Mainframe Guard

A deception-powered solution for protecting the bedrock of the business from APTs

Mainframe systems are silent enablers of the global economy— powerhouses that process 68% of the world's production workloads and support over 30 million transactions per day, including 87% of all credit card transactions, 29 billion ATM transactions per year, and four billion passenger flights annually.* But from a cybersecurity standpoint, mainframes are often weak links that leave enterprises vulnerable to significant risk.

As growing attention is paid to securing web applications, mobile payments, cloud services, smart devices and other aspects of digital innovation, security for mainframes too often takes a back seat, even though many of these new offerings rely on mainframes for essential backend data processing and storage functions. *Mainframe Guard is a 100% non-intrusive solution that stops advanced attackers from reaching mainframe systems, preventing data theft, espionage, and disruption to critical services.*

Securing the enterprise nerve center: APTs demand a new approach

There is a common misperception that mainframes are inherently more secure than other platforms. But particularly with older mainframes, standing up security solutions is labor-intensive. With limited integration options and a shrinking pool of mainframe talent, it can be difficult to configure security controls and collect logs for adequate mainframe monitoring.

Newer mainframe models embed data encryption functions, but mainframes are often viewed as 'untouchable' for fear that configuration changes or upgrades will cause business disruption, so migration to newer, more secure platforms is rare.

But whether the platform is new or old, encryption won't stop an attacker who's using stolen credentials from accessing sensitive information, nor does it ensure the integrity of the system itself or the applications it hosts. Mainframes ideally do need to be hardened, but a controls-centric approach can allow advanced attackers to go undetected until well after the damage has been done.

With Deceptions Everywhere® the network is your mainframe defense

As an enhancement to Illusive's Core Solution, *Mainframe Guard* works by spreading traps across the network so that wherever the attacker first gains entry, his movements toward mainframes and other high-risk systems can be detected and derailed. There is a 99% chance that an attacker will be discovered within his first three lateral moves. "Traps" are deceptions – fake data and objects that appeal

* IBM Mainframe Ushers in New Era of Data Protection, on www.ibm.com, IBM, July 17, 2017.

to the attacker's desire to find and move toward high-value targets. When a deception is used, an alert is triggered. A forensic snapshot records what the attacker was doing at the time of detection, and is instantly attached to the incident record to support rapid action. Solution components include:

- **Purpose-built mainframe deceptions** for mainframe environments and clients;
- **A visualization of mainframe "Crown Jewels"** within Attacker View — a part of the Illusive management console that shows security staff potential attack paths and attacker proximity to mainframes;
- **Views of the mainframe environment** that enable defenders to proactively identify and monitor unexpected connections to mainframe servers;
- **An interactive Trap Server layer** that mimics mainframe behavior and login screens. This layer incorporates knowledge of actual tactics used to carry out known attacks on mainframes, tricking attackers into believing they are interacting with an actual, exploitable system.

No matter the state of your current mainframe security architecture, Mainframe Guard can help compensate for some of the challenges inherent in securing mainframes. But most important, it provides a solution to the long-standing challenge of how to detect APTs that otherwise lurk unseen. With so many vital end-to-end services dependent on mainframes, integrating them into a comprehensive deception solution is a significant advance in reducing business-critical cyber risk.

Benefits

- **Detect APTs early.** Avert a cyber crisis by trapping attackers before they reach the mainframe.
- **Improve mainframe security without mainframe talent.** Our out-of-the-box solution eliminates the need for piecemeal, custom-built integrations.
- **Install quickly and easily, with no downtime.** Our agentless technology deploys automatically — *around, not ON* — mainframe systems, and with no disruption to users.
- **Prioritize response activity.** Illusive generates no false positives and provides risk context to focus efforts on what matters most.
- **Streamline incident analysis** with source-based forensic data instantly embedded in incident records.
- **Adapt automatically** as the business and threat environments change — with little ongoing effort.

Contact us

For additional resources or to subscribe to our blog, please visit us at www.illusivenetworks.com.

To arrange a meeting about how to protect your mainframe-enabled services and operations, call:

US: +1 844.455.8748

Outside the US: +972 73.272.4006

ABOUT ILLUSIVE NETWORKS

Illusive Networks is a pioneer of deception technology, empowering security teams to take informed action against advanced, targeted cyberattacks by detecting and disrupting lateral movement toward critical business assets early in the attack life cycle. Agentless and driven by intelligent automation, Illusive technology enables organizations to significantly increase proactive defense ability while adding almost no operational overhead. Illusive's Deceptions Everywhere® approach was conceived by cybersecurity experts with over 50 years of combined experience in cyber warfare and cyber intelligence. With the ability to proactively intervene in the attack process, technology-dependent organizations can preempt significant operational disruption and business losses, and function with greater confidence in today's complex, hyper-connected world. For more information, visit us at **www.illusivenetworks.com** or contact info@illusivenetworks.com.