+1–855–249–4453
www.trapx.com

BUILD YOUR OWN TRAP - SOLUTION BRIEF

No matter how good the security of your network perimeter is, there will always be a group of extremely talented and sophisticated hackers waiting and willing to compromise it. In the end, building the most robust defense perimeter fortress will not entirely guarantee security; but **the only way is to outpace these hackers by knowing their ways and beating them on their field.**

Deception technology is the next generation in cybersecurity.

> *"All warfare is based on deception. Hence, when we are able to attack, we must seem unable; when using our forces, we must appear inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near."*
> — Sun Tzu, The Art of War.

TrapX DeceptionGrid is a powerful threat detection platform that creates a shadow network to disorient and trap would-be attackers. The platform consists of built-in tokens (lures), patented emulations camouflaged as real assets and support for full operating systems, which diverts, exposes and misinforms these attackers.

In addition to our robust selection of workstations, servers, IoT devices, networking, medical, industrial and financial emulations, TrapX allows you to "Build Your Own Trap" for any device or application not already predefined in our solution set – giving you utmost coverage capabilities across any network in any market segment, no matter how obscure, old or forgotten your equipment may be. Said more simply … if it has an IP address – we can emulate it and protect it by camouflaging it, making it unavoidable to any attack.

> **With Build Your Own Trap (BYOT)– your real assets become harder targets allowing you to go from damage control to damage prevention. For more information on Build Your Own Trap, visit TrapX.**

BUILD YOUR OWN TRAP (BYOT)

Typically a deception platform would create managed honeypots using virtualized decoys. Those legacy honeypots use a lot of resources and require software to mimic legitimate assets across the network. These decoys would often be limited to a single virtual/physical instance and on top of that, it wouldn't entirely resemble the company's specific assets.

TrapX DeceptionGrid is a next-generation Deception Platform. It is capable of creating a simulated attack surface that misleads would-be attackers into turn-key traps. A hacker would never be able to tell the difference between what's fake and what's real because these traps can be tailored to look and behave like tangible company assets.

Build Your Own Trap (BYOT) allows you to create customized attack surfaces, with fake devices, applications, and even web applications. A crucial distinction of this feature is that each of these traps is not the usual fully virtualized (or physical) "honeypot server," which consumes precious resources and OS licenses but accurate emulations of those services.

Each DeceptionGrid appliance supports over 500 traps, which can be crafted quickly and easily to look identical to the company's real environment. Such a massive number of traps can be deployed on a large-scale enterprise network without consuming too many resources like licenses, servers, VMs, etc.

REDIRECT

Building a fake attack surface with your own traps makes it more convincing for the hacker to move forward over the entire virtual minefield, eventually leaving tracks and setting off alarms. These traps will ultimately detect malicious activity, and alert the cybersecurity agents with actionable steps.

BUILD AN ENTIRE DECEPTION ENVIRONMENT.

Experienced hackers already know and understand the possibility of stumbling upon a traditional honeypot. They might even be able to quickly identify the "too-good-to-be-true" server traps sitting outside DMZs, unprotected, and without outbound traffic.

But with the right type and density of traps, you can turn the tables around and trick even the most clever attackers running sophisticated hacking scripts.

Aside from building your BYOT “traps,” you can also take advantage of a myriad of predefined traps available with TrapX’ DeceptionGrid, so that you can reduce your deployment times. A few examples of some predefined traps:

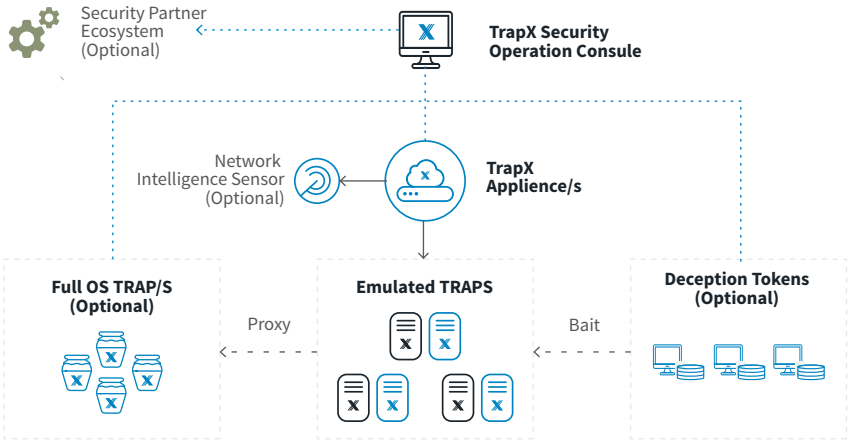
- SCADA Devices
- Cisco Devices
- Linux Servers
- Lexmark Printers
- WebCams
- IoT Smart Lights
- Windows Server
- POS (Point of Sale)
- And a lot more

Aside from the known devices, BYOT from DeceptionGrid, allows you to build an entire attack surface and camouflage it to look identical to your real IT, OT, IoT, or IIoT environment. **Depending on your strategy , you can build a low-to-high trap density with any level of interaction.**

For example, a diverse deception scenario might be filled with emulated decoys, which look like Windows PCs, printers, Cisco routers, medical devices, manufacturing monitors, smart thermostats, ATMs, IP cameras, etc., all with the purpose to attract attackers. In addition to these predefined emulated decoys, you can build a trap to emulate any proprietary system. Aside from devices, you can also place deception tokens, (or breadcrumbs) on the user's PC to disorient and lead hackers into high-interaction traps.

These emulated traps divert all traffic using a smart proxy to low-density and high interaction traps. These high interaction traps are the full-blown devices with operating system running apps and services, such as full Linux OS servers. These servers aim for deep deception. They attempt to keep the hacker engaged, while the cyber security team gathers intelligence on the attack.

You can also lure and trap the attacker with **fake authentication instances of websites and sensitive web applications**. These "web app" traps look, feel, and behave just like normal authentication paths, but when someone is attempting to compromise it with something like an SQL injection or a cross-site script (XSS), you'll be notified immediately.



All these advanced decoys will lure attackers with malicious intentions towards your specific assets with particular vulnerabilities. From the point of view of the attacker, these are attractive and easy targets which can be exploited. The attacker can run standard hacking tools or specific protocols like SMB, SSH, Telnet, WMI, DNP, bonjour, Modbus, etc., but can't run customized code that would compromise the trap itself.

PUTTING IT ALL TOGETHER.

Thinking ahead of time and attempting to anticipate what a potential adversary might throw at you is the key to successful threat detection and mitigation. **DeceptionGrid provides you with the right proactive approach (Detect > Deceive > Defeat) to not only defend but to defeat the attacker.**

Being able to build diverse contact points, makes it easier for security teams to detect threats, measure the intention, gather forensics, and ultimately attack the hacker.

> *"Attack is the secret of defense; defense is the planning of an attack."*
> — Sun Tzu, The Art of War.

1. Detect: DeceptionGrid 7.0 detects the attack and tracks down the activity of the hacker, reporting on what type of protocols and scripts are being used. The longer the system is able to engage "trap" the hacker, the more information will be obtained. This level of awareness is extremely helpful for taking down any level of attack.

The platform provides an attack intelligence service for receiving TTP (Tactics, Techniques, and Procedures) notifications from TrapX Labs. These notifications include insights into the attacker's behaviors, with details like; attack signatures, behavioral rules, new kinds of Malware, or any new hacking campaign that is targeting specific industries. These notifications allow time for patching and improving security.

2. Deceive: Deception mechanisms improve the detection accuracy by removing any dependency on signatures and attack databases. Deception is where the BYOT feature plays a key role. **It allows you to "appear weak" when, in reality, "you are strong."**

The BYOT feature gives you the right tools to lay down hundreds of customized traps and lures to attract attackers into decoy (high interaction) targets loaded with intrusion prevention/detection sensors and sensible alarms.

3. Defeat: Attackers landing on these traps, will be logged, alerted, and tracked down. These alerts also contain information on how to act immediately. Additionally, the DeceptionGrid platform allows you to build automatic response and mitigation workflows by integrating with third-party vendors such as CarbonBlack.

KEY BENEFITS.

• **Wide Coverage:** The ground-breaking "Build Your Own Trap" feature is the only solution on the market that can cover any network, from legacy, IT, OT, SCADA, IoT, and even IIoT. A trap can be tailor-made and disguised to look like any device based on your current network assets and industry.

• **Scale Easily:** With BYOT, you can build emulated traps and saturate the entire network with hundreds of fake hosts, apps, users, etc., all with sensing and alarming capabilities. A key advantage is that each of these hosts don't require a full virtual machine or physical server, but this is all done from a single TrapX appliance.

• **High Deception Probability:** Achieve a high detection probability with a distributed Intrusion Detection System (IDS). Build a combination of low density but high interaction full OS application traps (Linux or Windows server) and high density of low interaction emulated traps (printer, Cisco switch, IP camera, etc). Improve your distributed IDS by strategically placing deception tokens. These tokens are passive information elements on the user's PC that disorient and lead hackers into high interaction traps.

• **Centralize Management & Monitoring:** Create, manage, and monitor all your customized traps from a single management console. From this console, you can also keep track of attacks, including source IPs, protocols, ports, etc. To make it easier, you can access the interactive, and clickable attack map.

• **Save Deployment Time:** Besides customizing your own BYOT traps, you can reduce deployment times, by using the dozens of predefined traps provided by TrapX. You can also take advantage of TrapX's DeceptionNet Community where users have built and shared thousands of different traps, to use in your deception environment. These users also share their best deception strategies and practices to defeat the most sophisticated attacks.

• **Deception At The Exfiltration Phase:** Let's say the attack succeeded — the hacker located and gathered tons of valuable information. Now, the hacker has reconnaissance data (network topology, device names, etc.,) access data (passwords and usernames,) and even business-related data such as employee's data or business plans, etc. DeceptionGrid allows you to build and include decoy data files (deception tokens) to further deception at the exfiltration phase. You can build your own decoy data to make exfiltrated data look authentic.

For more information on Build Your Own Trap and the DeceptionGrid platform, Contact TrapX for your free demo.

ABOUT TRAPX SECURITY

TrapX Security is the pioneer and global leader in cyber deception technology. Their DeceptionGrid solution rapidly detects, deceives, and defeats advanced cyber attacks and human attackers in real-time. DeceptionGrid also provides automated, highly accurate insight into malicious activity unseen by other types of cyber defenses. By deploying DeceptionGrid, you can create a proactive security posture, fundamentally halting the progression of an attack while changing the economics of cyber attacks by shifting the cost to the attacker. The TrapX Security customer-base includes Forbes Fortune 500 commercial and government customers worldwide in sectors that include defense, healthcare, finance, energy, consumer products, and other key industries.
Learn more at www.trapx.com.

+1–855–249–4453
www.trapx.com
sales@trapx.com
partners@trapx.com
support@trapx.com