How to meet the security challenges of the modern, hybrid work environment

The Next Generation **Human Firewall**

Executive summary

With the move to remote working and the surge in highly targeted and sophisticated phishing attacks, the Covid-19 outbreak has highlighted the challenge of managing security for a dispersed workforce.

Remote working is here to stay. 25% of the workforce are continuing to work from home, according to a recent survey by SWZD[1]. Those able to, are most likely to work in a hybrid, part office/ part remote environment going forward, with 6% working fully from home. Whilst the concept of remote working is not new, there has been a shift in acceptance, and the security challenges it brings are growing.

Having the right security policies and IT tools in place is the first step. But endpoint, email and web security alongside Advanced Threat Protection using AI and machine learning i.e. the technology protective layers, are not the full story. Employees are the main targets of these sophisticated cyberattacks, they are vulnerable to threats and susceptible to human error, but, they are also crucial in plugging the gaps that technology leaves, understanding the subtleties in communication and behaviour that AI cannot possibly detect. Complete all-round security, relies on technology augmented by human intervention.

Enter the Next Generation Human Firewall.

Just as a decade ago we needed next generation firewall technology, we now need the Next Generation HUMAN Firewall to ensure a secure distributed, highly flexible, integrated workforce.

Next Generation Human Firewall

"A dispersed workforce, fully trained and ready to act on security threats with the right tools at their disposal."

1. SWZD - The Future of Remote Work

Top cyber security threats

Cyber criminals are using increasingly sophisticated ways of targeting businesses and individuals. Businesses of all sizes are vulnerable. The gap in the number of breaches experienced by large enterprises, compared to SMBs, is closing[2]. Email phishing scams and malware attacks increased during the recent pandemic, with attackers taking advantage of vulnerable remote workers, who are working on their own, on unsecured networks, away from colleagues and IT support.

85% of breaches worldwide involve a human element[2]. We are easy targets for cybercriminals who masquerade as trusted businesses and senior members of staff, then create a sense of urgency, or take advantage of our natural curiosity, to gain access to valuable data. The list of these types of phishing - from angler phishing, spear phishing and whaling, through to social engineering with baiting, smishing and vishing – is almost endless, even before you consider any new threats that might be approaching around the next corner.

In addition, we all make mistakes and human error is also an issue for IT security, with the potential for inadvertent transfer of data via USB, or selecting the wrong email address from autocomplete in your haste to get information out quickly and efficiently. These human factors, alongside email hacking, stolen passwords, malware, spyware and ransomware, are some of today's top IT security risks. While we do have access to some user security tools, password management and multi-factor authentication, for example, a strong human link in the security chain is still very much needed to counter potential breaches that are constantly changing and evolving at an unrelenting pace.

2. Verizon Data Breaches Investigation Report 2021

Stage 1:

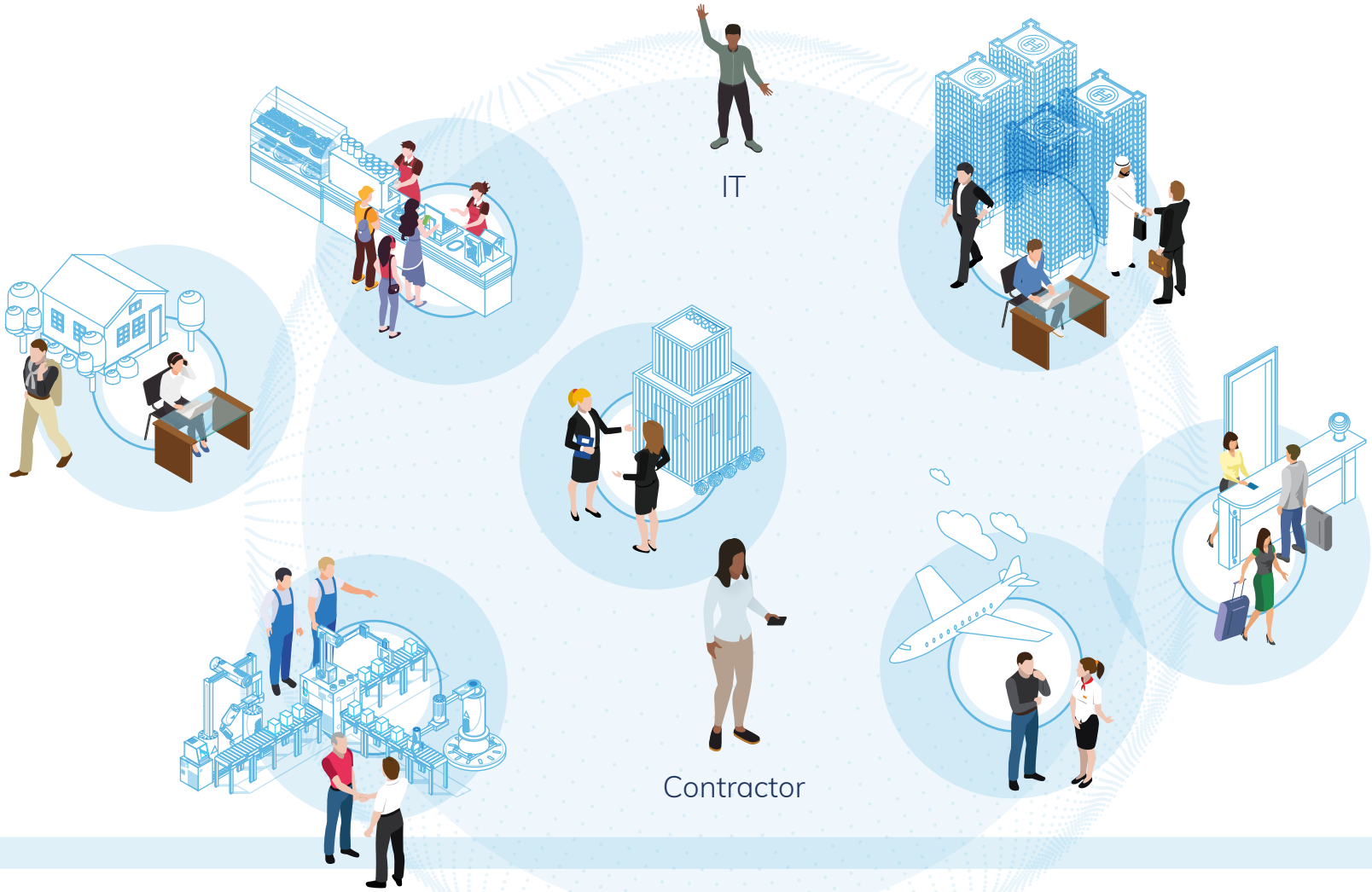
Security technology only.
No inclusive employee training.

Protection is inadequate.

Security & the modern workforce

During the pandemic, remote working became essential overnight, and, for most organisations, hybrid working is here to stay. Remote working brings additional security issues that need to be addressed by the IT team, and IT professionals say it is more difficult to support remote workers than those in the office. Workers need to be aware of security risks wherever they are located - in branch, at home, on site, in a café or hotel. Processes and procedures that are the norm in the office need to be adapted for the remote environment.

The modern 'workforce' is also diverse and highly adaptable. It is often comprised of contractors and freelance workers alongside permanent staff, or involves close intercompany partnerships where resources might be shared. Anyone accessing the network needs to be trained and aware of security risks.



Of technology professionals -

72% say the shift to remote work created additional work for IT

56% say remote work makes securing devices and data more difficult

SWZD – FUTURE OF REMOTE WORK

Security challenges of remote working

In addition to the increased numbers of personalised phishing attacks, there are other human security challenges which need to be considered with remote working:

BYOD devices – Employees are more likely to be using their personal devices when working remotely - whether that is their personal phone, laptop or tablet. This presents the risk of malware spreading from device to device due to a lack of consistent security measures across the organisation and no central security management system.

Home, café and hotel networks may not be as secure as the office, and browsing unsuitable websites can be a drain on productivity as well as a security risk.

Accidentally sending an email to the wrong people can also be a risk whether you are in the office, working from home or out on the road, particularly if you are working in a distracting or busy environment.

And, finally, if there is no reminder in place, **employees can forget to change their passwords**, or fail to do so if they find it too difficult when they are working remotely.

IoT devices - In the home and office, IoT is a potential weak point, with many users using easy to remember passwords and lax security, when using smart TVs and access devices.

Working at home, staff can be distracted (remember how relieved we were when the kids got back to school?), and in such situations it is harder to pay attention and easy to make mistakes, such as exposing sensitive or privileged information.

Staff may also feel that they can circumvent security. Procedures and processes designed for an office environment are simply not applicable in most remote working situations. For example, how do you take care of confidential documents, or ensure that USB drives are not used for storing confidential data?

The human firewall & security awareness training now

The term “human firewall” has been around for a while. It is hard to pinpoint the exact date of the term’s emergence, but it is commonly seen as a group of employees who help detect cyberattacks and follow best practices to intervene and help stop data breaches or suspicious activity, which may bypass security software. The mention of “group” in the popular definition of a human firewall also points towards only a few specialists.

The importance of security awareness and training, is recognised by enterprises who clearly understand the financial and reputational impact any security breaches might have. Acknowledging this need, security awareness training has become the norm in many organisations. However, to a large extent, it is often more of a nod in the right direction, with annual training as a compliance tick box item, rather than an ongoing security programme. Smaller companies may not have had the IT resources to put in place the tools or the awareness training needed, and as a result are potentially even more at risk.

In most organisations more is needed to improve security awareness and ensure that every member of the organisation is part of the human firewall, fully equipped to work in a distributed environment, where “the office” can encompass, not just the company or organisation itself, but close working company partnerships and “employees” who are freelancers and contractors working on a flexible basis.

Stage 2:
With training and a cyber security team.

Protection is improved but inadequate in majority of cases.

The need for a Next Generation Human Firewall

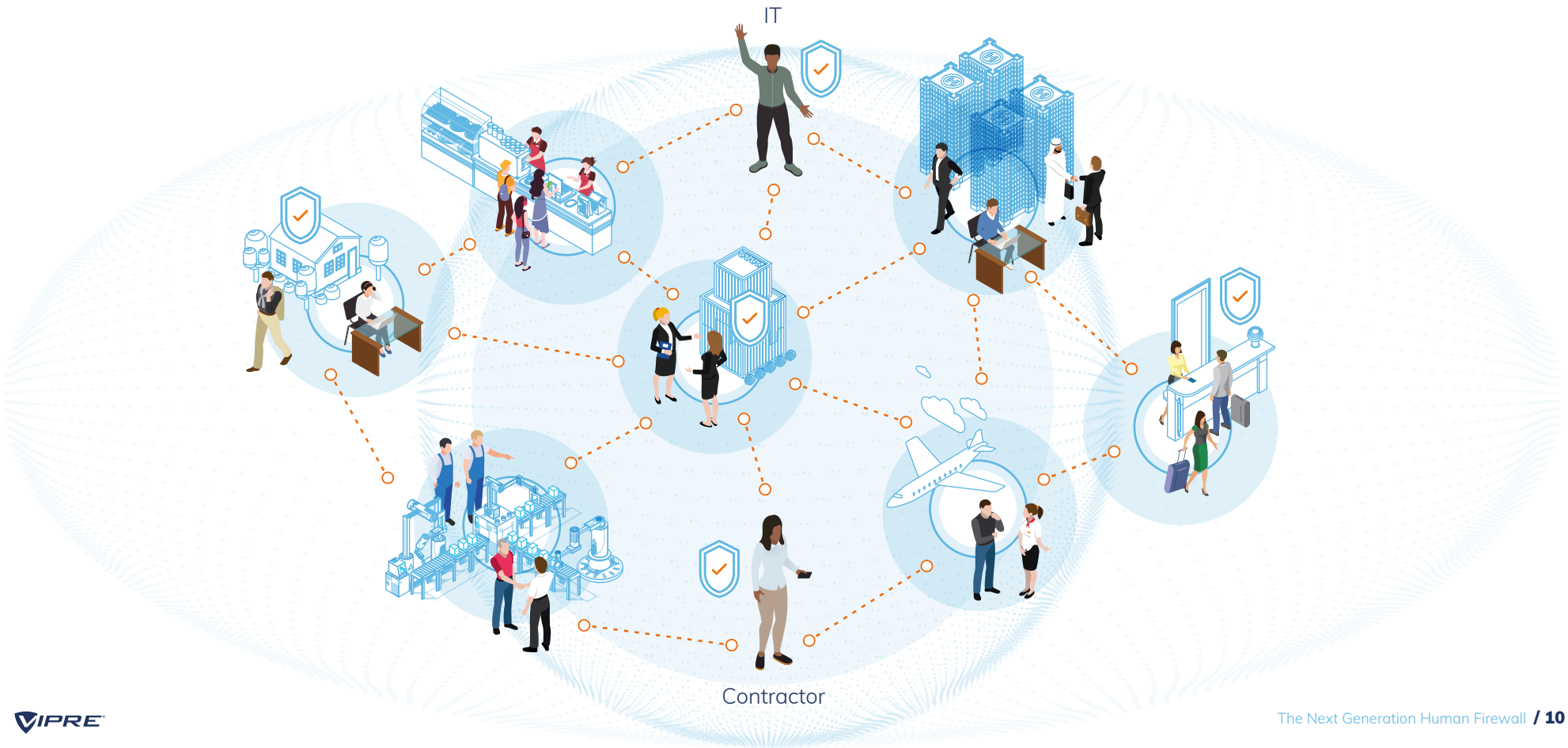
This modern work environment, and the security challenges it presents (alongside those of the traditional office-based workplace) needs the Next Generation Human Firewall.

Just as in the world of technology, the “Next Generation” Firewall, **as defined by Gartner**, has moved beyond port / protocol inspection and blocking, to bringing intelligence from outside the firewall, the “Next Generation Human Firewall” needs to operate outside of the office, the conventional workforce and IT tools. Tools are available to IT to identify potential threats and reduce the risk to the business. But this technology, including AI and machine learning, is not the full picture. Humans are still able to perform complex decision making better than machines and identify any subtle clues to indicate a phishing email, for example.

What is called for is a combination of IT tools and a well-trained Human Firewall made up of all employees and contractors across the organisation, within an intelligent security culture, to give 360 degree protection.

Features of the best human firewalls and best practices

More and more organisations are investing in training, but the key to a safe and agile workforce is to change the mindset of everyone in the organisation, so that all employees are alert, responsible, empowered and educated with regular training, backed up by tools that reinforce a “security first” approach.



An Effective Human Team

For an effective team and an "Evolved Human Firewall", the following 4 elements are needed:

01

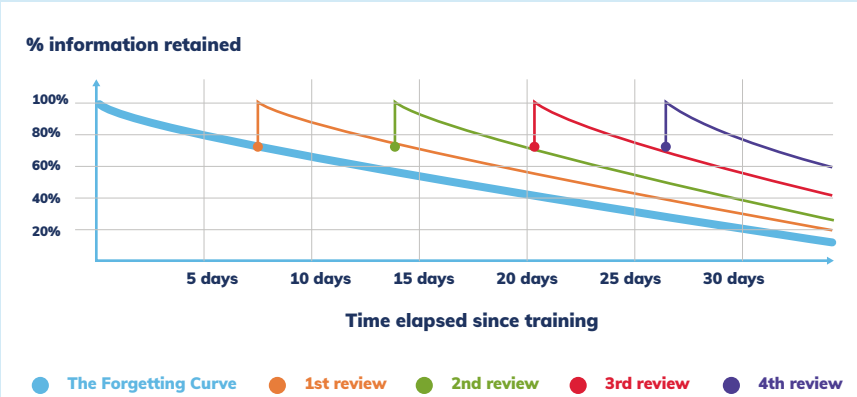
Fostering a security culture through recognition, reward and incentives, rather than fear. An understanding of human behaviour and how adults learn is crucial in creating a culture where security awareness is embraced across the dispersed organisation. The programme needs to be enjoyable and a challenge, where employees are incentivised and can reap rewards. It should ideally include flexible workers and partners.

02

Effective security awareness and learning that is relevant, engaging and speaks to a global audience. Content needs to be relevant and cover material that all audiences (around the world) can relate to. Varied high-quality content, such as micro-learning in small chunks, real-life situations, simulations and gamification, resonates with an audience and reinforces more in-depth courses covering different aspects of security awareness.

03 A process to reinforce learning and keep staff up-to-date and vigilant.

It has been long established that we do not retain the information we learn for long, there is a steep drop off after the initial learning (known as the Forgetting Curve), and approximately 50% of what we are taught in a course can be lost in 3 weeks and up to 90% in two months.[3] Memory can be improved by better representation, such as mnemonics and repetition based on active recall and spaced repetition. Therefore, one-off training is not effective and security awareness courses need to be continuously reinforced with additional content in microchunks, short video reminders, daily security tips, newsletters, alongside posters and screensavers to jog the memory.



04

Frequent measurement with threat simulations to gauge employee security awareness. Ongoing training and awareness should also be assessed for effectiveness through simulations, such as phishing and SMIshing, Vishing simulations and USB baiting, timed at random intervals. When done on a monthly basis phishing simulations can reduce a learner's susceptibility to phishing attacks from approximately 30% down to 2-4%[3]. Following a simulation, employees can be made aware of what to do via videos and other learning materials.

3. Protecting your Organisation by Empowering your Employees

Stage 3:

Employees are involved and a skilled part of the solution.

Protection is further improved, but still inadequate in some cases.

The final piece
IT Tools Working for and with the Next Generation Human Firewall

A vast range of security solutions are available to the IT team to mitigate security risks. Some of these tools are invisible to the user, such as endpoint security, for example, working away in the background to detect and stop cyber security breaches. AI and machine learning have come to the fore in identifying cyber security threats and stopping them in their tracks. AI however, is limited in its role, especially in instances where the subtleties of a phishing email, type of language used, or where the decision to send a document to a specific person, can only really be gauged through human intervention.

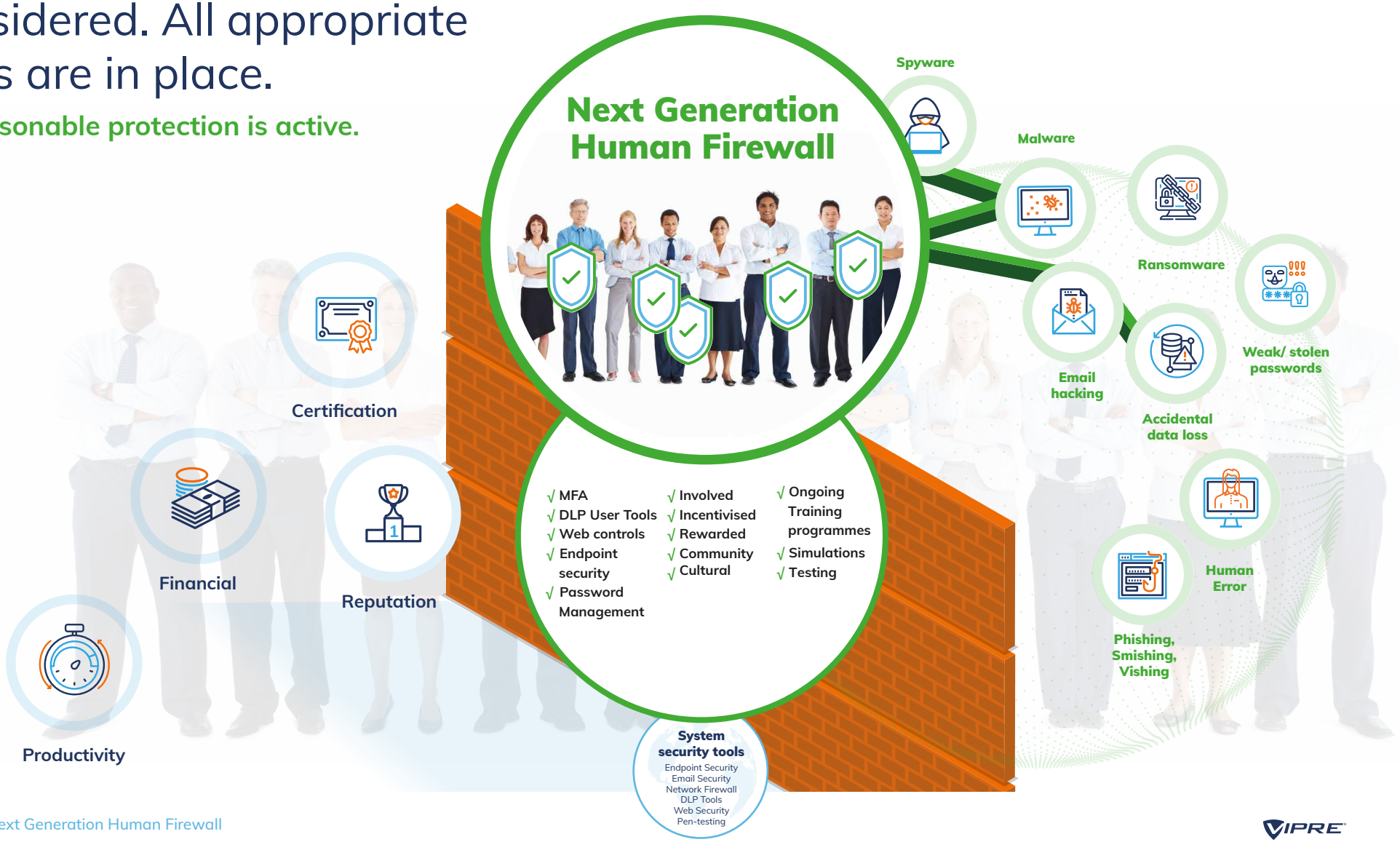
IT solutions are put in place to detect email hacking, malware, phishing and spoofing. But, sending emails is often prone to human error, with mis-deliveries to an incorrect recipient (internal or external) also representing a risk to data security. Tools which ask employees to confirm who they are sending to, along with the email attachments they are planning to send out, can help prevent these types of inadvertent data breaches without having an impact on employee productivity.

Other tools, such as password protection, multi-factor authentication, restricting web browsing and malware protection, are also visible and touched by the user, and the human firewall needs training in their use. When this final piece, an appropriate set of security tools - those visible and invisible to the user - is also implemented, with regular user training and practice; then we can say that the Next Generation Human Firewall is 'active'.

Stage 4:

Diverse workforce fully considered. All appropriate tools are in place.

All reasonable protection is active.



VIPRE

Getting your human firewall programme off the ground

It is a good idea to give some time to planning your programme in advance to ensure success. Here are some next steps to help get your programme up and running:

1) **Understand** the security risks to your organisation and your goals.
2) **Determine** the resources you will need (staff and technology) and secure the budget. Assess the cost of a data breach (resolution and impact on the business) vs. Cost of ongoing training/ awareness.
3) **Obtain** leadership buy-in.
4) **Roll out** the programme with visible leadership endorsement so that it is seen as an intrinsic part of the company culture and success, and is a strategy for the long-term.

Conclusion

The distributed workforce presents additional security challenges, but these can be resolved by embracing a next-generation human firewall with thorough ongoing training and awareness for all with access to company property and information, alongside the right tools to support and assist them, wherever they are located. By building a next-generation human firewall approach, cyber security threats, which will only continue to become more sophisticated in the hybrid workplace, can be fully addressed.

A truly successful human firewall consists of some key underlying principles:

- √ Security awareness is embedded as part of the company culture (alongside already well-established traditional health and safety standards, for example), with all employees involved as champions of security.
- √ Security awareness is second nature. All employees understand that it is in their best interests, not a chore, or solely IT's problem, to spot security issues.
- √ Security supports business success, ensures customer satisfaction, protects business assets and IP, and ultimately results in job security.
- √ Security awareness is also a key benefit outside of working life.
- √ Security awareness and training is an ongoing process. The workforce are made aware of security challenges and education is an ongoing activity which is carried out on a regular basis, not just the annual tick-box item.
- √ Staff are kept informed of new threats and understand how to use the tools at their disposal.

Further reading...

> Protecting Your Organisation By Empowering Your Employees

> Essential How - To Guide Prevent Accidental Emailing

> Data Loss Prevention: Artificial Intelligence vs. Human Insight

VIPRE®

For more information on how to help protect your organisation, please get in touch with a member of the VIPRE team:

global.VIPRE.com/sv | +46 8-5000 94 20