Can AI Make Data Security Simpler (and Smarter)?

Cybersecurity teams often face tough choices, and there's typically much at stake. For example, do you rely on already overworked team members to manually sift through threat alerts, running the risk of an overlooked anomaly or trend? Or, consider this situation: You deploy an automated solution to generate attack alerts, only to get bogged down in a torrent of warnings. Many may be false positives that, again, waste the team's time.

Still, there's plenty of untapped potential for AI and data security—especially when it comes to the anomalies that precede an attack. Let's look at how things are evolving with AI and security.

Fight Fire with Fire to Improve Data Security

Security threats are evolving and growing increasingly sophisticated. Artificial intelligence (AI) and botnets are behind some of the slickest attacks.

Per IDC:

- More than 90% of organizations acknowledge being attacked by malware.
- Of those, 87% were attacked successfully.
- One-third of organizations have suffered an attack that blocked access to data or systems within the past 12 months.

The best way to stay ahead? Arm your systems and infrastructures with the same smarts and efficiency.

Why? On a security level, AI's value lies in its speed, repetition, and accuracy. Machine learning ensures algorithms get smarter over time, learning from wins and misses. Additionally, it can help by assessing risk and uncovering warnings faster than humans can. (And given the IT security talent shortage, that extra help can't hurt.) Coupled with security tools, AI can perform repetitive, tedious tasks, minute by minute. This reduces security teams' "low-brain, high-repetition" tasks, like reviewing system alerts, and frees up some of their time. Lean teams can tackle more strategic projects, like proactive "threat-hunting" exercises that detect gaps in security.

But it's not just about AI—it's also about AIOps. Coined by Gartner, AIOps is the use of AI to automate and streamline operational workflows. AIOps helps you simplify operations by removing infrastructure limitations and burdens toand having a guaranteed clean storage environment.In fact, in a study conducted by Bredin IT Research and Pure Storage, respondents listed AIOps as **the biggest effort to advance business transformation** in the U.S. and Australia.

AI on the Offense: How Analytics Can Prevent Attacks

AI can support a proactive posture for data security, so you don't have to sit and wait for attackers to get a foot in the virtual door. Instead, you want to get clues about what they're up to before the worst has occurred.

Fast analytics is the key to data security and delivering:

- **Big-data analytics:** These tasks tend to fall in the category of "needle in a haystack" applications. Think scanning millions of data points for outliers and anomalies, like large file transfers or suspicious uploads.
- **Predictive analytics:** AI can predict or forecast the likelihood of future events based on analysis of past trends and events. For example, AI may be able to predict which assets attackers are most likely to strike.
- **Behavioral analytics:** AI's unbiased approach can spot behavioral patterns such as repeated login attempts. What's the probability that a certain user's behavior is malicious? AI can analyze it quickly and with great accuracy. Once those outliers are located, a human can step in and do the critical thinking.

Without a powerful analytics platform underneath these efforts, however, this can be wishful thinking. The sheer volume of the data set required by AI to paint a full picture is staggering—but with the right platforms, these efforts are getting smarter and more viable every day.

AI is also a driving force behind email filters that can flag suspicious messages that may contain ransomware's most popular vehicle: phishing attacks. If attackers do manage to breach systems, there are other ways AI can defensively swing into action.

AI on the Defense: Security That Can Keep Pace

Don't underestimate your defense—something many organizations already admit hasn't kept pace with the complexity of their IT environments. Here's where AI adds another layer of support.

AI- and AIOps-enabled workflows can help security teams recover faster, which can reduce costs incurred. Full backups and snapshots on autopilot keep accurate, up-to-date backups on standby. Once you kick into recovery mode, automated workflows can manage some of the time-consuming tasks associated with triage, investigation, and containment processes. High-speed forensic analysis can locate indicators of compromise so you can restore backups that are clean.

AI can also help fortify one of the weakest links in the defensive security chain: ineffective passwords. By automating the enforcement of better passwords and more frequent password updates—privately and securely—AI-powered password managers can reduce attacks at this often overlooked level.

AI and ChatGPT: Threat or Protector? (It's Complicated)

Part of a holistic security strategy is staying up on the latest trends—and ChatGPT has made waves. But how will this AI-powered technology disrupt the security landscape?

But, as it learns from its users, it's up to us to keep confidential data confidential.

While the extent of ChatGPT-based threats isn't yet fully understood, we know ChatGPT can be used by cyberattackers for various bad acts. Take phishing, as ChatGPT itself mentioned. ChatGPT can help cybercriminals quickly produce sophisticated phishing attacks by training the AI tool to write phishing emails and malicious code in seconds. ChatGPT can also easily emulate the writing tone and style of a public figure, a corporate executive, or a company representative.

As in the now famous case of infostealer, ChatGPT can also help cybercriminals looking to steal sensitive corporate data and software codes in ransomware attacks. Hackers could also use ChatGPT for advice on penetrating networks, bypassing certain types of security controls, or even writing malware.

But as the saying goes: "fight fire with fire." Don't cross your fingers that ChatGPT will be a passing trend; get familiar with its capabilities and share best practices with employees.

The 5 Key Characteristics of a Modern Data Protection Platform

We can summarize all of the above into five key things to look for in a modern data protection platform (AI plays a critical role in all of them):

- **Speed**—Meaning rapid detection of anomalies, restoration of data, instant recovery, having usable clones, and guaranteed shipping of clean arrays next business day.
- **Security**—Meaning immutability and instant recovery from all attacks, including ransomware and malware, while planning in advance using a data protection assessment and thoughtful recovery plan.
- **Simplicity**—Meaning automated, API-driven, integrated, intuitive, non-disruptive, and self-healing, along with an onsite engineer augmenting your staff to simplify operations when you need it the most.
- **Scalability**—Meaning efficient and targeted scale with a disaggregated architecture, and options for a scalable cloud experience.
- **Sustainability**—Meaning a reduced environmental footprint in power, cooling, and infrastructure, guaranteed as the cleanest STaaS technology on our planet.

Start at ground zero for data security—data storage—with the latest in AI and automation. This isn't just simple redundancy. It's next-level technology that marries AI to data storage to deliver always-on protection. It's something we've built into Pure data storage solutions. Pure1 Meta® is the AI-driven, full-stack analytics platform behind Pure's self-driving storage management system. Machine learning and the accumulated real-time data from a global fleet of arrays provide predictive analytics at scale. And with Meta, it's possible to forecast and troubleshoot data storage issues before they occur.

Pure's Evergreen//One™ offers all of the above and adds a new one to the list: an SLA for ransomware recovery that guarantees clean storage arrays shipped next business day, a recovery plan, and an 8 TiB/hour data transfer rate with bundled professional services onsite to speed up recovery. Learn more about how Pure's ransomware recovery SLA guarantees customers can get back up and running faster than ever.

According to the 2021 *ITDM Thought Leadership Research* report from Pure Storage and Bredin, 67% of IT decision makers said that data security and compliance are the biggest risks to building a digital business.

https://www.veritas.com/content/dam/Veritas/docs/ebook/V1117_GA_EB_2020-ransomware-resiliency-report_EN.pdf

https://www.securitymagazine.com/articles/91572-weak-passwords-caused-30-of-ransomware-infections-in-2019