MICRO FOCUS

Flash Point Paper

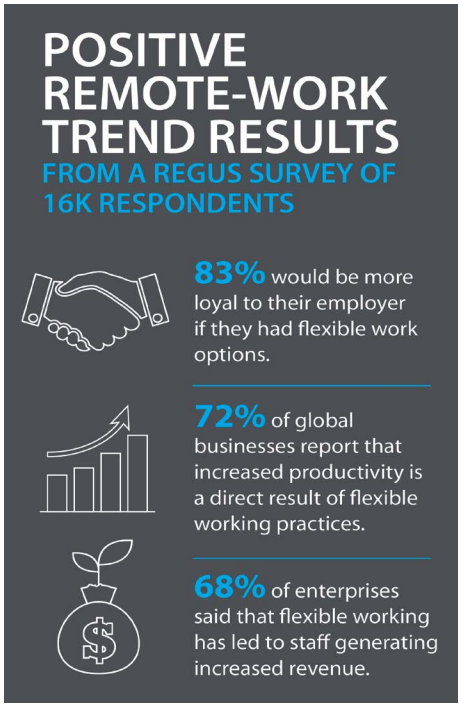
Security

Securing Today's Remote Access

Thinking Outside of the Box—or the Building

The necessity of business owners delivering remote access to business users continues to rise at a notable rate. Working away from the office is no longer just for road warriors or the occasional off-hour employees that use their personal devices to occasionally conduct some business. Working remotely is part of the new way that business gets done, from wherever you're sitting. Remote access needs now span across the organization. But making that access secure has the potential of being cost prohibitive if yesterday's security models aren't brought up to date.

The question is how far will this trend extend and how responsive will IT need to be in enabling it? One survey[1] of human resources professionals indicated that over a fourth of them had at least some employees working remotely. That statistic more than doubled for multinational organizations to 2 out of 3 employees working remotely. Of course, percentages vary depending on industry.



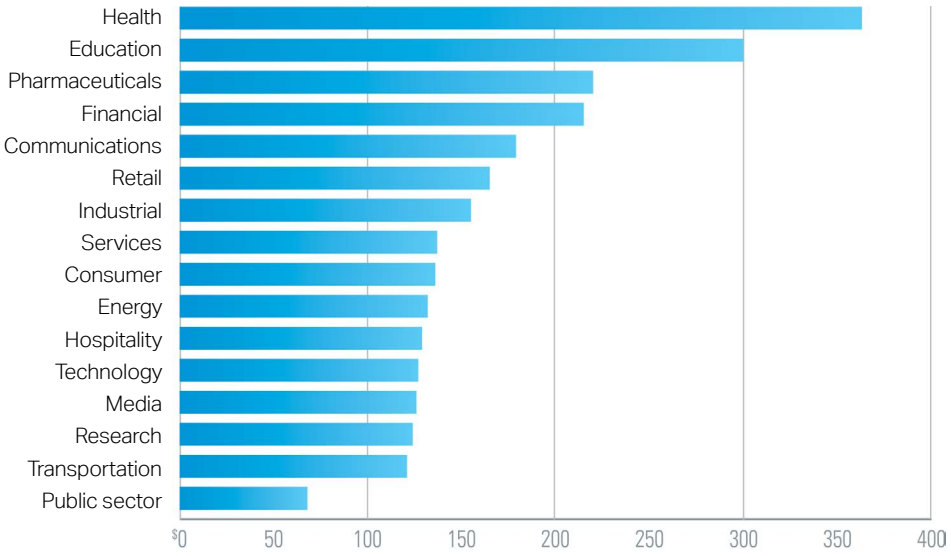
Source: **www.regus.com**

Critical Success Factors for Making Remote Workers Productive:

- *The right combination of people and facilities and technology*
- *The right communication equipment, training and support*
- *Technological connectivity: plug and play, data sharing, network access, virtual meeting and wireless capabilities*
- *Maximize online capabilities*
- *Measure performance*

1 **www.regus.com/images/Flexibility%20Drives%20Productivity_tcm8-49367.pdf**

The average cost of data breach is $217 in the U.S.



Source: 2015 Ponemon Breach Study

The Risks of Working Outside the Box

It seems that every week a headline points out that another organization has disclosed (or admitted to) a large data breach. The corporate-named victim in the headlines is often a broadly recognized one and clearly spans across all industries.

For a decade, the Ponemon Institute has conducted annual surveys tracking the cost of these cyber-attacks, which continues to rise. The total costs of a breach have gone up 23 percent in the last two years. And worldwide the average cost of a stolen record is now at $154, a notable portion of which is due to loss of customers (and in many cases, patients). That's real money—money that was coming in the door. In terms of planning actionable remedies, it's important to note that stolen credentials enable 8 out of 10 data breaches. So when an organization examines how they're going to update their access control to enable and empower their remote and mobile workforce, the risks posed by stolen credentials can't be ignored.

And in case small business managers think they're immune from this type of risk, last year 1 out of 3 breaches were with small to medium businesses (SMBs). The reality is that while criminals understand that the payoff from stealing information from SMBs is significantly smaller than a large enterprise, the barrier to obtaining valuable digital information is usually much lower, often gaining unauthorized access through social engineering. And as it has been demonstrated again and again, the payoff is well worth the criminal's time.

---

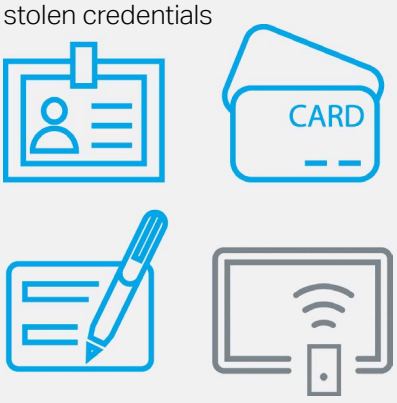
2 *The Global State of Information Security Survey 2015, by PwC, CIO and CSO:* **www.pwc.com/gsiss2015**

3 *US cybercrime: Rising risks, reduced readiness, by PwC* **www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf**

7 out of **10**
security attacks
target small businesses

Source: Global Security Report by Trustwave

3 out of **4**
breaches are through
stolen credentials



Source:Verizon DBIR study

Reasons why corporations are growing their remote workforce:

- Reduced costs in real estate and office space
- Job sharing–people sharing a job, and space
- Flexible schedules, based on needs rather than regimented work times.

Source: from research and work done by Sandy Burud, PhD at **flexpaths.com**

1 of 4 organizations in North America have at least some of their employees work remotely

The Rewards of Working Outside the Box

If IT and security teams decide that clamping down on remote access is the way to go, they need to keep in mind the ultimate objective: to empower the business teams to be as productive as possible. So security must be intertwined in the strategy, productivity and flexibility is what keeps businesses and other organizations thriving. One of the key components is to ensure that professionals are able to access the information and services they need regardless of where they are located or what device they are using. So, if security is an afterthought, sooner or later the business will lose. But hampering business productivity isn't the way to win either.

Although virtual private networks (VPNs) continue to be the most popular solution for providing secure access to remote users, other remote access technologies are proving to be even more effective. These technologies include virtualization solutions that remotely deliver applications, specialized services, or full desktop views and require only modest network bandwidth and client processing power. They also keep private information off remote devices while keeping access to it convenient. As the business leverages these remote technologies and as professionals interact with them, the expectations continue to mount. The right answer isn't to be the department of "no," but rather to be the expert of "how."

Professionals Would Just as Soon Not Be in a Box

Regardless of whether you're using a traditional VPN for your remote access needs or some type of virtualized technology, it's critical to protect that access. And since 8 out of 10 breaches involve stolen credentials, verifying the user's identity is fundamental to security. One of the most effective approaches to verifying someone's identity is to invoke two-factor authentication. In other words, to invoke another type of authentication once someone enters their credentials, which could be stolen. It requires users to provide something they have, such as a code from a device, or

Micro Focus gives you the freedom to incorporate whatever authentication type that works best for your business.

Contact us at:
www.microfocus.com

Like what you read? Share it.

something they are: their finger, face, voice, and so on. When done properly, providing a step-up in the authentication process has proven most effective in keeping outsiders out.

If you're part of an organization that still relies on hard tokens for two-factor authentication, you're probably paying too much for license fees and administration overhead. And as you continue to expand who gets secure remote access, sooner or later it's going to be clear that the old way of authenticating VPN users doesn't scale: neither financially nor in the hours required for administration. Micro Focus® has a lot to offer in both areas.

If you currently allow VPN or other types of remote access technology to access sensitive information with nothing more than user credentials, you're playing with fire. And if you have noticed the headlines of late, sooner or later you're going to pay for your security shortcut. But Micro Focus can help. With its open architecture and straightforward user licensing, the NetIQ® Advanced Authentication Framework is the way to get started.

To learn more about Advanced Authentication Framework visit **www.microfocus.com/en-us/products/netiq-advanced-authentication**.