Why Human-Centered AI is the Future of IT Security

PETER BRETTON
VP, PRODUCT STRATEGY

ninjaOne®

Introduction

On-prem, remote, and hybrid endpoints located across multiple offices, cities, and countries lead to complexity and expanded attack surfaces. Not only have attack surfaces expanded in size and scope, but networks are exposed to more threats than ever.

132 CVEs/day

33% rated High/Critical

According to cve.org there are an average of 132 CVEs a day, with 33% of those being rated “High” or “Critical.” Add to these numbers the fact that these CVEs are being created by increasingly sophisticated threat actors, and it becomes clear that traditional, reactive security approaches are no longer sufficient.

AI enables your IT Ops team to detect issues faster, respond more intelligently to alerts, and develop proactive defense strategies. Unfortunately, if AI is not also used to analyze these logs, alerts, and telemetry data gathered by the detection tool, then the speed and accuracy gained slows down while IT techs manually review and determine how best to act on the reports. Including AI-driven analysis in the cybersecurity tool ensures the potential threats discovered during detection can be quickly evaluated and prioritized for remediation.

Speeding threat response

Beyond detection, automated response mechanisms powered by AI can take predefined actions — such as isolating a compromised device, terminating malicious processes, or blocking suspicious network traffic — within seconds. This speed is critical in limiting the spread of ransomware and other fast-moving attacks. AI also helps prioritize alerts while distinguishing between false positives and genuine threats, allowing your security team to focus their efforts on the true threats while setting the false positives aside for later review if needed.

Continuous learning improves threat detection

Another key advantage of AI is its ability to learn and adapt. Unlike static, rule-based systems, AI models continuously improve as they're exposed to and assimilate new data. This adaptability is essential in a threat landscape where attackers constantly change their tactics. For example, AI can detect previously unseen malware variants by identifying behavioral similarities rather than relying solely on known signatures.

This shift from signature-based to behavior-based detection represents a major advancement in cybersecurity effectiveness. For example, when a vulnerability is exploited for the first time, no signature exists yet. But behavior-based AI can catch a zero-day attack by recognizing that an application is doing something it has never done before, such as a PDF reader attempting to access system credentials or initiate a network connection. Another example is polymorphic malware which is designed to constantly rewrite its own code to avoid signature detection. When an AI security tool is trained on behavioral patterns it can identify the malware regardless of how the code is packaged, because the underlying actions — data exfiltration, privilege escalation, lateral movement — remain consistent.

How threat actors are using AI

AI's ability to learn and adapt isn't a capability exclusive to defenders. Threat actors are leveraging the same technology to stay one step ahead. They're increasingly using AI to automate phishing campaigns, generate convincing deepfakes, and identify vulnerabilities at scale. AI-generated phishing emails, for instance, can be highly personalized and grammatically accurate, making them harder for unsuspecting users to detect. They'll also use AI techniques to evade detection by subtly manipulating inputs. These practices reinforce the need for robust, AI-powered defenses that can keep pace with AI-driven threats.

NinjaOne human-centered AI is helping strengthen cybersecurity

At NinjaOne, we believe the future of AI lies in how it empowers humans, not replaces them. Our approach is built on accountability, transparency, and trust for our customers. The Unified NinjaOne IT Operations Platform enhances technician expertise, supports learning, and delivers automation that's always testable, traceable, and under your control. You determine the level of autonomy that's right for your organization, and NinjaOne human-centered AI works within those boundaries.

That philosophy shapes the AI features within our platform, starting with how we approach endpoint visibility and risk identification. By embedding AI into endpoint monitoring and management workflows, NinjaOne gives your team deeper insight into your IT environment while reducing the manual effort required to act on it.

By analyzing historical endpoint data, NinjaOne can identify patterns that suggest potential failures or vulnerabilities before they are exploited. For example, unusual system behavior, outdated software, or misconfigurations can be flagged proactively, allowing your IT team to address them before they become security incidents. This proactive approach shifts cybersecurity from a reactive defense activity to continuous risk management.

Autonomous Patch Management and Patch Intelligence AI

Nowhere is this proactive shift more tangible than in our Patch Management solution. Keeping systems up to date is one of the most effective ways to reduce risk, yet it remains a challenge for many organizations. NinjaOne Autonomous Patch Management with Patch Intelligence AI uses AI-powered insights to prioritize patching based on risk level, exploit likelihood, and system criticality. It also automatically pauses bad or risky patches without the need for IT intervention. This ensures that the most important vulnerabilities are addressed first, bad patches are paused, and your organization's overall security posture is strengthened without overwhelming your IT team.

Together, proactive risk identification and autonomous patch management close the loop between finding a vulnerability and fixing it. Your team stays in control of the decisions that matter, while NinjaOne handles the scale, speed, and consistency that no manual process can match.

Looking ahead

Despite the advantages, it's important to remember that AI is not the answer to every cybersecurity challenge. Effective cybersecurity requires a layered approach that includes strong policies, user education, and human expertise. AI should be viewed as a tool to supplement the capabilities of your security teams rather than a tool to replace them. It's important to ensure that your AI systems are transparent, well-governed, and regularly updated to prevent misuse or bias.

Looking ahead, the role of AI in cybersecurity will only continue to grow. As threats become more sophisticated, the ability to detect, analyze, and respond in real time must adapt as well. The Unified NinjaOne IT Operations Platform combines intelligent automation with robust endpoint management, integrating human-centered AI into everyday IT operations. The result is stronger security, improved efficiency, and empowered IT teams and end users.

Learn more about the NinjaOne Unified IT Operations Platform at www.ninjaone.com/platform

ninjaOne®