Omnisperience

A NEW CYBERSECURITY CATEGORY: USER ISOLATION PROTECTION

Principal Security Analyst, **Kevin Bailey**

In general, cybercriminals target two key areas: the individual and the computer. Access to these two provides access to data, which can be stolen or altered, and enables access to that data to be removed or used for illegal purposes.

The cybersecurity industry covers every permutation of possible proactive and defensive strategies which they believe increases the protection and security of businesses and individuals. The security categories covering these strategies are forecast to generate more than $248 billion in revenue by 2023[1]*.*

This Green Paper introduces a new security category, which we term User Isolation Protection (UIP) and which targets the primary point of failure – the user. We argue that by refocusing on the user, organisations can shift from mopping up breaches and firefighting to proactively preventing future incidents that critically damage data, systems and businesses. To do this they need to securely isolate the user, without compromising the user’s capability to engage.

[1] Cybersecurity market worth $248.3 billion by 2023, MarketandMarkets

OVERVIEW OF EXISTING USER PROTECTION CATEGORIES

The security industry, and the businesses it protects, approaches user protection from two main perspectives: the individual and the interaction. But existing approaches to tackling these two areas all have their challenges (see *Figure 1*). In general, cybersecurity vendors make user protection security complicated and challenging, requiring users to utilise repetitive and insecure practices. This is because, in many cases, the vendor loses track of their product's original purpose - believing that extra functionality convinces their customer that their product has a greater value than other products. Unfortunately, this often has the opposite effect as part of the user's day-to-day interactions with the product.

Omnisperience advocates that vendors should keep their offerings simple and aligned to the original purpose of their product – with secondary functionality treated as an option to be activated by the end user if required.

We also believe that any user protection solution should provide confidence, not doubt, during user engagement; should be as non-intrusive as possible; and should limit the number of confirmatory interactions between the user and the software. It is these interactions that create the 'Air-Gaps' that cybercriminals exploit to attack the user.

Figure 1 Existing cybersecurity approaches

Activity	Focus	Challenge	**Solution**
Cybertraining	The Individual	Training follows a curriculum of content that is built to inform and alert. It is usually delivered as computer-based training which is periodically embedded into the operational workflow and augmented with reality to build effectiveness. Some outlier organisations build this operational functionality consistently into their businesses. Most content used for cyber training, however, is generalised and out-of-date before it can be delivered, because threats constantly and quickly evolve. Trying to get all users to become proficient in cybersecurity has always been an optimistic goal. It requires users to get used to doing something regularly and thus security-aware from habit. Unfortunately, cybercriminals do the irregular, always evolving their attacks meaning that learnt skills rapidly become ineffective and outdated.	Embedding constant operational cyber training into everyday tasks and activities is the only way to build resilience.
Access	The Individual	It's always about the key that unlocks the door. One or two keys are usually used to provide access to the device, system or application that you wish to enter and interact with. These techniques still rely on the belief that only the legitimate user has access to the systems and devices used to convey or build the keys. But a password or code can easily be copied or cloned, convincing whoever is guarding the access that a user is legitimate. While two-factor authentication (2FA) is better than single passwords or codes, it still doesn't provide sufficient security. Hackers can utilise a wide variety of techniques, such as malware, phishing, man-in-the-middle or account recovery schemes to avoid the 2FA feature or to intercept one-time-access passwords and software tokens.	Multi-factor authentication needs to be advanced, increasing the rotation of various approved categories and distinct user habits or operational limitations.

Source: Omnisperience 2020

Figure 1 (continued) **Existing cybersecurity approaches**

Activity	Focus	Challenge	Solution
Trust	The Individual	The cybersecurity world uses a zero-trust approach. This works on the premise that users are never to be trusted and need to prove their identity before being authorised to do anything. This environment can be overbearing and over-controlling. It inevitably means that rules, processes and procedures can overwhelm and create complex and contextual challenges. Because of this, security frameworks are often perceived as restricting business efficiency, rather than enhancing the user experience and protecting assets. Zero-trust also requires organisations to be constantly aware of changes in roles and responsibilities – with users often being forced to wait for authority to proceed.	Individuals have a number of behavioural traits that are currently being overlooked but which can be used as positive indicators of trust.
Devices	The Interaction	Known in the security world as endpoints, devices include personal and business phones and fixed computing assets. They are usually secured with a mixture of on-premise and subscription software. Such solutions are designed to validate access to the device by the end user and to stop the entry and execution of malware, as well as ensuring data and credentials are being handled appropriately. The most popular endpoint or device is the smartphone, with almost three-quarters of connected users forecast to access the web and applications solely via their smartphones by 2025. As businesses continue to embrace mobile technology both within and outside the office, securing the huge and diverse estate of devices is becoming ever-more challenging.	The increasing choice of devices, as well as their differing personal & business uses and deployments, needs to be automatically recognised and sanctioned for the purpose being requested. Automatic recognition of device protection needs to restrict access and execution to protect wider interactions.
Communi-cation	The Interaction	Technology-enabled interaction is an integral part of our lives. Phishing, ransomware, SIM swaps, etc are all enabled by our thirst for fast, interactive communications. We are continually told that communication security products that encompass e-mail, IM, chat rooms and so on will ensure that our content and data is safe. But data breaches continue to escalate and increasing user-deception attacks have created an environment of mistrust and uncertainty. Cybercriminals use our communications to build pictures of us, including our likes, follows, favourites, traits and interactions. This enables them to engage us and influence our actions.	'Air-Gaps' in interactions that create the entry point for cybercriminals need to be eliminated by combining the enforced use of secure access and authority confirmations with guaranteed malware-free applications and websites.
Acquisition	The Interaction	Digital technologies in the form of e-books, websites and social media have replaced physical books, bricks-and-mortar shops and real-life meetups. But technology has not only replaced real life interactions, it is also employed to eliminate cyber breaches and attacks. The acquisition of knowledge, friends, content, assets, and so on via digital platforms will continue to accelerate, presenting new challenges, while at the same time many existing security architectures take a retrospective 'repair after the incident' perspective, which accepts that someone has to be the victim before anyone else can be protected.	Authentication, authority and secure isolation technology already exists to protect these interactions – allowing organisations to be more proactive. Website access should always be malware-free; data should be stored and access to it based on purpose and intent; payments should be approved only after user authority is confirmed. Inappropriate data movement should also not be preventative but explicitly proactive.

Source: Omnisperience 2020

A NEW SECURITY CATEGORY USER ISOLATION PROTECTION (UIP)

Who is the user?

The depiction of a user creates an image that immediate aligns to the operator (employee) or individual (human) who is interacting with the computing platform or device but, as shown in *Figure* 2, 'the user' can infer a range of different entities that can influence, think, decide and act and doesn't necessarily have to be human. In the same way, cybercriminals continue to create new personas that increase the type, scale and damage that cybercriminality can effect.

Why focus on the user?

The blame or focus of suspicion when a cyber-attack is successful always comes down to probing what an individual employee, partner, user or consumer did or didn't do to cause the incident – whether they are in a leadership, functional or operational role. As individuals we get through life by making the best choices and decisions that we can. But even when making good or decisive decisions, users are fallible.

Historically, human users determined their next action based on learnt behaviour driven by their current attitude to their environment. These attitudes are generally either positive or negative but can also be ambiguous at times - especially during periods of conflict, stress or change.

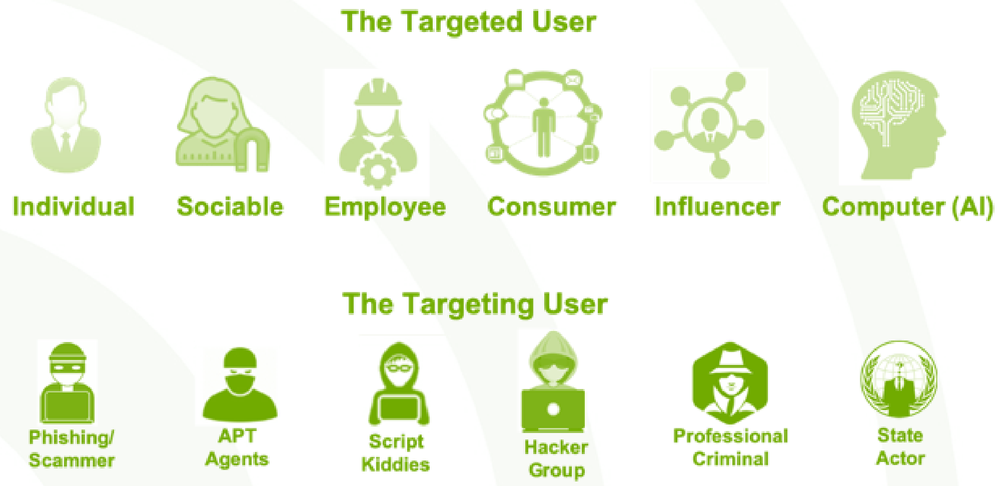
This 'experience-based' approach is retrospective and reactive. When applied to cybersecurity it means that teams spend an inordinate amount of time detecting, isolating and mitigating the damage caused by rogue malware and adversaries that have already gained access to the computing platform.

Exacerbating this effect is the fact that even when 'users' are no longer human, as seen in *Figure* 2, they could be automatically executing algorithms within various programmes based on the outcome of a previous action – which is essentially what machine learning involves.

Users will always be targeted as the weakest point that cybercriminals can compromise to gain entry to a platform, which is why businesses should place far greater emphasis on protecting the user and their associated data.

Omnisperience believes that organisations should reconsider the priority they apply to protecting users and their chosen engagement platforms from the growth in targeted cyber-attacks. Securely isolating the user, without compromising their capability to engage, is an approach we call **User Isolation Protection (UIP)**.

Figure 2 The concept of the user is evolving



Source: Omnisperience 2020

User Isolation Protection (UIP) is a security category whose purpose is to allow seamless digital engagement while proactively securing the user and their data from cyber abuse

UIP combines many of the existing features found in current cybersecurity and information security protection but requires that interactions with the security solution should be as non-intrusive as possible for the user – whether that is directly or indirectly non-intrusive.

- **Directly non-intrusive solutions** ensure that any function minimises the interaction with the user. The user wants their experience to be seamless, minimising any unnecessary technical interaction or delays in achieving the user's intended purpose. A directly non-intrusive solution only requires ratification of the expected process(es) that are aligned to the tasks being undertaken and does not require any unexpected real-time upskilling or diversionary interactions.

- **Indirectly non-intrusive solutions** ensure that the technology understands the capability of the user, intelligently informing them when delays in the interaction occur rather than leaving the user in a state of limbo without access or the ability to complete a task. A lack of interaction at such a time introduces risk, because users may attempt to speed up the process and inadvertently open up 'Air-Gaps' that cyber-criminals can exploit.

What is driving the requirement for UIP?

Firstly, user behaviour is creating more opportunity for criminals to target individuals. Living in an on-demand world means users can engage with everyone they want, whenever they want and wherever they are.

Consideration has been replaced by a demand for faster speed and wider choice. At the same time, individuals are less loyal than ever before because it is so much easier for them to find what they want in ever-more diverse places at the lowest possible prices. In this context, data is both a currency and a passport. But as digital customers move around and interact more, they leave behind a digital wake that exposes them to increased risks.

The second major driver for UIP is changes in criminal behaviour. Professional criminals now look for digital windows not physical windows to break into. Digital crime has a lot of appeal to modern criminals – who range from lone operators to professional organised crime gangs - because it gives them access to vulnerable individuals and also everyone that an individual is connected to (including friends, colleagues and business associates).

All a criminal needs to become a cyber-criminal is an internet connection, details of their first targeted individual, a basic knowledge of coding (or the purchase of an application from the Dark Web), and a plan. Armed with these tools they can quickly expand the scope of their criminality from being a local operator to being a global operator.

INTRODUCING THE USER ISOLATION PROTECTION BRIDGE

It is important to address current cybersecurity technologies and practices that are not working to increase cyber resilience. That said, the greatest challenges that service providers have to battle is the protection of the entry, engage, entrust, expense and exit points where many user-focused attacks occur. By removing the vulnerability when the user is asked to interact, attacks can be foiled before they begin.

The purpose of the UIP bridge is to allow seamless digital engagement while simultaneously and proactively securing the user and their data from cyber abuse. It mitigates the capability of cybercriminals to gain access to individual data, relationships and finances. As can be seen in *Figure 3*, the UIP bridge adopts a 'first-point-of-access' methodology that maintains basic principles for the device, the platform and the ability to interact.

- **Entry** is secured via non-intrusive access across all device types to the digital platform
- **Engagement** is secured via trusted interaction with the digital platform without user deliberation
- **Entrust** – trust is boosted by providing secure data that will not be shared beyond its intended purpose
- **Expense** – merchants are able to validate that transactions are legitimate and honoured
- **Exit** is secured - protecting users from any post-engagement threats and through ongoing data security.

The ability to transition across the UIP bridge requires each of the 'first-point-of-access' elements of security technologies to be addressed, as shown in *Figure 4*.

Access Isolation Layer

Every user needs an endpoint (device) to action an operation, and via which they will subsequently gain multi-directional access to the application or platform and also the permissions they need to conduct their tasks. We call securing this layer Access Isolation. This involves:

- **Devices** – approved device types need to be honoured, optimising the known meta data related to their characteristics, usage and current level of protection.
- **Authentication** – this involves ascertaining that I am the real user by using diverse indicators about my knowledge, traits and unique attributes.
- **Permissions** – once you are sure I am the real user, permissions let me do what I'm permitted to do, while intelligently and non-intrusively safeguarding my data, relationships and finances.

Execute Isolation Layer

Once the user has been granted authorised access and permissions via a device, they need to be assured that the platform(s) they intend to engage is legitimate, which enables them to complete their tasks securely. We call securing this layer Execute Isolation. This involves securing:

- **Operation** – the freedom to engage with the chosen platform or application means ensuring it is free from hidden malware that will misappropriate data, redirect users to compromised websites and use access credentials to steal data or even money.

Figure 3 The User Isolation Protection Bridge

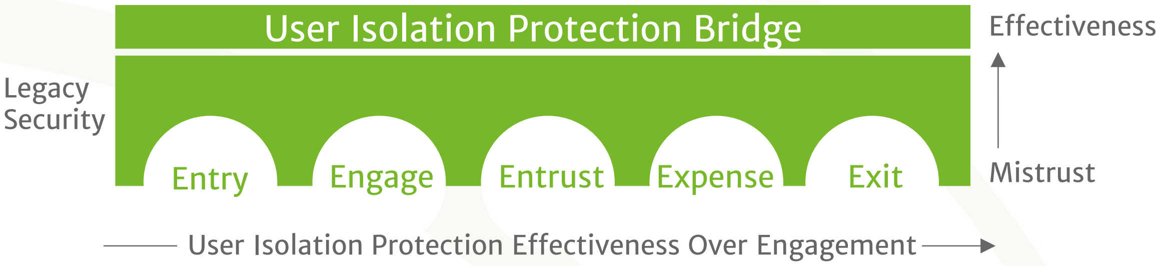
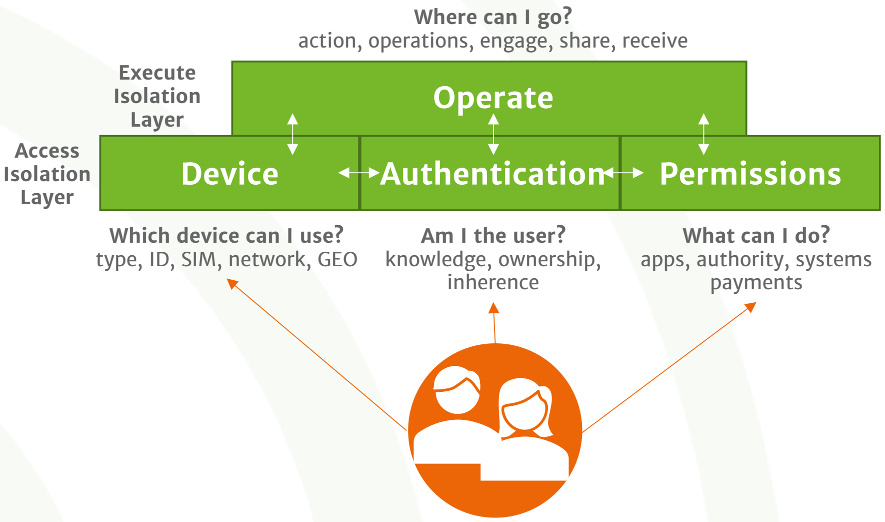

User Isolation Protection Bridge
Effectiveness
Legacy Security
Entry
Engage
Entrust
Expense
Exit
Mistrust
User Isolation Protection Effectiveness Over Engagement

Figure 4 The concept of the user is evolving



Source: Omnisperience 2020

OMNISPERIENCE RECOMMENDATIONS

UIP addresses the first two layers of user interaction with devices and platforms. We acknowledge that there are many other areas that are critical to securing operations and we are not dismissing the importance of these. Rather, our approach with UIP is to start with the basics - the areas frequently used to target users, that damage the user experience, and which subsequently open up all connected activity to further attacks.

1.

Don't stop using existing technology

Nothing is ever achieved overnight and the journey to sustained UIP operation will be evolutionary and not a revolution.

2.

Don't try and make your existing products more complex

You will only frustrate the end user and restrict current operational flows.

3.

Don't turn off existing policies and rules

You will only open yourself up to internal bad practices and circumventions, as well as exposing yourself to external attempts to breach your defences.

4.

Don't rush to swap out existing technology

Your UIP approach needs proper consideration and you need to ensure it addresses both your current and future needs.

5.

Don't support a blame culture

Even though humans are fallible, most people are doing their best in a pressured environment. The only users that deserve blame are those insiders who are deliberately acting to actively damage your business and your colleagues

6.

Do acknowledge that you have operational environments that expose the user

Obtain statistics and analytics that prove you could do better.

7.

Review the UIP layers

Analyse each element to understand your protection capabilities.

8.

Discuss the needs of the entire organisation

Including their current needs for access and authority. Inspect existing and planned internal and external platforms and portals to ensure they are malware-free.

9.

Educate users about cyber awareness

Educate employees so they understand the various methods that cyber-criminals are using to target individuals and your business.

10.

Keep patching your hardware and software

Many updates inhibit the flow of specific malware, and also restrict the spread of zero-day attacks.

Review the **User Isolation Protection Requirements Selection Process** Green Paper that accompanies this one, which will help you chart your journey when considering alternative solutions that meet the requirements of UIP.

You can download a copy of this from our website www.omnisperience.com

About the author

Kevin Bailey is the Principal Analyst and subject matter expert for security, storage and go-to-market strategies. He has over 20 years of practical experience leading teams for major brands such as Symantec, BAE Systems AI, and Clearswift in the security space, including leading the EMEA research for security software at IDC. He is a judge for the GSMA's GloMo Awards for security and identity management and a regular contributor to industry media.

About Omnisperience

Omnisperience is a leading independent research and advisory firm focused on the telecommunications, media and technology (TMT) industry. Our purpose is to help B2B service providers become more profitable by understanding and meeting the evolving needs of their customers. We provide in-depth expertise and fresh insights that help customers reimagine their businesses and improve commercial success.

This is achieved through insightful primary research, distinctive analysis, factual and authoritative papers delivered through direct and consistent interaction with B2B telecoms service provider clients. Deliverables are pre-tailored to the needs of clients in formats that make them easy to consume and apply to the target audience. Omnisperience engages and inspires your teams, partners and customers, delivering Value Through Experience.

About this paper

Omnisperience Green Papers are preliminary reports intended to provoke thinking and further discussion. They are often the precursor to an in-depth white paper on this topic. Those wishing to provide feedback to this paper, or who wish to sponsor further research in this area, are welcome to contact us directly. You are free to circulate the paper to your peers and customers. You may also re-use content from it provided you attribute it to source (Source: Omnisperience 2020).

Omnisperience, 71-75 Shelton Street,
Covent Garden, London WC2H 9JQ

For more information:

Blog and podzine: omnisperience.com

Email: editorial@omnisperience.com

Linked In: Omnisperience

Check out our website for more complimentary research papers.