Lean on the Machine

Harnessing machine learning for data-driven cybersecurity

In today's cyberthreat environment, security teams are up against a constant flood of incoming risks. But by leveraging advanced security analytics, machine learning, and their own intuition, security experts are fighting back with agile, adaptable defense systems.

The Problem

SECURITY SHORTFALLS

While security teams comb through tens of thousands of cybersecurity alerts—trying to separate legitimate risks from the noise—attacks can slip through the cracks unnoticed and do significant damage.

Too much to handle:

16,983

17,000 alerts
number of malware warnings the average large organization has to sift through each week[1]

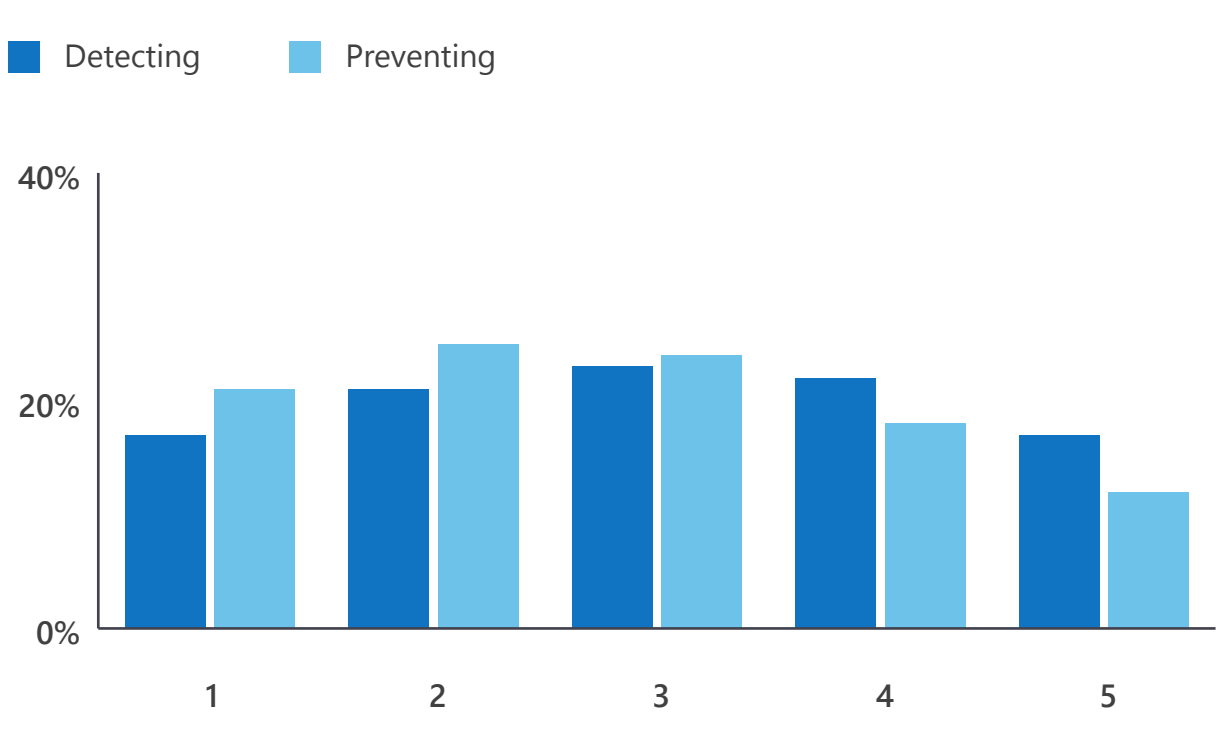
99 days
median amount of time for an organization to discover a security breach[2]

<48 hours
time it takes for attackers to have complete control of a network[3]

$4 million
average cost of a data breach to a company, not including unquantified costs of damaged brand image and compromised trust[4]

In a 2016 survey of nearly 600 IT security professionals, a majority worried they had trouble keeping up with the risks:[5]

Effectiveness of handling cyberattacks
(scale of 1–5 with 1 being not effective and 5 highly effective)



Tasks that take a significant amount of time:

68% Chasing False Positives

32% Prioritizing Alerts

Barriers to remediating serious threats:

76% Lack of visibility of the threat

63% Inability to prioritize threats

55% Lack of in-house expertise

The Process

TEAMING UP HUMAN AND MACHINE

The best system for detecting these cyberthreats—and even predicting them—is when big-data analytics, machine learning, and human expertise team up. This intelligent partnership enables security analysts to focus on the most suspicious events flagged by the system and then provide feedback that increases the machine's accuracy.

So how does it work?

STEP ONE
An AI program sifts through millions of threat data points and uses rules and algorithms to identify which are highly suspicious.

STEP TWO
It then presents a condensed list of the most probable attacks or vulnerabilities to a human cybersecurity worker.

STEP THREE
Based on feedback and actions taken by the human, the program updates its model and rules system to better identify threats.

STEP FOUR
Machine learning enables the AI to apply automation in places where a human is not needed, while getting smarter about what activity to alert to the human as a priority.

The Power

EFFICIENT AND AHEAD

A data-driven, human-guided security approach detects and responds to attacks more quickly and accurately. And with Microsoft's global network of real-time threat intelligence, it continues to evolve, anticipate, and stay ahead of risks.

One of these systems from MIT, called "AI²" exemplifies the proactive power of detecting threats as they come in.[6]

Reviews over **40 million lines** of data per day.

Narrows the number of suspicious events to **100–200 per day** for human analysis.

Incorporates analyst feedback **daily** in order to adapt to threats in real time.

Detects **85%** of cyberattacks after three months of learning feedback.

Detects **5x** fewer false positives than machine-only systems.

Intelligence matters—Microsoft's cybersecurity data comes from the most extensive technology chain of products and services in the world:[7]

18+ billion
Bing webpage scans per month

450 billion
authentications processed every month

400 billion
emails scanned for phishing and malware

200+
cloud services monitored for security risks

Even as cyberthreats and attacks continue to bombard organizations, the systems of defense are getting smarter—thanks to the powerful combination of data-driven machine intelligence and human expertise.

Learn more about Microsoft's extensive security intelligence and services by visiting www.microsoft.com/security

1 "7 steps to a holistic security strategy," 2017, Microsoft.
2 "M-Trends 2016," 2016, Mandiant Consulting.
3 "Anatomy of a Breach," 2016, Microsoft.
4 "Cost of Data Breach Study: Global Analysis," 2016, Ponemon Institute.
5 "The State of Malware Detection and Prevention," 2016, Ponemon Institute.
6 "System Predicts 85% of Cyber-Attacks Using Input from Human Experts," 2016, MIT Computer Science and Artificial Intelligence Library.
7 "Protect and Manage Your Digital Transformation," 2016, Brad Anderson: Ignite Security General Session.

Microsoft