Data Story

The power of AI: Security

Now more than ever, time is the currency of cybersecurity. We can't make more time, but we can make much better use of the time and resources we have. To thwart the around-the-clock threat of cyber attackers, we need more people, more capacity, and more proactive capabilities. The challenge: how do we do all that in an era of stretched budgets and hard-to-find talent?

Today's hybrid cloud environment consists of many players, each contributing to security outcomes. What sets cloud security leaders apart is how they bring together talent, technology, and partners to manage their potential attack surface. The secret is how they make economies of scale work for them, not against them.

Cloud security leaders understand that effective defense happens before a threat materializes—through planning, prevention, and proactive decision-making. These leaders enhance their cyber risk posture to prevent attacks, streamline security operations, and work with partners to extend capabilities and resources.

43%
of organizations are outsourcing their security program governance and operations to partners.[2]

40%
higher Return on Security Investment (ROSI) for organizations with the most mature security AI and automation capabilities.[2]

$3.05m
average reduction in data breach costs for organizations with fully deployed security AI and automation – by far the leading factor in reducing the overall costs of a data breach.[3]

A growing body of research indicates that organizations deploying security AI and automation capabilities are realizing transformative operational gains. Through these force-multiplying technologies, companies can detect and respond to cyber incidents with greater speed, which can significantly reduce the frequency, cost, and impact of security incidents.

New technologies like generative AI are changing the playing field—both for cyber defenders and threat actors. As our reliance on connected services grows, ecosystems are evolving. Instead of being sources of vulnerability, suppliers and partners can become allies in fostering greater cyber resilience. Whoever can establish trust faster and more efficiently enjoys an operational advantage.

66%
of operations executives regard cybersecurity as a revenue enabler.[1]

43%
higher revenue growth over the past five years for organizations with the most mature security capabilities, as compared with their least mature peers.[1]

81%
of executives view security, assurance, and trust as brand attributes that differentiate their organizations.[4]

Actions to achieve

1. Re-envision security around shared responsibility and shared outcomes.
2. Adopt a unified strategy that modernizes security operations in line with cloud investments.
3. Leverage security AI and automation to drive scale, speed and efficiency across the security lifecycle, using technology to make the most of high-value talent.

Security AI delivers faster incident detection and response.

"It's an AI and automation arms race between cyber defenders and threat actors. They're using new technologies like generative AI to modernize their tactics and techniques and to adjust procedures in real-time. We need security AI and automation solutions to help us stay a step ahead."

Chief Information Security Officer
Consumer goods company

Security AI and automation capabilities are changing our approach to security operations. When we embed security capabilities at the design stage, we make security controls automatic. Security becomes more a source of assurance and less a source of friction. Operating at higher levels of confidence opens the door to new efficiencies and new enterprise and ecosystem-level value propositions.

Instead of cyber talent being in short supply, we can use the combination of security AI and automation to support high-value talent. The secret to raising our operational capacity is making more of the cyber expertise and judgement we already have.

150 days
It takes an average of 150 days, or nearly 5 months, to fill a cyber talent vacancy with a qualified candidate.[5]

99 days
If an organization takes 230 calendar days to detect, respond to and recover from cyber incidents, it can cut that time by up to 99 days (over 14 weeks) with security AI and automation.[2]

60%
of security AI adopters report that automated data enrichment and second-screen capabilities help analysts operate more efficiently.[2]

Actions to exceed

1. Use AI and automation to redefine the security value proposition around performance, resilience, and competitive advantage.
2. Focus on business resilience by embedding security holistically across enterprises and ecosystems.
3. Think of security as a community and use this to foster trust across the ecosystem.

"With a global shortage of over 3 million cybersecurity workers, businesses and governments must step up efforts to automate their cybersecurity operations. The combination of automation and AI frees up staff to focus on threats that require specialized expertise or judgement. These solutions are a smart way to address the cyber talent crunch."

Chief Human Resources Officer, Government agency

Interested in more insights and discussions on this topic?

Check out:

Cost of a Data Breach Report

AI and automation for cybersecurity

To learn more about the power of AI, click here

Subscribe now to receive research-driven insights to help you make smarter business decisions.

IBM Institute for Business Value

1. Prosper in the cyber economy. 2. AI and automation for cybersecurity. 3. IBM cost of a data breach (2022). 4. The new era of cloud security. 5. Getting started with zero trust security.
BYLG6LWR-USEN-00