FLEXENTIAL®

Remote work security assessment

Reduce the Security and Business Risks of a Remote Workforce

The new world of remote work has created both increased security vulnerabilities and increased threats from bad actors. According to William Altman, senior analyst at the Global Cyber Center of NYC, "Organizations of all kinds are facing an uptick in email-based threats, endpoint-security gaps, and other problems as a result of the sudden switch to a fully remote workforce."

Organizations had not planned to move their office workforces to remote working, and IT departments were unprepared for transitioning a workforce while still ensuring security and compliance. Nevertheless, IT teams had to enable nearly all their office staff to work remotely, sometimes with only a few days' notice and little to no planning time. As a result, this quick shift happened in emergency mode.

Under pressure to keep organizations functioning, many made operational compromises. Hard decisions were faced, and security measures were relaxed to enable employees to work remotely. Simultaneously, bad actors have dramatically increased activity.

The new security risk

This unexpected and unplanned shift to remote work has resulted in a dangerous perfect storm of security risk:

- A larger security perimeter and increased threat surface to monitor and protect
- Substantial increases in bad actor activity, such as phishing and ransomware
- More demands on IT to support and enable a remote workforce

Security teams are now challenged to reduce risks and adapt security measures to avoid social media and chatbot threats, and breaches from phishing, whaling, and ransomware. Increased remote work exacerbates threats from inadequate laptop security, personal devices use, remote access methods, and home networks.

"Working from home is going to be a long-lasting reality within many organizations, and the security assumptions we once relied on in our traditional offices may not be enough as our workforce transitions to new, less controlled surroundings. Organizations need to use a risk-based approach with work-from-home models, then reassess and build from the ground up."

—Charles Henderson
Global Managing Partner &
Head of IBM's X-Force Red

A risk-based action plan

IT organizations need to understand the current vulnerabilities in their distributed workforce and execute a risk-based approach to protect their organizations. The Flexential Remote Work Security Assessment evaluates and provides organization-specific security recommendations for meeting compliance and regulatory requirements, closing gaps and reducing risks in:

- Remote access methods
- User authentication methods
- Endpoint protection
- Encryption methods
- Business-critical systems security
- Incident response plans

The remote work security assessment provides a roadmap to strengthen security and reduce the risk of breaches and data loss, as well as the resulting recovery and remediation costs, PR damage, lost business and lost customers.

Customers receive a detailed risk-based report which includes:

- Organization-specific IT security recommendations for a remote workforce
- Recommendations prioritized by criticality, cost to implement, and time to implement
- Guidance for security controls
- Technical details for system administrators to use as a risk mitigation guide

Organizations have entered an age of distributed work and, at least temporarily, a remote-first workforce strategy. IT security needs to match this new reality.

Features

- Highly certified security experts
- Stakeholder interviews and technical reviews
- Review of compliance and regulatory requirements
- Assessment of critical vulnerability areas
- Risk-based security recommendations
- Prioritized action plan with remediation guidance
- Professional project management

Benefits

- Documented remote workforce security plan
- Risk-based action prioritization
- Remedies for risks from the shift to remote work
- Addresses compliance and regulatory security