stealthINTERCEPT

# StealthINTERCEPT®

Monitor and prevent threats in real-time

stealthbits

Active Directory is secure when it's clean, understood, configured properly, monitored closely, and controlled tightly. StealthINTERCEPT is a real-time change and access monitoring solution that safeguards your organization against malicious and unintended changes made in Active Directory, File Systems, and Exchange, by providing organizations the operational and security intelligence necessary to achieve these goals—without relying on ineffective native logs.

## Noisy irrelevant data prevents action

For years, organizations have struggled to obtain contextual, actionable intelligence from their critical Microsoft infrastructure to address security, compliance, and operational requirements. Even after pumping SIEM and other log aggregation technologies with every event possible, critical details are lost amidst excessive amounts of noise or are too difficult to interpret for administrators to make heads or tails of what is really happening in their environments. As bad actors continue to leverage more and more sophisticated methods to elude detection, the need for a new way to analyze changes and activities for violation of security and operational policies is paramount to detecting and preventing an inevitable breach.

## Cut through the noise

By intercepting all traffic without any reliance on native logging, StealthINTERCEPT is able to identify authentication-based and file system attacks, monitor usage and abuse of privileged accounts, and detect critical changes made to the environment. Furthermore, StealthINTERCEPT is capable of initiating preventative controls that lock down your most critical assets and actually enforce the written policies. Together, these capabilities help thwart critical elements of credential theft attacks by limiting exposure of administrative credentials across multiple threat vectors. From Enterprise Password Enforcement to LSASS Guardian—DCSync protection to enforcement of ESAE Administrative Forest Designs, StealthINTERCEPT combines cutting-edge enhancements and enforcement of recommended practices to elevate Active Directory security.

### Policy enforcement

Prevent the changes and activities that put your organization at risk.

### Active Directory security

Protect critical objects from unauthorized change or access and prevent credential abuse

### Simplified audit & compliance

Automate the generation of critical compliance artifacts in alignment with industry and regulatory standards

### Empowered SIEM

Correlate threat data providing crucial context about attack techniques and behaviors without the need for native logs

### Preventive controls

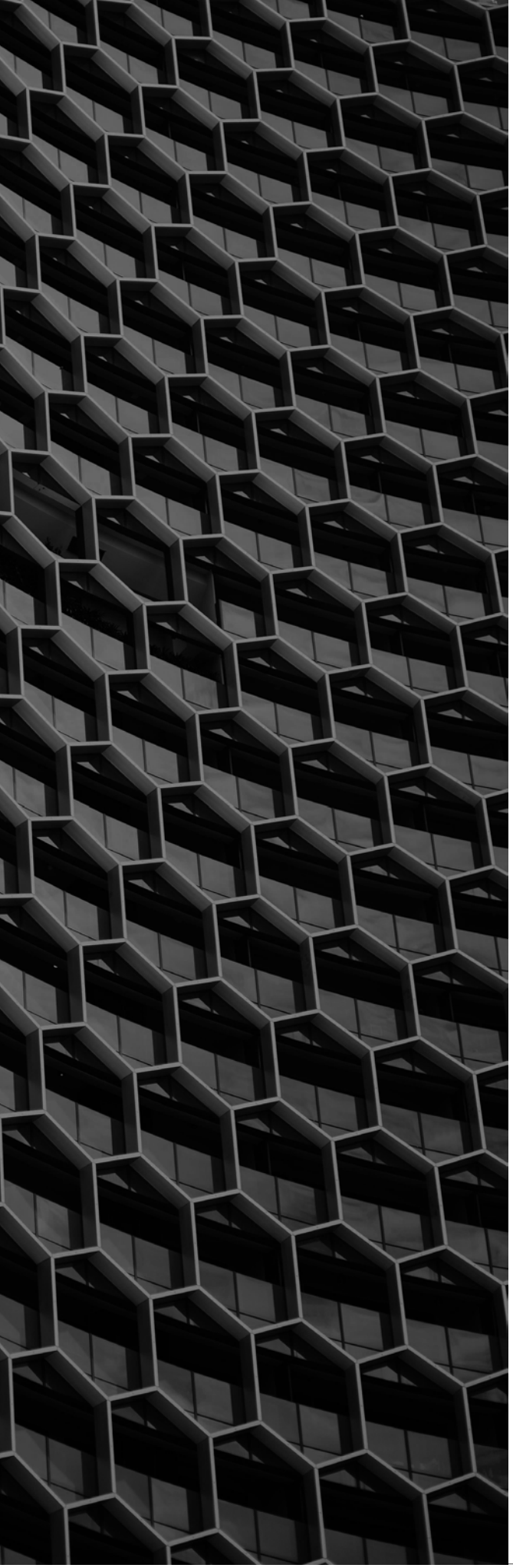
Monitor changes, access, and queries to and against critical objects, attempts to compromise credentials, achieve persistence, and circumvent security controls

### Complete event details

Comprehensive event details for every event improves visibility and context, making data more actionable

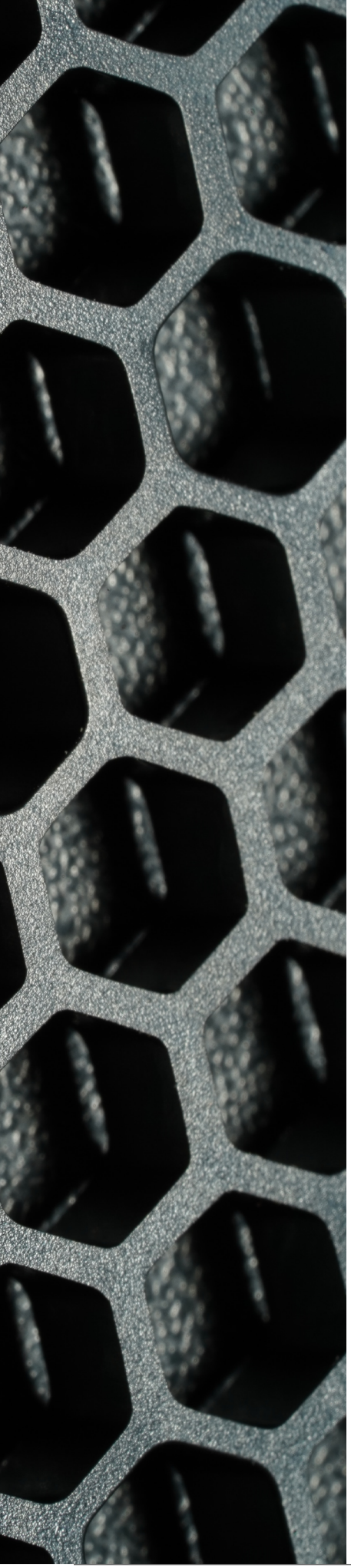
# Features

- **Enterprise Password Enforcement** – Attackers often use dictionaries of previously breached passwords or knowledge of well-known passwords to compromise accounts. To mitigate this risk and the likelihood of generic or known password use within organizations, StealthINTERCEPT has been enhanced to proactively prevent their usage when passwords are set – regardless of whether or not they meet complexity requirements – further enforcing password hygiene and reducing the opportunity for attackers to crack or guess passwords in automated or manual fashions.
- **LSASS Guardian** – Advanced Active Directory attacks like Skeleton Key malware allow an attacker to inject malicious code into the LSASS process, giving attackers the ability to authenticate as any user with a password of their choosing. LSASS Guardian also protects against malicious Windows SSP injections that log locally authenticated credentials, effectively preventing unauthorized injection of code into the LSASS process, protecting Active Directory from total compromise.
- **DCSync Detection & Prevention** – Attackers are increasingly improving their techniques to fly below the radar. Mimikatz DCSync, for example, allows an attacker to impersonate a Domain Controller to pull current and previous password hashes from a DC over the network without requiring interactive logon or gaining direct access to Active Directory's database – the NTDS.dit file. This enhancement to StealthINTERCEPT allows users to detect, prevent, and alert on malicious requests to a Domain Controller, allowing organizations to mitigate the threat of credential compromise using this method of attack.
- **Attack Analytics** – Built-in authentication and file system analytics allow organizations to catch and automatically block internal threats as they're unfolding using customizable, pattern-based detection techniques.
- **Reconnaissance Detection** – Reconnaissance is the first phase of every targeted attack. StealthINTERCEPT's ability to surgically monitor LDAP requests and auditing attribute read events against Active Directory enables real-time detection of suspicious queries and possible reconnaissance activity such as the membership of privileged security groups and the location of sensitive assets.
- **In-line Monitoring** – StealthINTERCEPT eliminates reliance on native logs through in-line monitoring of events. By intercepting event details at the source, organizations get better data, faster, and more efficiently than native logging can provide.





- **Change & Access Prevention** – Add an additional layer of security and control to your Active Directory, File System, and Exchange environments through integrated blocking capabilities at the finest levels, including AD objects and GPOs, authentications, files, and mailboxes.
- **Real-Time Alerting** – StealthINTERCEPT will alert any audience of your choosing to critical events in real-time at global or policy-specific levels.
- **True SIEM Integration** – So much more than just a syslog feed, StealthINTERCEPT provides direct, certified integration with many of the market's leading SIEM technologies, including IBM® QRadar®, Splunk, RSA® Security Analytics, and HP® ArcSight®. Events feed in real-time, formatted and parsed properly out of the box, along with rich pre-packaged dashboards that provide a complete, ready-to-use experience.
- **Dynamic Policies** – Leverage existing security investments to dynamically enrich the context of StealthINTERCEPT policies, such as a list of critical security groups to monitor for membership changes or privileged accounts to monitor for unauthorized authentications.
- **Powerful Investigations** – StealthINTERCEPT's Investigation Grid provides users with easy access to the Who? What? Where? When?™ of any event, including before and after values, complete originating and destination IP Addresses and Host Names, and more. Any investigation can also be saved for one-click viewing in the future from the console or the web.
- **Extensible Actions** – Administrators can save time and add advanced actions using the easy automation and scripting functionality provided by PowerShell, VB, and C#.
- **Role-based Access** – Whether in the console itself or via StealthINTERCEPT Web Reporting interfaces, the controls are there to ensure the right people have access to only the right product components and data, saving time and ensuring security for administrators, auditors, and other data viewers.
- **Integrated Security** – StealthINTERCEPT not only protects your critical assets, but itself as well by generating a tamper-proof audit trail of all activities performed inside the product, hardening deployed agents, and ensuring compatibility with embedded OS security features like FIPS.
- **Integrated Reporting** – From the console or the web, users can take advantage of StealthINTERCEPT's Investigations Grid, Analytics, and Reporting facilities.



# NEXT STEPS

## Schedule a demo
stealthbits.com/demo

## Download a free trial
stealthbits.com/free-trial

## Contact us
info@stealthbits.com

**IDENTIFY THREATS. SECURE DATA. REDUCE RISK.**

Stealthbits Technologies, Inc. is a customer-driven cybersecurity software company focused on protecting an organization's sensitive data and the credentials attackers use to steal that data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, our highly innovative and infinitely flexible platform delivers real protection that reduces security risk, fulfills compliance requirements, and decreases operational expense.



stealthbits