Business Software Alliance

Smarter Shields: How AI Is Improving Cybersecurity Today

How Leading B2B Software Companies Are Using AI to Improve Security

Artificial Intelligence (AI) has become a critical tool in a security team's tool belt. It helps predict and remediate vulnerabilities, expedite threat detection, and automate incident response. AI for cybersecurity is delivering value for businesses today.

The Challenging Environment

As the world has gone digital, the importance of cybersecurity has grown. Simultaneously, malicious actors have improved their tactics, techniques, and procedures, including by leveraging AI for the malign purposes, in attempts to increase the frequency and impact of their illegal activity. Yet AI is helping to turn the tide in favor of defenders, giving them tools that can make them more effective against malicious actors. These AI-enhanced tools are not science fiction or even currently in the research departments of leading B2B software companies. Rather, they are being deployed today to meet malicious actors and secure businesses' information.

AI for Cybersecurity: Deployed Today

Policymakers should take note that leading B2B software companies are already deploying AI-enhanced cybersecurity tools and as they consider ways to manage high-risk AI, if those efforts unintentionally slow the adoption of AI for cybersecurity, they will unintentionally degrade security.

cisco

AI-Enhanced Phishing Defense

A financial institution was experiencing a surge in sophisticated phishing attempts targeting its employees, potentially exposing sensitive customer data and financial systems to risk. By deploying Cisco XDR, which leverages agentic AI to verify threats and execute tailored investigation plans, while AI-driven prioritization helps boost the effectiveness of security operations teams, the institution received integrated security across the network, endpoints, email, and cloud environments, enabling comprehensive visibility and automated response capabilities. This implementation improved the security posture against phishing and other cyber threats and helped to streamline compliance processes, positioning the bank at the forefront of financial cybersecurity.

elastic

Open-Source, AI-Driven Security

A US state agency faced an unprecedented surge in cyber threats and data volume during the pandemic, overwhelming its legacy on-premises information technology and putting public funds at risk. By migrating to Elastic Security, the agency consolidated its security

operations into a single view in the cloud, leveraging Elastic's security and AI capabilities to detect fraudulent account takeovers by analyzing unusual login activities in real-time. This migration enhanced the agency's visibility into fraud schemes, reduced incident response times, and safeguarded $50 million taxpayer dollars.

IBM

AI-Enhanced Vulnerability Management

An e-commerce company struggled with identifying and prioritizing vulnerabilities across its expansive digital infrastructure. By adopting IBM's AI-based security solutions, the company employed machine learning to continuously scan for vulnerabilities and assess their potential impact to its business. This enabled the security team to focus on remediating the most critical issues promptly, thereby reducing the risk of exploitation and enhancing overall system resilience.

Microsoft

AI Agents for Security Teams

A health care provider faced challenges in managing the volume and complexity of security incidents, leading to delayed responses and increased risk. By integrating Microsoft's Security Copilot—which leverages Security Copilot Agents for activities like threat protection, device management, and threat intelligence—the health care provider's security team received real-time guidance and automated analysis during incidents. This streamlined its response processes, reduced resolution times, and improved its ability to protect sensitive patient data.

okta

AI-Empowered, Risk-Based Multi-Factor Authentication (MFA)

A SaaS company faced challenges with managing access to information systems, while not reducing productivity. By implementing Okta's adaptive MFA, the company could adjust authentication requirements based on risk; for low-risk logins indicated by typical user behavior, the user may utilize simple authentication while for high-risk attempts, Okta protected the company by requiring extra steps like biometric verification or one-time passcodes. AI-enabled adaptive authentication helped the company manage risk, without additional products or unnecessarily cumbersome steps.

paloalto NETWORKS

AI-Driven Security Operations Centers (SOCs)

A US state was supporting 34 agencies and 35,000 users to detect and prevent incidents on the state's 300,000 endpoints. By leveraging Palo Alto Networks' AI-enhanced SOC, the state reduced its mean time to resolve from more than 24 hours to less than two minutes and resolved 86 percent of incidents automatically. This proactive approach enabled the state to refocus security staff from the administrative tasks to higher-level work like threat hunting and incident response.

SAP

AI-Driven Data Privacy Integration Anonymization

A customer in the manufacturing sector needed to conduct sensitive internal personnel audits. By using SAP's AI-enabled Data Privacy Integration (DPI) Anonymization Service the customer could generate pseudonyms to complete those audits but subsequently link the audit information to actual individuals. This AI-driven service enabled the customer to ensure the security and privacy of the audits.

servicenow

AI-Supported Security Operations

A Fortune 500 SaaS company faced a challenging cyber threat environment. By leveraging over 20 ServiceNow AI agents to help support a wide range of security operations and tasks, including triage, investigations, and drafting of audit-ready post-incident reports, it achieved significant productivity gains by allowing analysts to complete work in a fraction of the time, thereby accelerating defensive actions. The combination of integration, automation, and AI streamlined operations, helping strengthen the company's security posture through faster, more effective detection and response solutions.

Moving Forward

These use cases demonstrate that applying AI in cybersecurity is not theoretical but securing businesses today. By investing in AI-enhanced cybersecurity solutions, businesses and government agencies can effectively manage their cybersecurity risks and better deliver for their citizens and customers.