RevBits®

DATA SHEET

Deception Technology

The Only Deception Technology Available Which Deploys Real, Desirable, Attractive Server-Based Honeypots to Trap Malicious Actors in Dual-Layered Virtualization.

As malicious actors have become more sophisticated the need for smart security has increased. Once the malicious actor is inside and capable of moving laterally, the existence of honeypots may be the last line of defense against catastrophic loss of data.

Solution Features and Capabilities

Robust monitoring
RevBits Deception Technology provides insight into current attacks to detect, track and respond to sophisticated threats in real time.

Fortified jail
Dual-layered virtualization of the honeypot, ensures escape by malicious actors is nearly impossible.

Deploy popular servers and applications
RevBits Deception Technology utilizes the most common database servers, file sharing services, and many others.

Cloud ready
Cloud images for Amazon, Google and Azure are available for use with the deployed deception technology.

Attractive bait
RevBits Deception Technology leverages two methods of implanting attractive bait. System administrators have the option to manually implant breadcrumbs in application config files or automatically deploy credentials (honeydrops) across workstations in the network. Both breadcrumbs and honeydrops will lead attackers to honeypots and reveal their source.

The goal is to attract the threat with real servers and once there, trap the threat and prevent escape.

Simple and rapid deployment
Install RevBits Deception Technology on any server within the network.

Low resource consumption
Numerous honeypots can be launched within each VM, minimizing system resources and maximizing operational efficiency.

Immediate image access
All honeypot images are maintained by RevBits and automatically pulled and deployed to the client network on demand.

Advanced integration and reporting
RevBits Deception Technology integrates with SIEM products to deliver real-time alerts. SMS and email alerts are sent to system administrators on incident occurrences. Detect and block attacks designed to impersonate trusted senders. Malware-less attacks are thwarted through real-time scanning of emails, detecting header anomalies, similar domains, and sender spoofing.

Software Requirements

Server: Hosted in client's network and is Linux based

Available Cloud Images for Deployment: Amazon, Google, Azure

Deception Technology Benefits

Affordable deployment – Through unique design, RevBits Deception Technology allows for extensive deployment of honeypots without increasing the use of resources. One RevBits server can host multiple honeypots in the network.

Increase the value of deployment through successful threat hunting - The value of deploying RevBits Deception Technology is increased because of the use of real server-based honeypots. The use of real server-based honeypots increases the likelihood of capturing the malicious actor and preventing them from accessing other important assets in the network.

Built with security in mind – RevBits Deception Technology uses dual-layered virtualization to ensure entrapment of the malicious actor or insider threat. This dual-layer virtualization ensures that the investment in the product is realized - once trapped in a RevBits Deception Technology honeypot the likelihood that the malicious actor can escape is significantly reduced.

Simple deployment – RevBits Deception Technology is simple to deploy - no specialized software is required for deployment of the technology, with multiple cloud-ready images ready for use.

Additional Solution Features

Manage malicious actors and insider threats – RevBits Deception technology is designed to take on the malicious actor who has gained unauthorized access in the network, as well as the insider threat trolling the network to access valuable assets. In both cases, the goal is to attract the threat with real servers and once there, trap the threat and prevent escape. RevBits Deception Technology is built to accomplish these two vital requirements in deception technology.

Easy to deploy, easy to manage – With RevBits Deception Technology, real honeypot database servers (MySQL, PostgreSQL, MSSQL, etc.), file servers (FTP, SMB, etc.), network devices (routers, firewalls, etc.) and common network protocols (SSH, RDP, VNC, etc.) can all be launched with a single click. A central dashboard allows network administrators to manage, configure and monitor all honeypots throughout their enterprise.

Unique design – The dual-layer virtualization architecture of RevBits Deception Technology provides superior encapsulation of attackers in honeypots. In addition to the security benefits, RevBits Deception Technology allows for ease of deployment, efficient management and low resource consumption.

Keep Your Enterprise Protected. Get a Demo or Free Evaluation.
To learn more, visit www.revbits.com

34 Willis Avenue • Mineola, NY 11501 • 844-4REVBIT (844-473-8248) • www.revbits.com