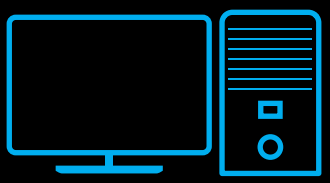
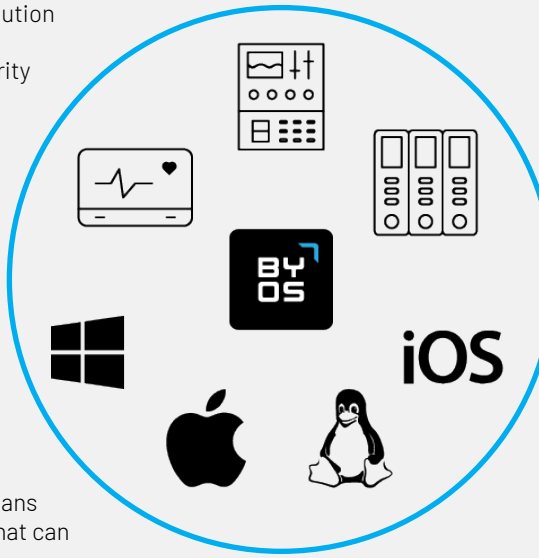
BYOS

A Byos Approach to Counteracting Social Engineering



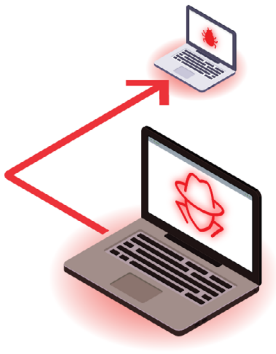
Recent attacks against MGM and Caesars entertainment highlight the sophistication and evolution of Social Engineering attacks. Today's adversaries are using advanced techniques that are outpacing industry attempts to educate their workforces and/or maintain network data integrity with legacy security solutions. These attacks can be devastating to a company's hard-earned reputation and revenue. Though no official number has been reported in the Caesars attack, estimates are in the millions, while MGM disclosed that it could realize as much as a $100M impact to its business.



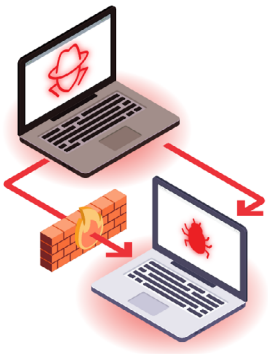
These enterprises have some of the most advanced security operations centers in the country, in many instances exceeding the security found in many other industries. They spend millions of dollars annually on in-service training for their employees, and perhaps tens of millions of dollars to maintain their security posture. Still, Social Engineering has proven to be a soft spot in even the most resilient network environments.

Ironically, Byos was developed to protect assets at a Black Hat Convention in Las Vegas. These conventions are renown for attracting the best and brightest hackers from around the world. Our founder did not want his asset to be compromised, which is a commonplace occurrence and something that hackers do for sport at this convention. What started as a means of protecting his mobile asset from compromise has evolved into a fully-featured capability that can prevent even the most advanced attempts to exploit a network through Social Engineering.

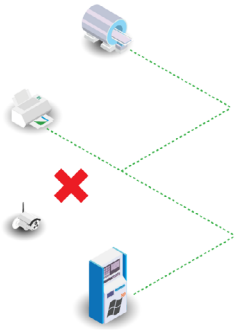
Without Byos



Software **can't truly isolate threats before they reach the asset** because it runs **inside** the asset and is controlled by the OS.



Software is **vulnerable to bypass and stealth attacks**, a core reason why lateral movement is so difficult to detect and contain.



Software **cannot be installed on legacy or unmanaged devices**, leading to more widespread attacks on critical infrastructure

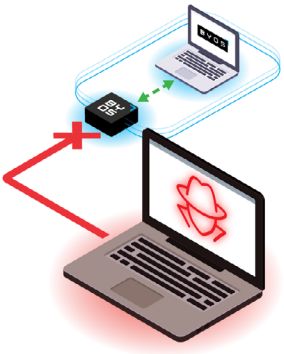
A few things Byos can do

For starters, Byos eliminates the Risk of External Attacks: By making your assets invisible to the internet, Byos eliminates the risk of attacks such as DDoS, Exploitation, man-in-the-middle, lateral movement, network & asset discovery, route alteration, and much more. In the case of Social Engineering, an adversary would not be able to locate the network from the outside. Having access to an employee's login and password would be useless when trying to connect to a network that is undetectable to non-authenticated assets.

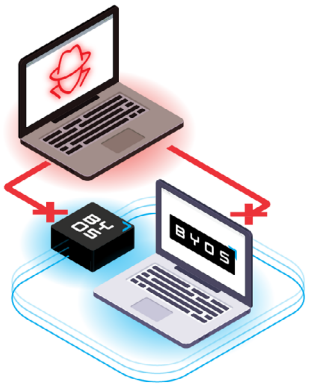
Next, Byos reduces the Attack Surface/Blast Radius: By physically separating the assets, Byos reduces the attack surface, making it more difficult for cybercriminals to find and exploit vulnerabilities. From the perspective of Social Engineering, if an adversary were to somehow gain access to the network, the amount of "damage" they could do to an enterprise could be limited to the assets on a given portion of the network (where a Byos subnet is created), or in the case of a 1:1 deployment, fully contained. An adversary would have to have access to the specific machine that holds the specific data they were attempting to exfiltrate or exploit. No lateral movement or privilege escalation is possible. And the attack surface is reduced by 99%.

Additionally, Byos Increases and Hardens Asset Security: By removing visibility of assets from the public or private networks (while allowing the network owner to access and manage the assets), Byos increases and hardens the security of assets as cybercriminals can't find the assets to attack them. This introduces additional layers of Zero Trust within a network, by creating subnets for different job functions / departments / users. Adversaries can't attack what they can't see. If an adversary gained access to a hotel reservation server, they would not be able to take control of all electronic hotel room locks, for example.

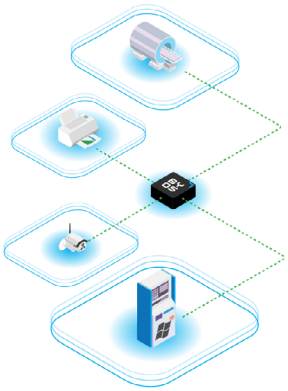
With Byos



Byos lets you **monitor and control the traffic at the outer edge**, physically stopping attacks before they reach the asset



Byos **runs independently from the asset and OS**, providing a stronger containment strategy against attacks



Byos delivers **device and OS-agnostic protection**, minimizing the attack surface and broadening the coverage area

Prevention over mitigation

The power of Byos goes beyond its network obfuscation capabilities. Device Authorization ensures that even if a Social Engineering attack is successful, and an adversary were to gain login and password information, that information cannot be used to breach a network without a Byos-authenticated endpoint, and an additional asset for independent user authentication (a cell phone or tablet authorized to receive a random-generated login code, finger-print scan, facial scan, etc.). An adversary would need login/password info, a Byos-enabled asset, and the correct mobile device of a user authorized to receive the authentication code for that specific asset. Translation: Your Social Engineering threat surface is effectively eliminated, even in the presence of human error whereby a successful attacker obtains login and password info.

Furthermore, assets can be geo-fenced. This means that some assets might only be allowed to connect to the network while on premises, or from a specific off-site location. In this instance, an attacker would have to have deep inside knowledge about which assets were authorized for remote access, gain access to one of those devices, and have a login/password/external authentication vector to gain access to the network.

Human error is and will remain the #1 cybersecurity threat in all industries. People make mistakes, and we can't train or engineer human error out of every equation. Sadly, these mistakes can cost companies tens or even hundreds of millions of dollars in lost revenue. Byos reduces the risk of human error, and mitigates the risks of advanced Social Engineering techniques. This allows security teams to determine where, when, and how their assets are protected all the way out to the edge, and beyond the edge due to network obfuscation and multi-factor authentication.

Byos makes it Easy to Deploy and Secure against Social Engineering

Byos is simple to deploy, manage, scale, without having to change the underlying network. If you're looking to counteract and contain the risks of social engineering on your network, simply connect with us at engage@byos.io request a demo here: byos.io/request-demo