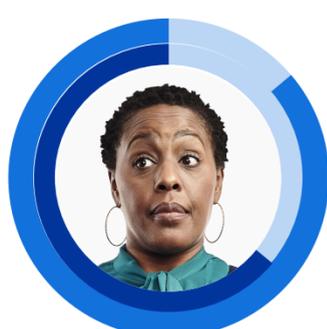


The Impact of Human Nature on Security Posture and the Need to Adapt

The volume, frequency, and sophistication of security threats are escalating. It's critical to adopt solutions that address the unchanging nature of human behavior, while enabling users to get work done.

ALL THE TRAINING IN THE WORLD won't safeguard against mistakes or well-intentioned workarounds



95% have a formal, documented security policy that is shared with employees

72% conduct security awareness training **more than once** per year

SIMPLY TIGHTENING SECURITY CONTROLS ISN'T THE ANSWER

92% stated increased security has noticeably impacted productivity

58% prioritize strict security controls over ease of use and convenience

Too-strict static security tools and solutions contribute to well-intentioned employees seeking workarounds

THERE REMAINS A PERSISTENT NEED TO CONSTANTLY RESOLVE EMPLOYEE MISTAKES



95% IT professionals are not confident in the ability of employees to adequately safeguard data

falling victim to phishing and social engineering attacks, sharing files using publicly available sites, employing weak passwords, using unapproved software, devices, or insecure Wi-Fi connections

Consequences persist despite training and formal security policies

Lost productivity, exposure of sensitive data, reputational damage, breach of contract, penalties and fines, loss of revenue

91% ...and it is needlessly interfering with IT tasks

resolving issues from "shadow IT", workarounds and employee mistakes is interfering with IT tasks

COMPANIES POINT TO WEAKNESSES IN THEIR SECURITY POSTURE

Confidence in status quo is low



34% Strongly confident their current endpoint security solutions effective in preventing malware threats

18% Strongly agree their current security policies dynamically adapt to keep pace with fast-changing risks

70% It's only a matter of time before the window of vulnerability has a negative effect on their business continuity

68% Relying on humans to push security policies down to devices has proven inadequate

And yet...

68% still have rigid static policies

IT'S TIME FOR SMARTER SECURITY

It's no wonder **Adaptive Security and Predictive AI** are emerging as a means to dynamically keep pace with the fast-changing situational risks experienced by users

99% have shown interest

- 42%** currently evaluating
- 36%** have implemented to-date
- 16%** plan on implementing within next 6 months
- 10%** plan implementation in 12 months or more
- 1%** have no interest

High Interest Driven By

- 57%** potential for better protection of sensitive data
- 52%** improved employee productivity and satisfaction
- 48%** improved customer confidence
- 47%** the ability to reallocate staff to other higher value projects

MOST IMPORTANT WHEN EVALUATING ENDPOINT SOLUTIONS

Productivity

74% Flexibility to enable productivity while also increasing security

68% Secure access to apps from enterprise accessible device

Smarter Security

72% Security policies that dynamically adapt to risk by users

68% AI powered mobile threat detection

67% Continuous Authentication

IS YOUR SECURITY HUMAN NATURE-PROOF?

Adaptive Endpoint Security

Instead of applying inflexible static policies, machine learning and predictive AI dynamically adapt security policy to keep pace with fast-changing risk.

BlackBerry® Persona

- Instantly knows when to shut down lost, cloned or impersonated devices.
- Proactively quarantines devices and apps before they can be used for malicious purposes.
- Enables streamlined access to apps and services without having to re-authenticate when in trusted locations.

Mobile Threat Detection

Get in front of malicious cyber attacks with AI-driven security that prevents attacks before they can damage your devices, network, or reputation.

BlackBerry® PROTECT

- Protects mobile endpoints against malware and phishing attacks
- Prevents common and unknown threats without a cloud connection
- Safeguards against script-based, fileless, memory and external device-based attacks