Solving the security/efficiency stalemate with context-aware security

While end-users and IT professionals agree in general on the philosophy of organizational security, they see its enforcement very differently. End users see it as an inconvenient barrier to productivity. IT professionals see it as a necessity to protect the organization's data and intellectual property. Context-aware security offers a way to please both groups.

Q What is context-aware security?

A Context-aware security is an adaptive security process that evaluates requests in real time, determines a risk score and grants or denies access based on this score. It allows you to implement security across multiple applications and processes with minimal IT intervention.

Factors affecting security

Location- telecommuting and remote access

- **93%** of business users rely on cloud applications for their work
- **82%** of remote workers say they are required to use additional security measures when accessing corporate assets remotely
- **47%** of IT pros say non-standard access at their organization requires their intervention

Origin of access request BYOD

- **65%** of businesses allow employees to use their personal mobile devices for work
- **46%** of enterprise employees actually use their personal mobile device for work
- **95%** of mobile users access corporate assets on their own device, with **83%** doing so daily

User Identity/role

3 out of 5 employees think they're not responsible for protecting corporate IP.

Target of access request

- On-premises
- Company-owned apps
- 3rd party owned data
- SaaS
- 3rd party access

58% of enterprise end users have to remember as many as 5 passwords to access multiple work applications. **11%** have more than 10 enterprise-issued passwords!

Determining your risk score

Global survey recap

What **end users** say

- **85%** have multiple login password combinations
- **92%** are negatively impacted by their organization's remote-access policies
- **87%** feel security standards take precedence over employee convenience
- **91%** said productivity is negatively impacted by employer security measures

What **IT professionals** say

- **97%** see the benefits of context-aware security
- **71%** have not fully embraced a context-aware security approach
- **93%** said a lack of context-aware security causes challenges
- **60%** say lack of awareness is the greatest barrier to delivering context-aware security

Organizations see the benefits of context-aware security practices and the value in having the ability to prioritize threats based on context. Context-aware security gives IT the power to adjust the security level in real time, so users have the convenience they need to get their work done without having to resort to risky workarounds and the confidence that the organization is secure.

Compare your perceptions to your peers. Read the in-depth Global Survey results.

Learn More