A Frost & Sullivan Executive Brief

Identity Crisis: Why the Modern Work Environment Needs Advanced Digital and Physical Security for User Authentication

Powering clients to a future shaped by growth

FROST & SULLIVAN

The number of remote workers has been on the rise since the dawn of telecommuting in the 1970s. The internet, Wi-Fi, and the smartphone have made it easy for frequent business travelers, employees living far from their places of employment, and part-time workers to connect to the office from anywhere and at any time. The COVID-19 pandemic and resulting workplace closures, however, propelled work from home (WFH) from an interesting trend to standard practice for millions and millions of employees in a matter of weeks.

Since the onset of the WFH measures, many businesses have been adjusting to the situation and even finding advantages, such as lower real estate costs and more availability from employees. About 77% of companies have stated they will continue to allow WFH even after any restrictions are lifted, and a survey from IBM in mid-2020 reported that over 60% of employees would like to remain as remote workers. Companies across industries are working to adapt to these trends. Notable tech giants such as Twitter and Facebook are enabling WFH for half or more of their workforces. International technology and manufacturing conglomerate Hitachi has stated that as much as 70% of its 300,000 global employees may be working remote permanently. Google has stated, as of the time of this paper (mid-2020), that its 200,000 employees could work from home through mid-2021. Amazon, Salesforce, Microsoft, Dell and many others have followed suit, extending work from home through at least 2020, if not permanently. Even industries where face-to-face interaction was commonplace, such as education, healthcare, and banking, have had to adjust. JP Morgan Chase has approximately 200,000 employees working from home, and Bank of America had to purchase over 90,000 laptops for its WFH transition, though, as of the time of this paper, had not stated for how many employees the move would be permanent. As things remain fluid, and certain WFH benefits are coming to light, it seems likely that despite being initially disruptive, this is a trend that will persist.

CHALLENGES OF THE NEW MODERN WORKPLACE

The challenges of having a large portion of a business's employees work remotely cannot be underestimated. First and foremost is the issue of user identification and authentication, and its impact on a company's overall cybersecurity risks. Network and even physical security are related concerns in these less-controlled environments.

Addressing Cyber Challenges for the New Normal

SECURITY CHALLENGES HAVE INCREASED:

- Endpoints are the main entry point for threat actors
- Boom in IoT devices makes them hard to
- manage and secure
- Employees using personal devices add vulnerabilities
- Cybercrime is on the rise

- Insider threat—both inadvertent and malicious—is prevalent
- Work-from-home environments vary by user and are hardest to secure
- Data breaches can impact productivity, brand image, stock value and regulatory compliance
- In-house measures to increase security can complicate user experience and reduce IT team efficiency

WHAT TO LOOK FOR IN A SOLUTION:

- **Endpoint-based technologies** will have the greatest breadth of security coverage
- **Flexible solutions** that adapt across different work environments and regions, and can evolve with the business
- **Comprehensive solutions** fully protect the user, company and data with a combination of intelligence—like sophisticated AI—and physical security—such as biometric-based multispectral imaging
- **Efficient solutions** are easy to install and roll out by the IT team and to access and operate by the user

The vast majority of threat actors gain entry through endpoints. Frost & Sullivan research attributed this to the rapid increase in the use of personal electronics as well as the boom in Internet of Things devices, which are expected to grow from approximately 27 billion in 2020 to more than 58 billion by 2025.[1] Endpoint management is critical for advanced cybersecurity.

While not all businesses have an assembly line or a fleet of connected vehicles, virtually all rely on laptops, smartphones, and other data and communication devices. Employees often use corporate-issued or BYOD devices for non-work applications such as accessing social media or third-party email, or connecting with home security or entertainment systems. They may have less-secure Wi-Fi connections than they would in the office setting—a concern that has grown exponentially in the new WFH environment.

> **"Unless well protected, any of these situations can make company applications on these devices vulnerable to man-in-the-middle attacks, phishing through third-party email or social media sites, or other threats. Strong, endpoint-based security technologies and practices thwart many cyber threats.**

Cybercrime is surging. Cybercrimes have jumped significantly in 2020. As early as April, the World Health Organization was reporting a five-fold increase in global cybercrime in the first quarter of 2020, and the FBI reported a 300% increase in monthly reports of attacks in the United States; by June, the number of attacks for 2020 had already eclipsed all those reported in 2019.[2]

Insider involvement, though often unintentional, is common. Internal actors are a common component of cyber-attacks. An estimated one-third to one-half of all breaches in the healthcare industry, and one-third in manufacturing, have some level of employee involvement. Even the financial industry (one of the most advanced in terms of ensuring that employees follow cybersecurity protocols and training) has equally high rates of insider involvement. The vast majority of these incidents are accidental on the part of the employee; phishing emails are the most common entry points for threat actors and have become increasingly sophisticated in how they mimic legitimate communication. While appropriate awareness training is critical, it can only help to a certain extent.

WFH environments are generally inconsistent. Complicating matters for businesses is inconsistent technology and access. Issues that were minor when everyone was on the same secure office network now carry more risk and are of paramount importance, including the age, condition, and type of equipment (especially if a business supports BYOD measures); different levels of data access for each employee and function; differences in connectivity speeds and local network security; and even the physical environment and proximity to non-company individuals.

KEY FACTORS TO CONSIDER FOR SECURING REMOTE WORKFORCES

Businesses today are digitally connected across systems, employees, customers, and value chain partners, but most do not have a core competency in keeping this data safe. A dedicated and experienced authentication provider is necessary. Ensuring that the challenges of a remote workforce are well covered allows a business to focus on its strengths, unhindered by concerns of its endpoint security, workforce authorization, and data integrity.

This does not mean that businesses can be complacent about the solutions in which they engage. Numerous critical factors must be considered at the start of such a partnership so the business can maintain its focus on core activities. Overall, the technology behind the solution that a business chooses needs to be comprehensive, flexible, efficient in its rollout and usage, and advanced enough to take on new threats and changes with the business. Passwords alone are problematic: they can be forgotten, are often reused, and can be easy targets of theft through credential stuffing and brute force attacks. More than half of all people reuse the same password on multiple accounts, and 13% use the same password credentials across *all* accounts.[3] Multifactor authentication (MFA) is a leap ahead of password-only systems, and biometric-based security is better still. The gold standard for identification and authentication is biometric-based multispectral imaging, which can even detect faked fingerprints. This latter point speaks to another important quality many companies may not realize: a system should be "human proof" in other ways as well, especially for non-office environments, whether it be the home, an airport, or a worksite.

This means the technology can differentiate authentic fingerprints even if hard to read or dirty and can be ruggedized if needed. Going a step further, being able to fully leverage artificial intelligence in conjunction with advanced biometrics using multispectral imaging creates the most sophisticated solution available today.

Because security is the main driver for advanced authentication, the security of credentials and related information is paramount. Ensuring that this information remains with the enterprise rather than a vendor or third party helps to complete the technology circle.

Along with advanced technology, businesses should consider other aspects as well. Flexibility, for example, is critical and takes many forms. Solutions need to scale quickly and easily so that they can be rolled out across departments and locations, and make onboarding seamless and user removal quick and accurate. Flexibility in implementation also is important so that a business can be protected quickly and limit productivity losses during a rollout. Flexibility also means evolving as a business evolves so that organic growth, acquisitions, and expansions to new regions can easily be integrated into the same solutions.

Efficiency, which is related to flexibility, is crucial. For example, leveraging a vendor that already provides services relating to credentials and authentication can speed up implementation as well as add another level of comfort for employees and in-house IT teams using the system. Many remote employees who used to go into an office may have had smart keycards for entry: can those same cards and credentials now be leveraged to access information remotely?

ADVANCED AUTHENTICATION SOLUTIONS IMPROVE BUSINESS OUTCOMES

This is an opportune time for businesses to re-evaluate their security and authentication protocols and technologies, especially when considering the potential of having a large, long-term or permanent remote workforce. Even if a business has workers who will eventually return to the corporate environment, upgrades to identification and authentication will strengthen the security of devices used outside the workplace, such as after-hours work, temporary WFH, or when employees travel or visit other sites.

Advanced technology is the foundation for a flexible, efficient, and comprehensive solution. User identification and authentication systems need to stay ahead of threat actors and be immune to human error.

> **“Businesses need to ask themselves several important questions: What is the cost of a breach? Can they afford the losses to productivity, brand image, and stock value from a data breach? Have they considered additional risks such as regulatory penalties and litigation costs? Are email credentials or even two-factor identification protocols secure enough?.**

Take, for example, a software as a service (SaaS) company that, prior to the COVID-19 situation, had a combination of remote workers, frequent travelers, and office-based employees, all with different combinations of company-issued devices and personal devices accessing, for example, work email and databases. Now, after several months of having its entire workforce move to remote status, the company is noticing an uptick in attempts by threat actors to hack into email and data systems, likely due to increased cybercrime activity in general, and the difficulty in authenticating a broad, remote workforce operating off of different company and personal devices. The company responded by increasing its security steps and protocols. However, employees are finding that these measures are impeding their work by timing out applications too quickly, making them log in more often with two-factor identification, and even erroneously denying access to certain data systems that they require for their work.

In this situation, the business may benefit from a hardware solution that combines the best-in-class options noted previously, such as the biometrics-based MFA solution provided by HID Global. Its DigitalPersona Workstation improves upon password and two-factor authentication-based identification with simple-to-install devices that are easy to use and complete the security picture.

The HID solution can provide a contactless access card as the first step to access the laptop or workstation. The process is simple and quick for the user, and having a physical, RFID-enabled card that cannot be copied is significantly more secure from the business standpoint. Transferring the organization and its users to this solution can be further expedited by employing the same keycards that users already had for building entry, if available. HID also has an advanced biometric reader that provides enhanced security through the user's fingerprint. The solution can differentiate between real and synthetic fingerprints and can be used even if there is dirt on the finger. This latter instance may not be as much of an issue in a work-from-home situation but is useful for users who may be out at a job site, which is still the case for many types of businesses.

Many industries now find themselves with some tasks that still need to be conducted at a job site or in person. The healthcare industry, for example, may have shifted several of its roles to WFH, such as billing and finance, back-office insurance, and even some aspects of patient diagnosis and monitoring through telehealth technologies. However, even if some work can be done remotely, nurses and doctors will still need to visit patients in person. Advanced identity cards and biometrics facilitate an easy transition from home office to clinic or hospital, allowing the health professional to access patient information in a manner that is considerably more secure than password identification. Along with healthcare, this applies to numerous other industries where not all tasks or roles can fully transfer to remote work, such as those in government, insurance, and finance/banking.

CRITICAL NEED FOR BETTER SECURITY ALREADY EXISTED AND WILL INTENSIFY

The COVID-19 work-from-home situation has highlighted, and intensified, the challenges with password-based authentication. However, this need was prevalent well before WFH became a necessity: for years, frequent, massive data breaches that used stolen credentials have shown that password-based authentication is insufficient in protecting company and customer information.

Businesses have continuously needed to evaluate and upgrade their cybersecurity protocols and processes. This is a particularly opportune time to do so as the challenges of remote work and increased threat actor activity make evident. However, even if remote work mandates abate, cyber threats and the need for enhanced security will undoubtedly persist.

Businesses and other entities, such as governments and institutions, can take the following measures to assess and improve their situations and create plans to remediate vulnerabilities:

1. Consider which systems and data sets can be accessed by password-based log-in credentials. Look beyond email and CRM to shared drives, messaging platforms, and even endpoints and devices.
2. Consider unstructured data as well: Many companies have seen an increase in data shared via less-secure, non-corporate, third-party file-sharing programs. How can this be managed?
3. Place particular focus on endpoints: Laptops, tablets, and other access points secured via a combination of AI and hardware will provide significantly stronger security to all the data accessed through those endpoints.
4. Calculate how much time and effort the in-house IT team has spent in configuring and aligning security measures due to the WFH situation, both initially and on-going. How much of this time could be put to other tasks if security of identification were streamlined?
5. Evaluate partnering with a solution provider that provides the unbeatable combination of sophisticated software analytics with advanced hardware. Ensure that the vendor has expertise within the same industry, and see if other efficiencies can be recognized, such as re-using existing keycards.

Security through advanced authentication is a necessity, regardless of where employees work and access information. Highly sophisticated solutions will protect important institutional and customer data and help prevent breaches that can lead to lost business, reduced customer confidence, and impediments to business continuity. Engaging a well-vetted supplier with such solutions streamlines a business's ability to implement these improvements and allows it to focus more on its core competencies and customer activities.

ENDNOTES

1. Source: Frost & Sullivan research
2. Source: https://thehill.com/policy/cybersecurity/504389-fbi-sees-major-spike-in-coronavirus-related-cyber-threats
3. Source: 2019 Google survey, http://services.google.com/fh/files/blogs/google_security_infographic.pdf

NEXT STEPS

- **Schedule a meeting with our global team** to experience our thought leadership and to integrate your ideas, opportunities and challenges into the discussion.
- Interested in learning more about the topics covered in this white paper? Call us at 877.GoFrost and reference the paper you're interested in. We'll have an analyst get in touch with you.
- Visit our **Digital Transformation** web page.
- Attend one of our **Growth Innovation & Leadership (GIL)** events to unearth hidden growth opportunities.

Silicon Valley
3211 Scott Blvd
Santa Clara, CA 95054
Tel 650.475.4500
Fax 650.475.1571

San Antonio
7550 West Interstate 10
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

London
Floor 3 - Building 5,
Chiswick Business Park
566 Chiswick High Road
London W4 5YF
Tel +44 (0)20 8996 8500
Fax +44 (0)20 8994 1389

myfrost@frost.com 877.GoFrost http://www.frost.com

FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041