

Deception Technology

RevBits Deception Security Floats Like a Butterfly, Stings Like a Bee.



Just before Cassius Clay, who later changed his name to Muhammad Ali, fought world heavyweight champion Sonny Liston, he was asked about his approach to the upcoming bout. Clay responded, "Float like a butterfly, sting like a bee." His meaning? He would use his fluid and agile footwork while delivering powerful knockout punches. It was this combination of deception, agility, and power that made him such a fantastic contender.

Unfortunately, today's cyber criminals seem to be capitalizing on that playbook with nimble and powerful threat tactics that breach enterprise systems, compromise assets, and hold data for ransom. Security teams must become as wily and agile as their attackers, utilizing their own deceptive tactics that will take their opponents by surprise.

Turn the tables on bad actors using breadcrumbs and honeypots

Deception technology prevents bad actors from infiltrating corporate networks and causing significant damage. It generates decoys or honeypots that imitate legitimate digital assets within an organization's IT infrastructure. This tactic deceives cyber criminals into thinking they've discovered a way to attain privileges, exploit servers, and engage in data theft. Deception technology sets traps that mislead and capture even the stealthiest cyber criminals, delivering a powerful sting and knockout punch.

RevBits Deception Technology is a sophisticated early breach detection and capture system that thwarts external and insider threats.

RevBits deception technology detects, deceives, and ambushes

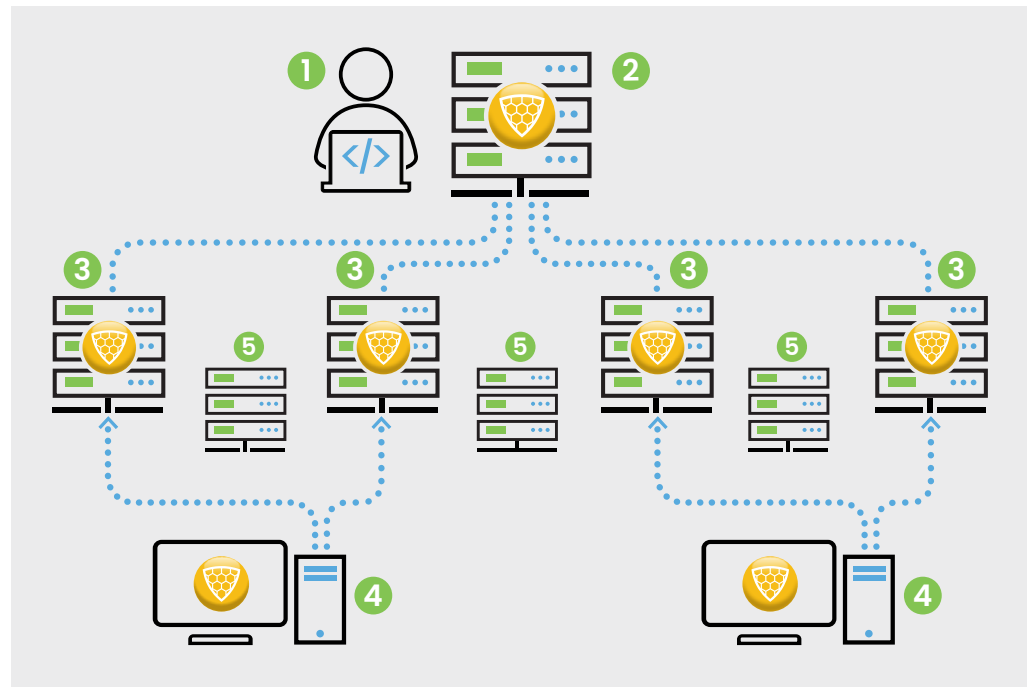
Effective cybersecurity, like RevBits Deception Technology (DT), enables the hunted to give the hunter a taste of their own medicine. RevBits DT is a sophisticated early breach detection and capture system that thwarts external and insider threats. It is the only deception technology on the market with dual-layer virtualization. This distinctive architecture efficiently and effectively deploys large numbers of real honeypots. The dual layer makes it easier to contain attackers, as it is impossible to escape once a honeypot is accessed.

Using real server decoys makes detection between real digital assets and honeypots impossible. A central dashboard allows administrators to configure, manage, and monitor all honeypots across the enterprise network. Rather than simulated or emulated honeypots, RevBits DT uses real honeypot servers, database servers, file servers, network devices, and standard network protocols that can be launched with a single click. Below is a list of twenty different real honeypots RevBits DT includes:

- Apache Tomcat
- SSH/Telnet switches
- Cassandra
- HTTP/HTTPS switches and generic authorization
- Elasticsearch
- Ethernet S7
- FTP
- Generic HTTP/HTTPS with redirection to a server
- LDAP
- RDP
- MongoDB
- Microsoft SQL
- MySQL
- PostgreSQL
- Redis
- Samba
- Modbus
- SNMP
- SMTP
- SSH


RevBits Deception Technology Architecture

- 1 System administrator
- 2 Deploys RevBits Deception Technology honeypots through the RevBits Controller into the network.
- 3 Deployed Honeypots are secured from attacker escape through dual-layered virtualization. All honeypots are real server types - not emulations or simulations.
- 4 Through MSI, RevBits Honeydrop credentials are distributed onto network endpoints and servers so if harvested by an attacker, will point to the network deployed honeypots.
- 5 Critical servers are protected through an early breach detection capability.



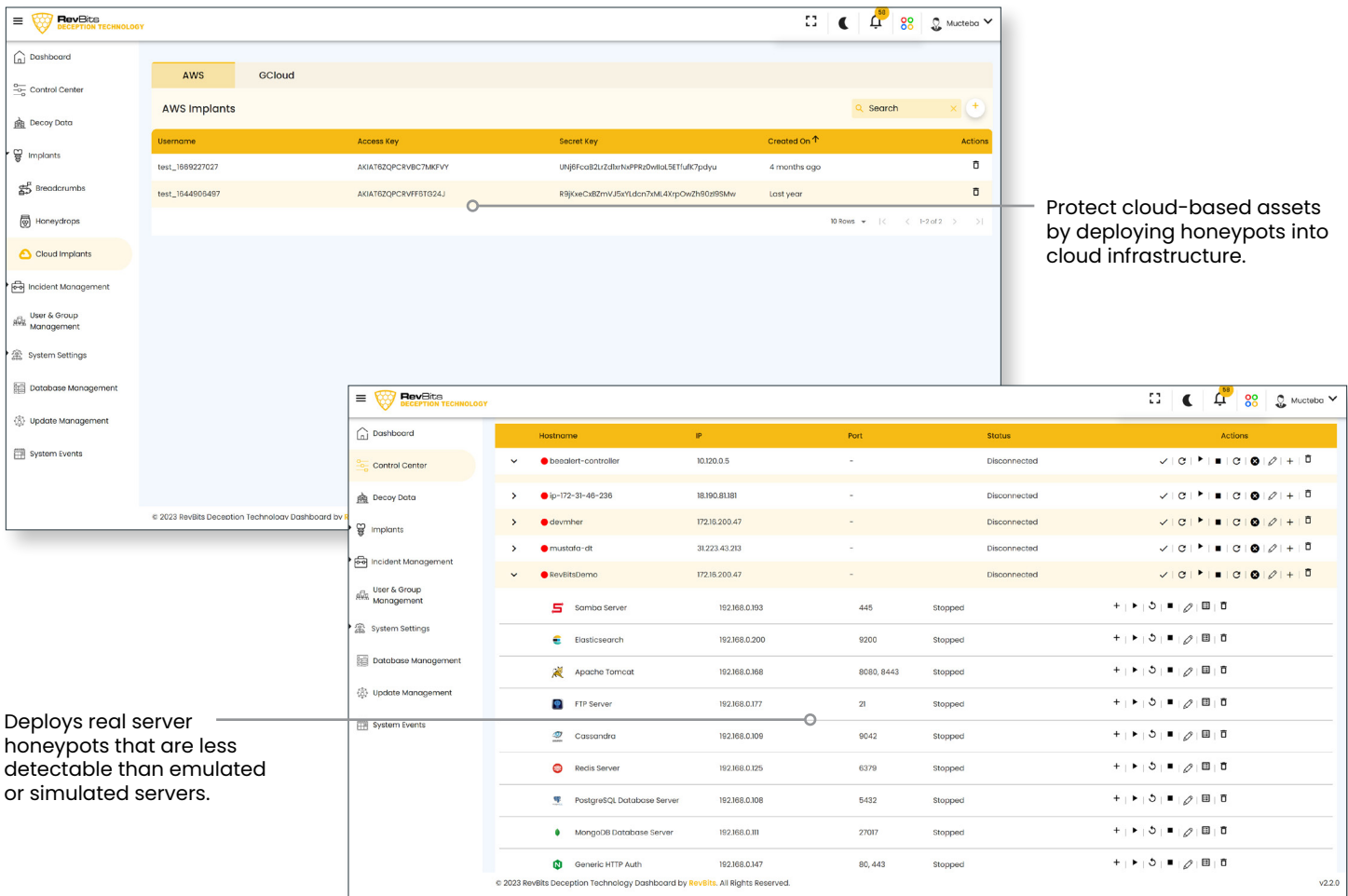
Deploying breadcrumbs to lure attackers

RevBits DT uses the Microsoft Software Installer (MSI) deployment package for Windows endpoints and the .run package for Linux servers to deploy breadcrumbs on endpoints with credentials that point to the honeypot. Breadcrumbs create a false trail that lead attackers to the honeypots. When an attacker hits a honeypot using credentials, the reporting dashboard identifies which honeypot was impacted and the source IP address of the attacker.

RevBits DT dual-layer virtualization

RevBits dual-layer virtualization uses a Controller Virtual Machine (CVM) as the first virtualization layer. Within the CVM, there are sub-VMs with real honeypot servers running inside. Within the second virtual layer, RevBits DT starts and stops the sub-VMS on-demand.





The dashboard is divided into two main sections. The top section, titled 'AWS Implants', shows a table with columns for Username, Access Key, Secret Key, Created On, and Actions. Two entries are visible:

Username	Access Key	Secret Key	Created On	Actions
test_1899227027	AKIA7QZQPCRVBCTMKFVY	UN9Fcoa8ZLzZdheNpPRzDvita5ETlufk7pdyu	4 months ago	[Icon]
test_1844905497	AKIA7QZQPCRVFF9T024J	RjYxwCotB2mVJ5xYtLdcn7ML4XpOwZ90t99Mw	Last year	[Icon]

The bottom section shows a list of honeypots with columns for Hostname, IP, Port, Status, and Actions. The list includes various services like Samba Server, Elasticsearch, Apache Tomcat, FTP Server, Cassandra, Redis Server, PostgreSQL Database Server, MongoDB Database Server, and Generic HTTP Auth.

Protect cloud-based assets by deploying honeypots into cloud infrastructure.

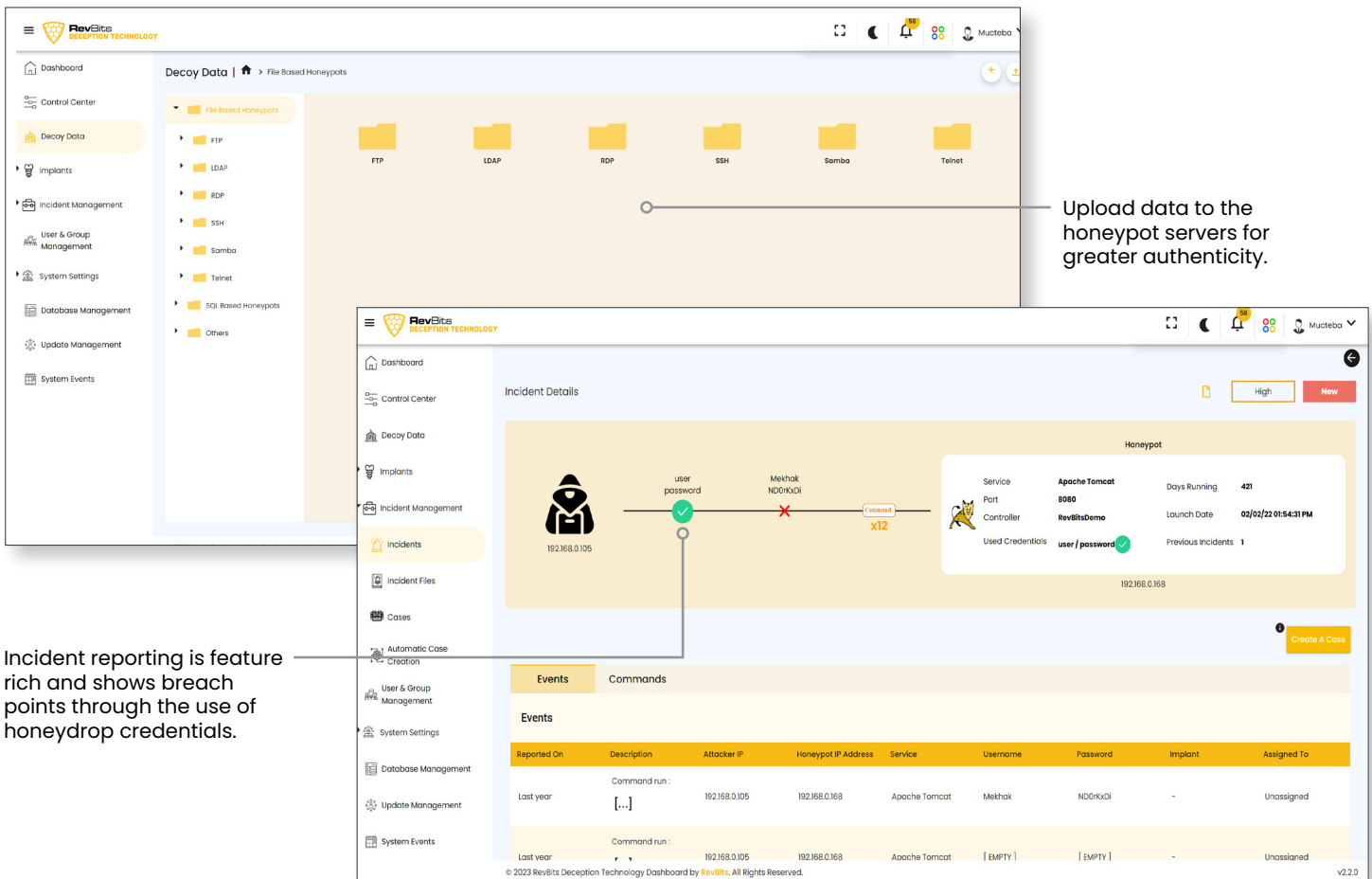
Deploys real server honeypots that are less detectable than emulated or simulated servers.

RevBits DT has 20 different real server honeypots that can be run on a single IP and port for low resource consumption. The operation begins with the CVM communicating with the network router to generate 20 MAC IP addresses to support the 20 honeypots. Each host honeypot the RevBits DT launches is allocated with a single IP, port, VM, and operating system.

Other deception solutions require one VM dedicated to each honeypot, which requires additional resources to maintain ten separate VMs, operating systems, and the added RAM and CPUs. Some deception solutions run a single VM that requires ten ports to support ten honeypots. These solutions don't use real servers; they emulate limited types of servers (e.g., SSH and RDP). This is a flawed approach, as smart attackers will see ten open ports for the same host, which is a telltale sign for hackers. Additionally, because they are only emulating servers, these solutions are limited in their depth of

implementation and the ability to drill down into the attack process. They cannot populate their honeypots with data, usernames, emails, passwords, and other important elements needed to keep attackers engaged.

The more sophisticated the attacker, the more sophisticated must be the honeypots. For deception technology to be effective, it must convince the attacker that the system they are targeting is real. This applies to external and insider threats. The longer a defender can keep an attacker on the honeypot, the more information they can collect on them, and conduct countermeasures. Rather than having the attacker go after the company's real systems, the objective is to convince the attacker that the honeypot is where they want to focus their time and efforts by running commands and querying SQL, FTP, and SMB database tables and users, and trying to export, backup, and download data.



The dashboard is divided into two main sections. The top section, 'Decoy Data', shows a hierarchy of 'File Based Honeyports' including FTP, LDAP, RDP, SSH, Samba, and Telnet. A callout points to this section with the text: 'Upload data to the honeypot servers for greater authenticity.' The bottom section, 'Incident Details', shows a diagram of a breach from attacker IP 192.168.0.105 to honeypot IP 192.168.0.168. A callout points to this section with the text: 'Incident reporting is feature rich and shows breach points through the use of honeydrop credentials.' Below the diagram is a table of events.

Reported On	Description	Attacker IP	Honeypot IP Address	Service	Username	Password	Implant	Assigned To
Last year	Command run: [...]	192.168.0.105	192.168.0.168	Apache Tomcat	Mekhak	ND0hXDi	-	Unassigned
Last year	Command run: [...]	192.168.0.105	192.168.0.168	Apache Tomcat	[EMPTY]	[EMPTY]	-	Unassigned

Advanced threat warning system

An important purpose of deploying deception technology is to have advanced notice of covert and threatening activity before damaging consequences can occur. RevBits DT employs a multi-channel alert system that provides instant notification via SMS, email, and SIEM, and full attack details are delivered to admins as they occur. Even better, alerts can be sent within the RevBits' Cyber Intelligence Platform (CIP) and correlated with other security products for immediate and decisive action across the enterprise security landscape.

The RevBits DT robust and continuous monitoring provides real-time detection, which immediately logs and stores all pertinent event data. It instantly shares the attacker's location, the source of the breach, the

breadcrumb used, and the executed commands. RevBits' Deception Technology is easy to deploy, enabling complex digital honeypot traps to be set up in minutes; from simple firewall honeypots to advanced database server honeypots, with a single click.

The complete quote from Ali includes, "Float like a butterfly, sting like a bee. The hands can't hit what the eyes can't see". Regarding cybersecurity, corporate defenders must be stealthier than their attackers, and their cybersecurity must be nimble while ensnaring their attackers within an inescapable trap. Don't leave your enterprise vulnerable to hit-and-miss attempts to thwart bad actors. Set your cyber-traps with RevBits' award-winning Deception Technology

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