MICRO FOCUS Government Solutions

## Remote Access and the Coronavirus

# Thinking Outside of the Box… and the Building

## Power. Protection. Partnerships.

## These are the advantages of Micro Focus Government Solutions. We are helping governments help people during this global pandemic.

Federal, state, and local governments as well as defense agencies trust our Secure Remote Access Management Solution to help you protect what matters most and to collaborate across your ecosystems with reduced risk.

The COVID-19 crisis continues to test us all, forcing us outside of our normal patterns and comfort zones. It's placing a strain on the various IT systems, applications, and processes we use on a daily basis. The dramatic increase in demand for telework and remote access is exceeding the boundaries of existing IT plans and security systems—going well beyond our capacity and too often straying outside of enterprise security policies.

Micro Focus believes traditional, single-factor authentication, including username and password, is no longer a sufficient approach to protecting corporate, employee, or client information. Micro Focus gives you the freedom to incorporate whatever authentication type that works for your business.

With sixty to eighty percent of the population now working from home, existing security strategies need to be re-examined. Since remote access infrastructure and citizen/user applications are the most frequently attacked systems by hackers, the need to quickly add capacity while complying with existing security policies is critical. We must step back, brainstorm better ideas, and think not just outside of the box, but also outside of the building.

## Thinking Outside of the Box or the Building

Society is evolving towards a mobile lifestyle, where people don't need to be in the office in order to work or at the store to shop. Industry analyst IDC claims that 1.3 billion workers are now mobile and connected. That's one third of today's workforce working outside of the building.

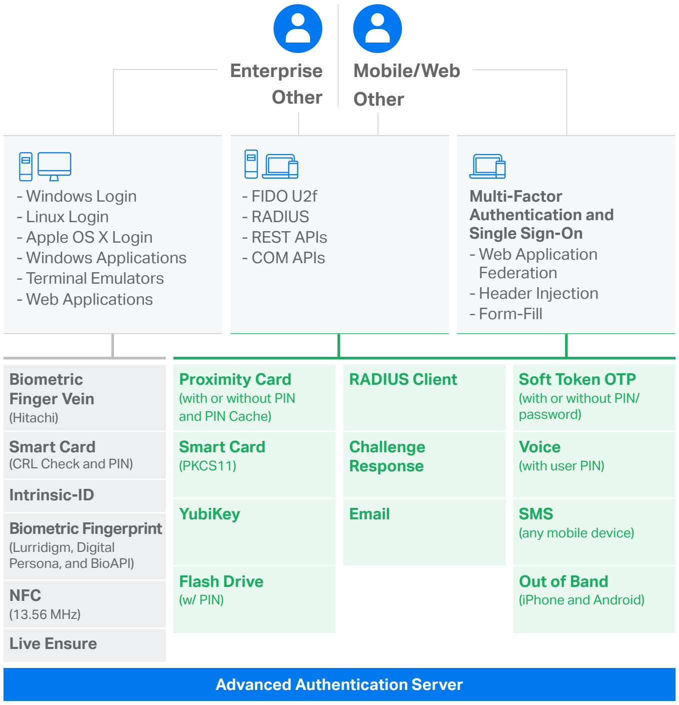
This creates a new normal where users and their devices are continuously connected to your network. These connections are constantly under increasingly sophisticated attacks. Traditional single-factor authentication of username and password is no longer sufficient to protect agencies, departments, employees, or citizens. You need to evolve to multi-factor authentication (MFA).

## Choosing the Right Solution

Micro Focus Advanced Authentication provides both choice and flexibility for your current and future MFA requirements. It doesn't lock you into a single authentication method or leave you stuck using outdated technology. Instead, it offers an open framework that aggressively updates as new authentication technologies and methods emerge, such as compatibility with FIDO U2F-based devices.

In addition, the Micro Focus Advanced Authentication framework delivers out-of-the-box integration with Access Manager, our market-leading access management and single sign-on solution. Access Manager provides a single platform for unified access management and advanced user and entity behavior analytics (UEBA). Of course, our Advanced Authentication framework also integrates with other single sign-on solutions.

For more information, please visit our NetIQ Advanced Authentication and NetIQ Access Manager web pages.



If done right, combining two or more authentication methods makes it exponentially more difficult for the bad guys to circumvent access policies, reducing the risk to the organization.

The National Institute of Standards and Technolgy (NIST) issued additional publications providing concrete guidance for these Federal Information Security Management Act (FISMA) mandates.

## NetIQ Access Manager

Deliver simple, secure, scalable web access to internal and external resources, with standards-based federation and support for advanced authentication.

Learn more ›

NIST SP 800-46, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security recommends that organizations consider the "balance between the benefits of providing remote access to additional resources and the potential impact of a compromize of those resources." To mitigate the risks associated with providing remote access, NIST recommends hardening resources against external threats and limiting access to the "minimum necessary."

Visit our COVID-19 website ›