



Market Insight Report Reprint

Coverage Initiation: Semperis helps fend off the growing threat of Active Directory attacks

September 2 2021

Garrett Bekker

The company has come to market with several products that that help detect, protect and recover from attacks against Microsoft's Active Directory and Azure AD, or what it calls 'identity driven' cyber resilience. Recent release Purple Knight is a free security assessment tool that lets firms identify any potential weaknesses or misconfigurations in AD, and take action to remediate them.

451 Research

S&P Global

Market Intelligence

This report, licensed to Semperis, developed and as provided by S&P Global Market Intelligence (S&P), was published as part of S&P's syndicated market insight subscription service. It shall be owned in its entirety by S&P. This report is solely intended for use by the recipient and may not be reproduced or re-posted, in whole or in part, by the recipient without express permission from S&P.

Introduction

It's no surprise that directory services, particularly Microsoft's Active Directory (AD), have become a prime target for attackers. Since AD is rarely safeguarded effectively, attackers have come to depend on weak configurations to identify attack paths, access privileged credentials, and get a foothold into target networks.

To address some of these challenges, Semperis has come to market with several products that provide what it calls 'identity driven' cyber resilience that can help detect, protect and recover from attacks against AD (and Azure AD) across hybrid environments. The newly released Purple Knight is a free security assessment tool that essentially lets firms get a handle on the security status of their AD estate (Kerberos, Group Policy, AD delegation, etc.), identify any potential weaknesses or misconfigurations, and take action to remediate them.

THE 451 TAKE

The pertinent question isn't 'why is AD security necessary,' but rather 'why has it taken so long to become such a big problem?' Certainly the acceleration in ransomware and the heightened publicity it has garnered has given a boost to what has effectively become a small, but rapidly growing, market focused specifically on protecting AD, which is effectively the central nervous system of most firms' IT estate and increasingly the target of ransomware attacks. Although there are other directory services available, Semperis remains focused primarily on AD and Azure AD (for now), and the security capabilities offered by Microsoft may be good enough for some organizations. In a highly fragmented security market comprised of products that are essentially missing features, we ultimately see AD security as a market likely to be subsumed within broader IAM offerings over time, and thus many of the vendors in the space could be acquisition targets.

Context

Directory services sit at the heart of most firms' IT strategies, and as such they have become mission-critical assets that can present dire consequences if compromised – as we have learned from the now infamous SolarWinds supply-chain attack, and the Hafnium attack on Microsoft Exchange.

The vital nature of directories has been further magnified by the ongoing migration of resources to the cloud, since each 'cloud' – whether IaaS platform or SaaS app – typically has its own identity repository that applications need to work with. Maintaining directories in a secure state has therefore become a considerable challenge, in part because most directories are constantly in flux as new users are added or change jobs, and new applications are installed.

Hoboken, New Jersey-based Semperis was founded in 2015. The company has roughly 200 full-time employees with additional offices in Ramat Gan, Israel. Semperis has raised a total of \$54m in venture capital from multiple investors, most recently a \$40m series B round in 2020 led by Insight Partners.

The company has devoted much of the past year to strengthening its executive team with industry veterans and practitioners such as E&Y veteran Jim Doggett as CISO, Dell EMC veteran Coley Burke as CRO, Bank of America VP of global information security Igor Baikalov as Chief Scientist, and former HPE Chief Technologist Guido Grillenmeier as Chief Technologist.

Products

Semperis offers two products: Directory Services Protector (DSP) and Active Directory Forest Recovery (ADFR), both of which now operate on both AD and Azure AD (for brevity, we will use AD to refer to both). DSP does security assessments, threat protection, monitoring and response for Active Directory to help detect and stop lateral movement and privilege escalation. Among its various features is the ability to discover insecure configurations and settings and monitor for pre-attack and post-attack indicators for weaknesses in an organization's AD security posture, with real-time tracking and alerting on changes to sensitive objects and attributes stored in AD.

DSP can also provide automated rollback capabilities to any point in time and logs any changes to accounts. The latest version of DSP added DSP Intelligence, which provides the ability to continuously scan a firm's AD environment for vulnerabilities and run tests against known attacks from attack frameworks like MITRE ATT&CK. For organizations that operate both on-premises and in the cloud, Semperis now offers DSP for Azure AD that provides visibility across the hybrid identity system.

ADFR was initially conceived as a disaster recovery tool that can restore AD forests to the latest backup, even if the backup was infected with malware, via the (patented) ability to abstract AD from the underlying OS and thus prevent OS-level reinfection. For that reason, ADFR has evolved into a ransomware recovery tool for AD. It can also auto-recover an entire AD forest and perform 'stress testing' of AD backups. The most recent update added unique encryption keys for backup sets, support for SAML, and multifactor authentication and advanced forensics search. ADFR can also provide post-attack forensics to help firms understand how attackers broke in and how to close remaining backdoors.

Purple Knight is a free security assessment tool that interrogates a firm's AD posture and produces a graphical report with a score based on 76 pre- and post-attack indicators across multiple categories. It also provides remediation guidance – essentially security posture management for AD.

Purple Knight maps to five key areas of AD security posture, including account delegation and the security of accounts, AD infrastructure, Group Policy and Kerberos, and can also correlate to security frameworks such as MITRE ATT&CK and others. The analysis generates reports and a risk score that can be used as a starting point for remediation. Identified risks can range from inappropriate Kerberos delegation or accounts with unnecessary elevated privileges to more recent AD and Windows-specific threats such as ZeroLogon, PrintNightmare and PetitPotam.

Semperis also provides extensive support, with access to AD security and incident response experts who can do in-depth security assessments and help with pre- and post-attack AD investigations.

Strategy

Semperis operates globally with a large presence in Europe, and currently has a mix of both large (400,000 FTEs) and small to medium-sized (5,000 FTEs) customers, particularly those challenged by legacy AD implementations and complex hybrid identity environments. Initially, Semperis was focused on primarily on-premises versions of AD, but it recently extended to the cloud by addressing Azure Active Directory (AAD), at first with the ability to track changes to AAD and analyze them in real time, and now with the ability to address pre-attack indicators that may lead to privilege escalation.

In hybrid environments, Semperis can display a single view of indicators of exposure (IOEs) and indicators of compromise (IOCs) in both AD and AAD – for example, monitoring for changes to privileged AAD role membership in the last seven days or additions to AAD privileged roles of non-privileged AD users. Looking ahead, we anticipate Semperis will address security for all major directories across hybrid and multicloud environments.

Competition

Thanks to the growth of attacks directly targeting directory services, AD security has evolved into somewhat of a cottage industry, with several new entrants entering the mix, alongside established security vendors that have added AD security to their arsenal. Aorato (acquired by Microsoft in 2014) was an early AD security specialist, with its Directory Services Application Firewall that essentially employed user behavior analytics to look for anomalous activity around AD.

Alsid (recently acquired by Tenable Security for \$98m) enables the analysis of exposures and the mitigation of threats to AD systems. Attivo recently released AD Assessor, which looks for vulnerabilities in AD and other directories that would let an attacker compromise a domain controller, and also provides a risk score that lays out what areas are vulnerable. SpecterOps has developed a new product that does attack path analysis to help mitigate misconfigurations in AD.

To the extent that Semperis can help mitigate lateral movement that often leads to privilege escalation, it could overlap somewhat with privileged access management vendors, some of which have AD security capabilities, including Quest's AD Recovery Manager, which is arguably Semperis' main competition, as well as Stealthbits (now part of Netwrix).

SWOT Analysis

| | |
|--|--|
| <p>STRENGTHS</p> <p>The company has a broad and experienced management team and technical incident response staff. It is able to protect AD and AAD across the entire directory attack lifecycle with continuous security assessment and configuration assurance, change tracking and rollback, autonomous threat protection and response, full forest recovery, and post-breach forensics.</p> | <p>WEAKNESSES</p> <p>Although most large firms still maintain on-premises AD instances – and may well do so for the foreseeable future – there are other directories that Semperis does not yet address, some of which are legacy LDAP-based directories that are nearing end of life.</p> |
| <p>OPPORTUNITIES</p> <p>Directories are arguably the central nervous system of many firms' IT estate, and the rise in attacks that target directory systems – including ransomware – has fueled substantial interest in tools that can help protect them.</p> | <p>THREATS</p> <p>Vendors in adjacent categories such as endpoint detection and response (EDR) and IAM are already being attracted to the AD security opportunity, and will likely join the party. Microsoft offers some security features for AD that may be 'good enough' for some firms.</p> |

CONTACTS

The Americas

+1 877 863 1306

market.intelligence@spglobal.com

Europe, Middle East & Africa

+44 20 7176 1234

market.intelligence@spglobal.com

Asia-Pacific

+852 2533 3565

market.intelligence@spglobal.com

www.spglobal.com/marketintelligence

Copyright © 2021 by S&P Global Market Intelligence, a division of S&P Global Inc. All rights reserved.

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively, S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers, (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global Market Intelligence does not endorse companies, technologies, products, services, or solutions.

S&P Global keeps certain activities of its divisions separate from each other in order to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain non-public information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its websites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.