminals are becoming more savvy and their attacks increasingly automated. Furthermore, it's evident that traditional DDoS mitigation methods, such as rate-based or manually tuned protection, are outdated solutions to safeguard sensitive data in the wake of automated cyberattacks.

IT organizations now face advanced persistent threats that are spearheaded not by human assailants but by automated bots. Security personnel are no match for these intense, sustained attacks and are incapable of keeping up with the sheer volume of incoming threats. Legacy DDoS mitigation solutions that leverage rule-based event correlation can generate thousands of alerts in a 24-hour span. On a good day, a SOC can only investigate approximately one hundred.

Additionally, their ability to make quick and impactful decisions to manually address an attack is equally inefficient. Research shows that machine-learning botnets are now capable, in certain situations, of scanning a network for vulnerabilities and successfully breaching its defenses in less than 20 seconds. That is why automation is becoming such a powerful and effective component of cybersecurity. To combat the onslaught of incoming threats, organizations must employ an army of equivalent strength and sophistication.

ATTACKERS LEVERAGE AUTOMATION

Cybercriminals are weaponizing automation and machine learning to create increasingly evasive attack vectors, and the internet of things (IoT) has proven to be the catalyst driving this trend. IoT is the birthplace of many of the new types of automated bots and malware.

At the forefront are botnets, which are increasingly sophisticated, lethal and highly automated digitized armies running amok on corporate networks. For example, hackers now leverage botnets to conduct early exploitation and network reconnaissance prior to unleashing an attack.

The Mirai botnet, which was made famous by its use in the *2016 attack on DNS provider Dyn*, along with its subsequent variants, embodies many of these characteristics. It leverages a network-scanning and attack architecture capable of identifying "competing" malware and removing it from the IoT device to block remote administrative control. In addition, it leverages the infamous Water Torture attack to generate randomized domain names on a DNS infrastructure. Follow-up variants use automation to allow the malware to craft malicious queries in real time.

Modern-day malware is an equally sophisticated multivector cyberattack weapon designed to elude detection using an array of evasion tools and camouflage techniques. Hackers now leverage machine learning to create custom malware that defeats anti-malware defenses. One example is Generative Adversarial Network algorithms that can bypass black-box machine-learning models. In another example, a cybersecurity company adapted Elon Musk's OpenAI framework[1] to create forms of malware that mitigation solutions couldn't detect.

AUTOMATION FOR DETECTION AND MITIGATION

So how does a network security team improve its ability to deal with these increasingly multifarious cyberattacks? Fight fire with fire. Automated cybersecurity solutions provide the data-processing muscle to mitigate these advanced threats.

Executives clearly understand this and are ready to take advantage of automation. According to Radware's *C-Suite Perspectives: Trends in the Cyberattack Landscape, Security Threats and Business Impacts* report, the vast majority of executives (71%) report shifting more of their network security budget into technologies that employ machine learning and automation. The need to protect increasingly heterogeneous infrastructures, a shortage in cybersecurity talent and increasingly dangerous cyberthreats were indicated as the primary drivers of this fiscal shift.

In addition, the trust factor is increasing. Four in 10 executives trust automated systems more than humans to protect their organization against cyberattacks, according to the same report.

How Hackers Use Machine Learning

- Increasingly Evasive Malware
  - Use Generative Adversarial Network algorithms
  - MalGAN generates adversarial malware samples
- Hivenets and Swarmbots*
  - Smarter botnets using self-learning "hivenets" and "swarmbots"
  - BrickerBot: Autonomous PDoS botnet
- Advanced Spear Phishing at Scale
  - Using Natural Language Processing (NLP) algorithms for better social engineering
  - Training on genuine emails, scraping social networks/forums, stolen records, etc.†
- Raising the Noise Floor
  - Poisoning a security model by flooding it with so many false positives that it causes recalibration of the model or "fooling" security solutions into creating new security policies via automated attack campaigns

* Fortinet Predicts Highly Destructive and Self-Learning "Swarm" Cyberattacks in 2018

† Stresspaint Malware Targeting Facebook Credentials

1 https://www.theregister.co.uk/2017/07/31/ai_defeats_antivirus_software/

Traditional DDoS solutions use rate limiting and manual signature creation to mitigate attacks. Rate limiting can be effective but can also result in a high number of false positives. As a result, manual signatures are then used to block offending traffic to reduce the number of false positives. Moreover, manual signatures take time to create because identifying offending traffic is only possible AFTER the attack starts. With machine-learning botnets now breaching defenses in less than 20 seconds, this hands-on strategy does not suffice.

Automation and, more specifically, machine learning overcome the drawbacks of manual signature creation and rate-limiting protection by automatically creating signatures and adapting protections to changing attack vectors. Machine learning leverages advanced mathematical models and algorithms to look at baseline network parameters, assess network behavior, automatically create attack signatures and adapt security configurations and/or policies to mitigate attacks. Machine learning transitions an organization's DDoS protection strategy from manual, ratio- and rate-based protection to behavioral-based detection and mitigation (see Figure 1).

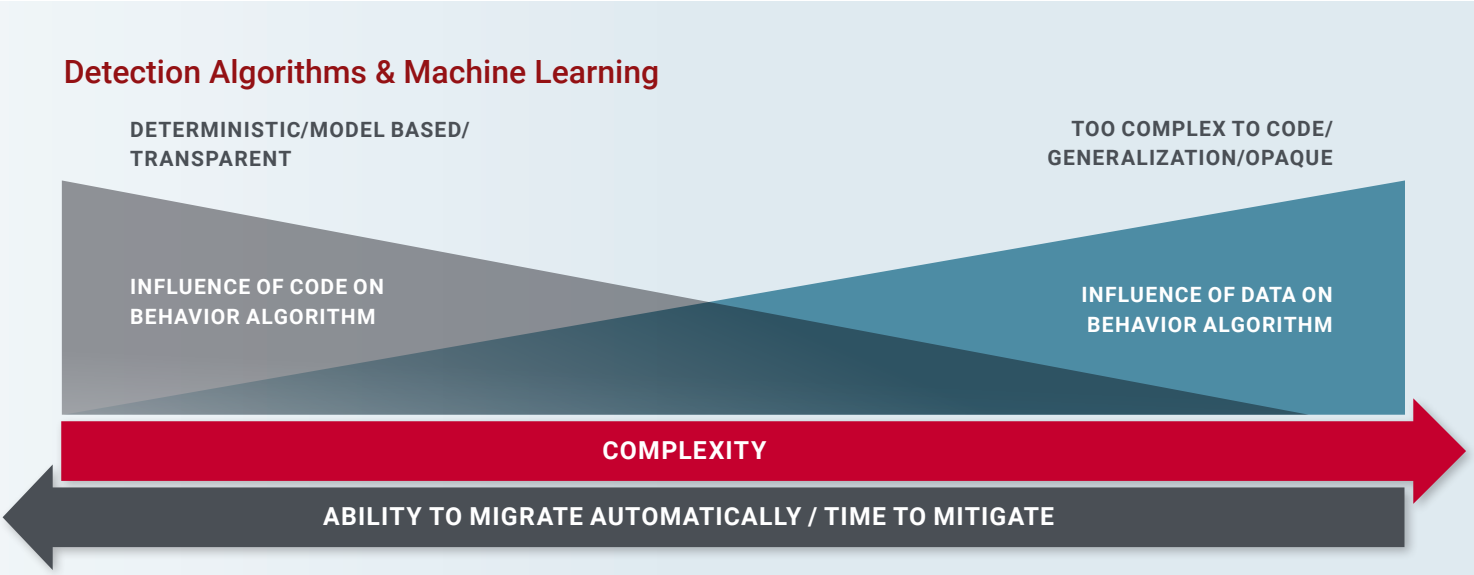

Figure 1: Machine learning moves DDoS protection models from the left to the right

A market-leading DDoS protection solution combines machine-learning capabilities with negative and positive security protection models to mitigate automated attack vectors, such as the aforementioned DNS Water Torture attacks made notorious by Mirai. By employing machine learning and ingress-only positive protection models, this sort of an attack vector is eliminated, regardless of whether the protected DNS infrastructure is an authoritative or a recursive DNS.

The final step of automated cybersecurity is automated self-learning. DDoS mitigation solutions should leverage a deep neural network (DNN) that conducts postanalysis of all the generated data, isolates known attack information and feeds those data points back into the machine-learning algorithms. DNNs require massive amounts of storage and computing power and can be prohibitively expensive to house and manage within a privately hosted data center.

Machine-Learning Algorithms

- K-Means Clustering
- Logistic Regression
- Bayesian Linear Regression
- Support Vector Machine
- Principal Component Analysis

As a result, ideally a DNN is housed and maintained by your organization's DDoS mitigation vendor, which leverages its network of cloud-based scrubbing centers (and the massive volumes of threat intelligence data that it collects) to process this information via big data analytics and automatically feed it back into your organization's DDoS mitigation solution via a real-time threat intelligence feed. This makes the input of thousands of malicious IPs and new attack signatures into an automated process that no SOC team could ever hope to accomplish manually.

The result is a DDoS mitigation system that automatically collects data from multiple sources and leverages machine learning to conduct zero-day characterization. Attack signatures and security policies are automatically updated and not reliant on a SOC engineer who is free to conduct higher-level analysis, system management and threat analysis.

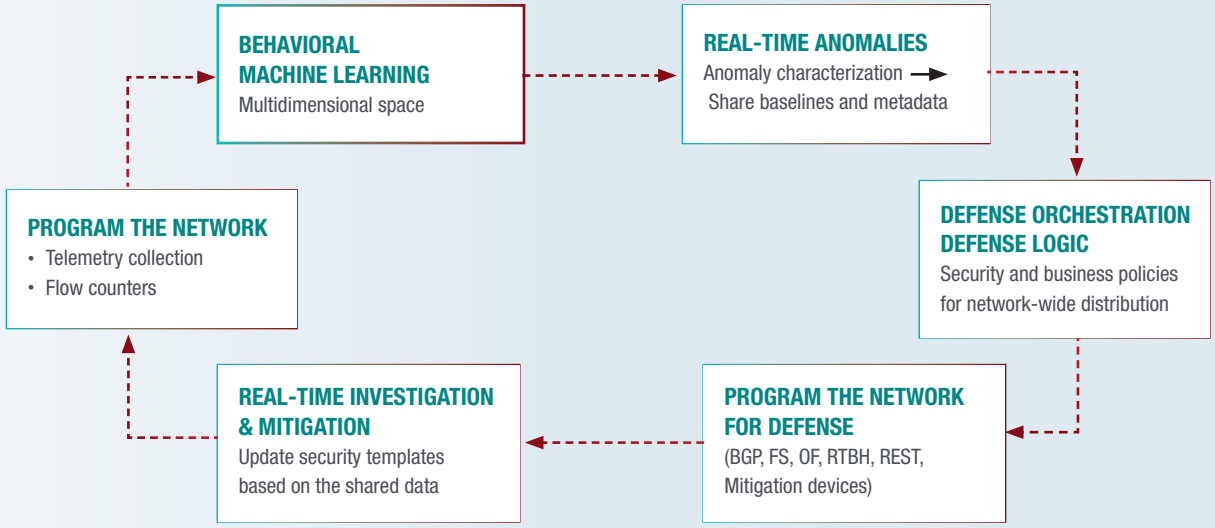

Figure 2: The security automation life cycle

AUTOMATION ACROSS THE SECURITY ARCHITECTURE

Automation expands across all facets, or layers, of the security architecture. A market-leading cybersecurity solution should be comprised of multiple systems. This includes on-premise DDoS mitigation appliances and firewalls, cloud-based scrubbing centers, command and control applications, monitoring and reporting systems and, last but not least, the aforementioned DNN.

The data plane is where traditional on-premise mitigation appliances and firewalls and/or cloud-based scrubbing centers reside. These systems are responsible for the actual detection and mitigation of cyberattacks and leverage the aforementioned machine-learning capabilities and positive and negative protection models to assess network traffic and identify malicious behavior.

Data generated by these solutions is fed to the control plane, which is comprised of a cybersecurity control solution. This is where automated policy generation takes place via workflows that take data inputs from the data plane and process them to generate and execute service provisioning, detection criteria and attack mitigation actions.

The data being fed into the control plane should be supplemented by additional data that comes from the big data/DNN plane. Ideally, this data is provided by the organization's DDoS mitigation vendor, which uses big data and analytics to identify, validate and catalog DDoS threats — like botnets, DNS attacks and zero-day malware — and feeds that information back into the control and data planes for preemptive protection.

Lastly, the management and visibility plane is the "single pane of glass" that provides a SOC team with visibility and reporting into network and application performance, an overview of attacks, security policies, etc.

Radware's suite of cybersecurity solutions, services and scrubbing centers leverage machine learning, automation and artificial intelligence across all facets of the security architecture. This allows organizations to classify, mitigate and block advanced persistent threats, zero-day malware, botnets, etc. in real time versus relying on manual and rate-based protections.

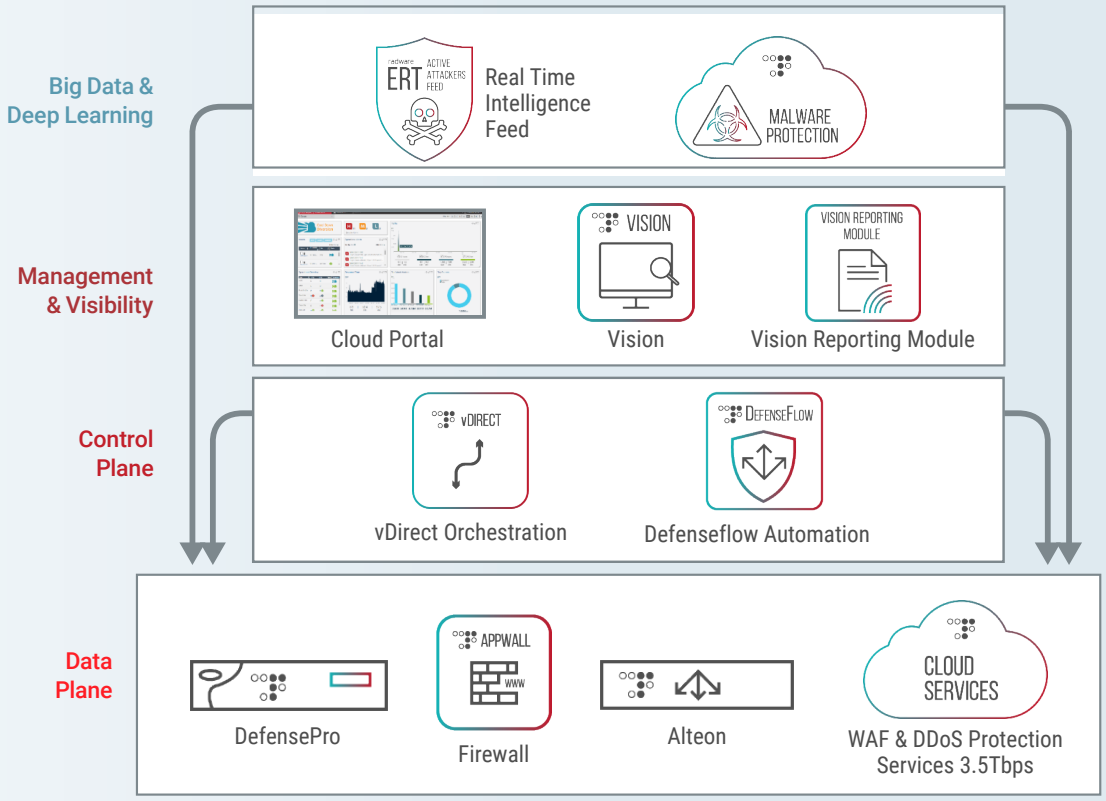

Figure 3: Real-time mitigation and detection with machine learning across Radware's security solutions and services

Automation is the future of cybersecurity. As cybercriminals become more savvy and increasingly rely on automation to achieve their mischievous goals, automation and machine learning will become the cornerstone of cybersecurity solutions to effectively combat the onslaught from the next generation of attacks. It will allow organizations to improve the ability to scale network security teams, minimize human errors and safeguard digital assets to ensure brand reputation and the customer experience.

Learn more about Radware's cybersecurity products and services.

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.