KuppingerCole Report

EXECUTIVE VIEW

by Mike Small | November 2017

STEALTHbits® Products Overview

Securely governing access is increasingly important to ensure compliance as well as to defend against cyber-crime. STEALTHbits' products provide a comprehensive set of solutions to address IT security risks covering Active Directory, Data Access Governance, Privileged Access Management, and Threat Detection.

by **Mike Small**
mike.small@kuppingercole.com
November 2017

Content

Related Research Documents

Leadership Compass: Privilege Management - 72330

Advisory Note: KRIs and KPI for Access Governance - 72559

Advisory Note: Enterprise Role Management - 70285

Advisory Note: Access Governance Architectures - 71039

Advisory Note: Entitlement & Access Governance - 71109

Advisory Note: Working to the Business not the Auditors - 70865

Advisory Note: Sustainable Infrastructures through IT Compliance - 72025

Leadership Compass: Identity as a Service: Single Sign-On to the Cloud (IDaaS SSO) - 71141

Leadership Compass: Identity as a Service: Cloud-based Provisioning, Access Governance and Federation (IDaaS B2E) - 70319

1 Introduction

Access Governance concerns the processes and technologies for the management of access controls in IT systems. Its objectives are to ensure legitimate access to resources and data while managing the risks of illegitimate access. These risks include the theft of information, fraud through alteration of systems or data, and the subversion of IT systems (through ransomware for example). The large number of reported incidents over the last twelve months shows the need to address these issues.

Access Governance is increasingly important to manage the cyber-risks related to organizational IT systems. These risks extend beyond misuse and mistakes by insiders with legitimate access, to external cyber-attacks that often use apparently legitimate access credentials to bypass the many layers of network defences are now generally implemented by organizations. Often, the first sign that a cyber-attack is in progress is abnormal activity by a legitimate user's account.

In addition to managing cyber risks, Access Governance is also relevant to regulatory compliance. For many industries, there are regulations that define how certain kinds of data must be acquired, stored, used and protected. These regulations range from those relating to the financial reporting of publicly listed companies, through pharmaceuticals and healthcare to manufacturing and public utilities. On top of this, the increasing number of privacy laws worldwide require stringent controls over how Personally Identifiable Information (PII) is collected and used. This brings not only CRM systems within the scope of Access Governance but also potentially Customer Identity and Access Management (CIAM) used by the organizations customers. Access Governance not only ensures compliance but also provides the evidence needed to prove compliance.

Access Governance uses a range of tools and techniques that covers several areas. KuppingerCole Advisory Note 72559[1], provides some Key Risk Indicators (KRI) to help organization manage and improve their approach to Access Governance. Access Governance covers:

- Classification of applications and information
- Identity Lifecyle Management
- Access Management
- Identity and Access Monitoring

Organizations should implement access governance processes using appropriate tools to cover these areas.

2 Product Description

STEALTHbits Technologies is a privately held software company with its head office in Hawthorne NJ in the USA. The company is focused on protecting organizational credentials and data. Its products focus on removing inappropriate data access, enforcing security policy, and detecting cyber threats to reduce security risk, to fulfil compliance requirements and to decrease operational costs.

[1] **Advisory Note: KRIs and KPI for Access Governance - 72559**

This report covers STEALTHbits' suite of products designed to address IT security risks, compliance requirements, and day-to-day management functions spanning Data Access Governance, Active Directory Management & Security, and Threat Detection.

2.1 STEALTHbits Products Overview

STEALTHbits provides several products to support credential and data security processes for a range of environments. The products include:

- StealthAUDIT®: Automated data collection, analysis, and governance
- STEALTHbits File Activity Monitor: monitors and stores file activity
- StealthDEFEND®: Real-time alerting and behavioural analytics
- StealthINTERCEPT®: Real-time policy enforcement and change monitoring
- StealthRECOVER®: Rollback and recovery of unwanted Active Directory changes

2.2 StealthAUDIT®

StealthAUDIT which is STEALTHbits' flagship product, is a platform designed to automate data collection, analysis, remediation, governance, and reporting tasks associated with the management and security of credentials and data. When applied to the various technologies StealthAUDIT supports (which include: Windows, NAS, and Unix File Systems, SharePoint, Office 365, Box, Dropbox, Active Directory, Exchange, SQL, Windows and Unix Operating Systems, etc.), it enables organizations to discover and remediate security risks at scale.

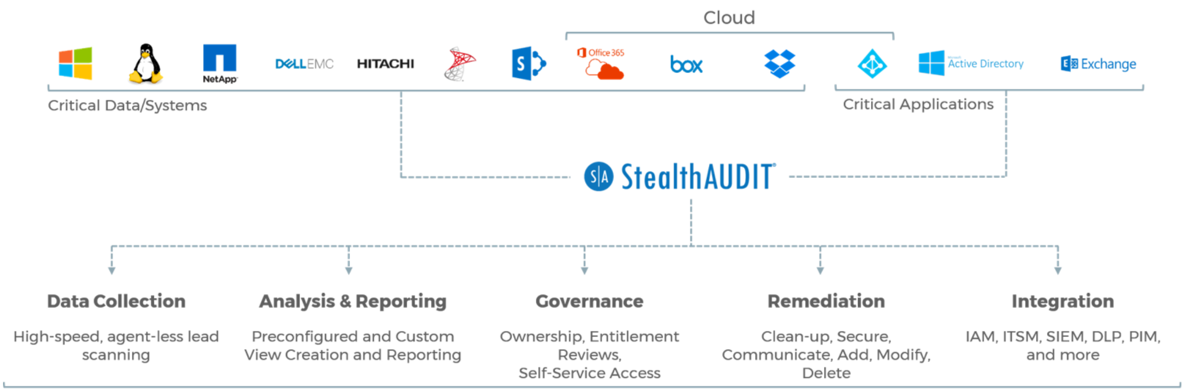
Cloud
NetApp
DELL EMC
HITACHI
Office 365
box
Active Directory
Exchange
Critical Data/Systems
Critical Applications
StealthAUDIT
Data Collection
High-speed, agent-less lead scanning
Analysis & Reporting
Preconfigured and Custom View Creation and Reporting
Governance
Ownership, Entitlement Reviews, Self-Service Access
Remediation
Clean-up, Secure, Communicate, Add, Modify, Delete
Integration
IAM, ITSM, SIEM, DLP, PIM, and more

Figure 1: StealthAUDIT Overview (Graphic reproduced with permission from STEALTHbits)

StealthAUDIT is most often leveraged for its Data Access Governance capabilities, focused on unstructured data sources. The following describes a typical campaign using the product:

- Beginning with an upfront discovery, StealthAUDIT discovers where data exists across an organization's IT infrastructure, establishing a baseline for more focused collection and analysis routines to follow.
- Once a baseline has been established for targeted scans, StealthAUDIT collects unstructured data access authorizations, permissions, file metadata and activity, examines file contents for sensitive information, and analyzes it all to begin the process of determining how to secure the data optimally.

- With a dataset containing the information needed to provision access rights in alignment with Least Privilege Access principles, StealthAUDIT automatically adjusts how access is granted to the data and assigns the role of controlling access to the data to the individuals responsible for it.
- With ownership in place and a security model that allows for control over who has access and at what permission level, StealthAUDIT instantiates automated workflows such as periodic entitlement reviews and self-service access requests for ongoing governance.

Additional items of note:

- StealthAUDIT scans the contents of a wide range of file types, including image files using Optical Character Recognition (OCR) technology. It provides out-of-the-box rules for several government and industry compliance standards together with the ability to add custom criteria specific to an organization's standards.
- StealthAUDIT can read and write file classification tags to enhance governance and increase the effectiveness of other security tools such as encryption or data-in-motion.
- StealthAUDIT is also leveraged by many organization to extend unstructured data entitlements into their Identity & Access Management (IAM) programs, providing certified integration with many of the market's leading IAM providers.
- StealthAUDIT's file activity monitoring module can be purchased as a stand-alone tool for organizations desiring file activity monitoring capabilities.

2.3 STEALTHbits File Activity Monitor

The STEALTHbits File Activity Monitor is a solution that monitors and stores file activity for NAS (NetApp, EMC, Hitachi) and Windows devices. The solution is designed to provide users with the ability to:

- Query all file activity for specific values or combinations of values;
- View query results executed against your data in a clean, simple UI grid;
- Feed file activity data to alternative technologies like SIEM (Splunk and QRadar) and/or export data in easy-to-understand end use formats;
- Analyze data feed into SIEM to gain insight into overall file activity, deletions, modifications, critical permission changes, and file system attacks like ransomware.

2.4 StealthDEFEND

StealthDEFEND is the real-time threat analytics component of STEALTHbits' Data Access Governance Suite. Leveraging unsupervised Machine Learning, StealthDEFEND eliminates excessive and undifferentiated warnings to surface meaningful trends and alerts on attempts to compromise sensitive data.

Incorporating file activity details in conjunction with the context of each file's sensitivity, StealthDEFEND aims to highlight abnormal behaviors that are likely to be Indicators of Compromise (IOCs) such as:

- Crypto Ransomware
- First-time access to data resources
- Unusual sensitive data access
- Abnormal denied activity

- Suspicious permission changes
- Data exfiltration attempts
- Unusual process execution
- Configuration file tampering
- Mass file deletions

2.5 StealthINTERCEPT®

StealthINTERCEPT helps organizations to monitor the usage of credentials and data, as well as enforce security policy in real-time.   Through visibility into every change and access activity across unstructured data repositories and critical applications, StealthINTERCEPT detects and analyses suspicious behaviours, proactively prevents changes and access, alerts, and integrates directly with the market's leading SIEM platforms, all without any reliance on native logging.

2.6 StealthRECOVER™

As part of STEALTHbits' Active Directory solution portfolio, StealthRECOVER enables organizations to rollback and recover unintended directory changes. It enables point in time rollback and recovery of AD objects, attributes, group memberships, DNS, state of accounts, and more; without downtime. It provides the functionality needed to browse multiple snapshots and leverage full text search to rollback and recover only those aspects that are required.

3 Strengths and Challenges

STEALTHbits products provide a comprehensive set of solutions to address IT security risks covering Active Directory, Data Access Governance, Privileged Access Management (PAM), and Threat Detection. The products provide support for some Access Governance processes and will be of interest to organizations using Microsoft Active Directory as the primary repository for entitlements.

Understanding who has access to what is the foundation for access governance. The products provide a detailed analysis of the permissions in Microsoft Active Directory and how they've been facilitated through Microsoft Active Directory user and group assignments. This includes coverage of Windows, NAS, and Unix file shares, SharePoint, cloud storage repositories, as well as structured data sources like Microsoft SQL databases.   This can help organizations to identify which resources are open for access and may be subject to excessive risks.

It enables the discovery of changes to permissions and in particular provides auditing of administrator activities, including local administrators. This is especially important since many external threats involve taking control over administrative accounts in addition to the threat of abuse by insiders with administrative privileges.

You can only protect what you know you have. The products can discover sensitive data held on file share, SharePoint and Office 365. This enables organizations to identify information assets at risk and then take appropriate action to protect these.

Monitoring user activity is also increasingly important. Often the first sign of a cyber-attack is abnormal user behaviour. The products include User Behaviour Analytics (UBA) that exploits machine learning to enable the detection of abnormal user activities while ensuring a low level of false alarms. There is also integration with leading SIEM products out of the box.

Ensuring that users entitlements match the needs of their jobs while ensure that organizational policies are met is a key capability of Access Governance. The product does not provide some necessary functionalities out of the box; for example, it does not include segregation of duties (SoD) analyses or role mining to identify the actual access permissions being used for specific jobs.

Managing the processes for requesting and managing changes to users and entitlements is also important. The STEALTHbits products integrate with IAM frameworks from leading product vendors as well as home grown tools for request management, provisioning and access recertification.

Strengths	Challenges
● Comprehensive functionality for organizations using Microsoft Active Directory; ● Provides detailed analysis of permissions across multiple resources, including File Shares, SharePoint Sites, and Active Directory objects. ● Covers a wide range of file systems including *nx as well as Windows; ● Discovery of sensitive information and file changes; ● Integration with leading IAM frameworks and in house provisioning systems; ● Includes activity monitoring with UBA functionality; ● Capabilities to roll back Active Directory changes.	● Lacks functionality for segregation of duties management; ● Lacks role mining functionality.

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

Kuppinger Cole Ltd.
Sonnenberger Strasse 16
65193 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com