Solving the security/efficiency stalemate with context-aware security

What is context-aware security?

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 work - 93% of businesses rely on cloud computing to do their work.
- 82% of enterprises access data they are responsible for in unsecure/off-network locations when accessing corporate assets remotely.
- By 2022, 47% of all cyberattacks will be targeted at access control Fail-Silence.

Origin of access request

- BYOD - 65% of businesses now empower employees to use BYOD solutions to access the web.
- 46% of enterprise employees actually use their personal mobile devices to access corporate assets in the past 12 months, with 49% expected to do so.

User Identity

- 3 out of 5 users do not follow policies for preserving corporate assets.

Target of access request

- Commonly accessed by
  - Cloud applications
  - VDI
  - SaaS
  - Multi-factor authentication

Determining your risk score

- Security analytics engine
- Policy
- Enforcement
- Thresholds

Global survey recap

What end users say

- 85% of end users rely on employee-generated data.
- 92% of end users say cyberattacks are routine.
- 87% of end users say they have personally experienced a cyberattack.
- 91% of end users say their organizations have been targeted by cyberattacks.

What IT professionals say

- 97% of IT professionals say cyberattacks are routine.
- 71% of IT professionals say their organizations have been targeted by cyberattacks.
- 93% of IT professionals say their organizations are better prepared to handle cyberattacks.
- 60% of IT professionals say their organizations are ready to handle a major cyberattack.

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

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

Learn More