IDENTITLEX PRODUCT BRIEF

Attivo NETWORKS
A SentinelOne Company

Organizations are adopting public cloud infrastructures at a significant pace that accelerates every year. With this growth comes unanticipated security challenges in the public cloud with user identity management and the explosion in "non-human" identities, such as applications, virtual machines, containers, serverless functions, and other objects. They must also comply with any regulatory requirements. Attackers can take advantage of these entitlements to access workloads and data within the cloud and leverage it to compromise the enterprise network.

The Attivo Networks IDEntitleX solution provides security teams with a unified view of identities and exposures across the organization to address provisioning management challenges while maintaining operational effectiveness.

OVERVIEW

In a typical network setting, user accounts are the principal identity and, therefore, the primary security focus. In the cloud, however, non-human identities also routinely have entitlements to other resources, resulting in a significant expansion of identities and entitlements the organization must manage. Gartner, Inc. estimates that 75% of security failures will result from inadequate management of identities, access, and privileges within the next few years, up from 50% in 2020[1].

The growing number of identities and entitlements within the cloud substantially increases risks related to:

- Complexity: The quantity of identities and entitlements in the public cloud introduces new levels of complexity. Instead of managing hundreds of identities, there may now be thousands.
- Privileged access: Many organizations use traditional identity management techniques in the cloud, which provide static and long-standing access and therefore increased risk.
- Excessive access: Identities often get granted more access to resources than they need and use, which adds unnecessary risk.
- Widespread access: Many customers synchronize Active Directory identities with the cloud. An exposure on an endpoint can inadvertently translate into a cloud breach.
- Limited risk assessment: The nature of the public cloud makes it hard to have consistent and comprehensive views throughout the environment, making it difficult to assess risk accurately.
- Limited visibility: Each platform has its own user interface, making it difficult to get a complete picture from a single pane of glass. Other CIEM providers also do not typically cover Active Directory attack paths and risks.
- Transient cloud access: The dynamic nature of the cloud makes it hard for traditional security tools to track access properly and provide accountability.

1 Gartner Research — Managing Privileged Access in Cloud Infrastructure Published 9 June 2020 - ID G00720361 - by Analyst Paul Mezzera

© 2022 Attivo Networks. All rights reserved.

BENEFITS

- Visibility to identity entitlement across multi-cloud environments
- Visibility to users, groups, and applications by risk
- Visibility to attack paths and identity exposures visually mapped from on-premises to Active Directory and cloud environments
- Detection for identity privilege escalation across cloud environments
- Easy management for on-premises and cloud environments

GAPS

Traditional IGA and PAM solutions are costly and struggle to address the unique security challenges with the cloud's granular and dynamic nature. Existing cloud security CSPM, CWPP, and CASB tools address specific aspects of cloud infrastructure security, but they generally lack identity and access controls. Manual methods to ensure a least-privilege approach to security do not scale in an environment with so many identities and entitlements. Existing security paradigms cannot inherently combat the new wave of identity security.

The Attivo Networks IDEntitleX solution provides these capabilities.

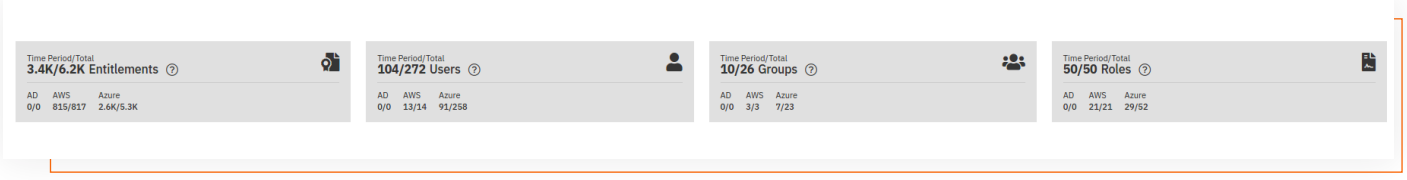
PROTECTING IDENTITIES WITH THE IDENTITLEX SOLUTION

The IDEntitleX solution plays a critical role in giving visibility and reducing the attack surface for identities and entitlements in the cloud.

The solution addresses many cloud permissions management gaps and:

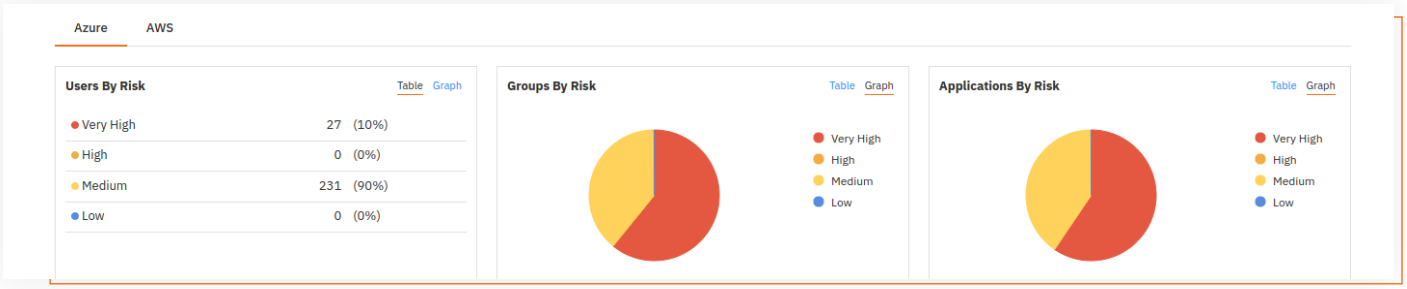
- Scales to discover all identities, resources, and entitlements
- Supports multiple clouds in a consistent fashion
- Tracks changes to entitlements over time
- Provides end-to-end visibility, analysis, and protection: from endpoint to Active Directory to the cloud
- Visualizes entitlements and risks from multiple points of view: identities, roles, and resources alike
- Enables clear and straightforward action to mitigate risk

With the IDEntitleX solution, Attivo provides end-to-end visibility for identities and entitlements from an easy-to-use dashboard that seamlessly integrates data and clarifies findings.

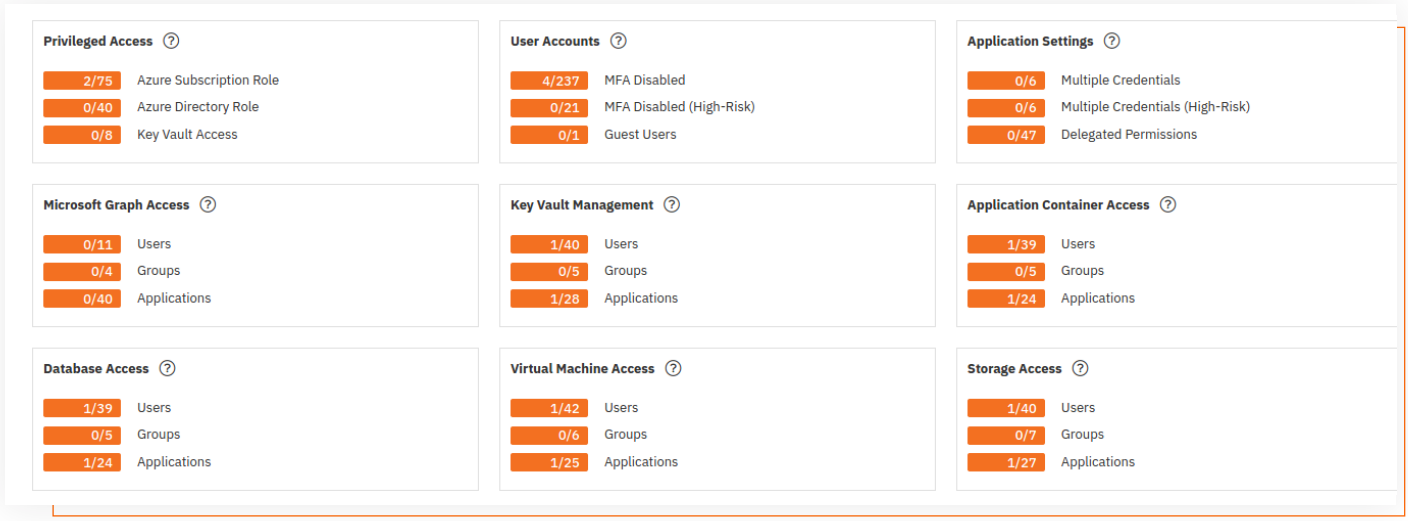


Summarize cross-platform and per-platform identity and entitlement counts

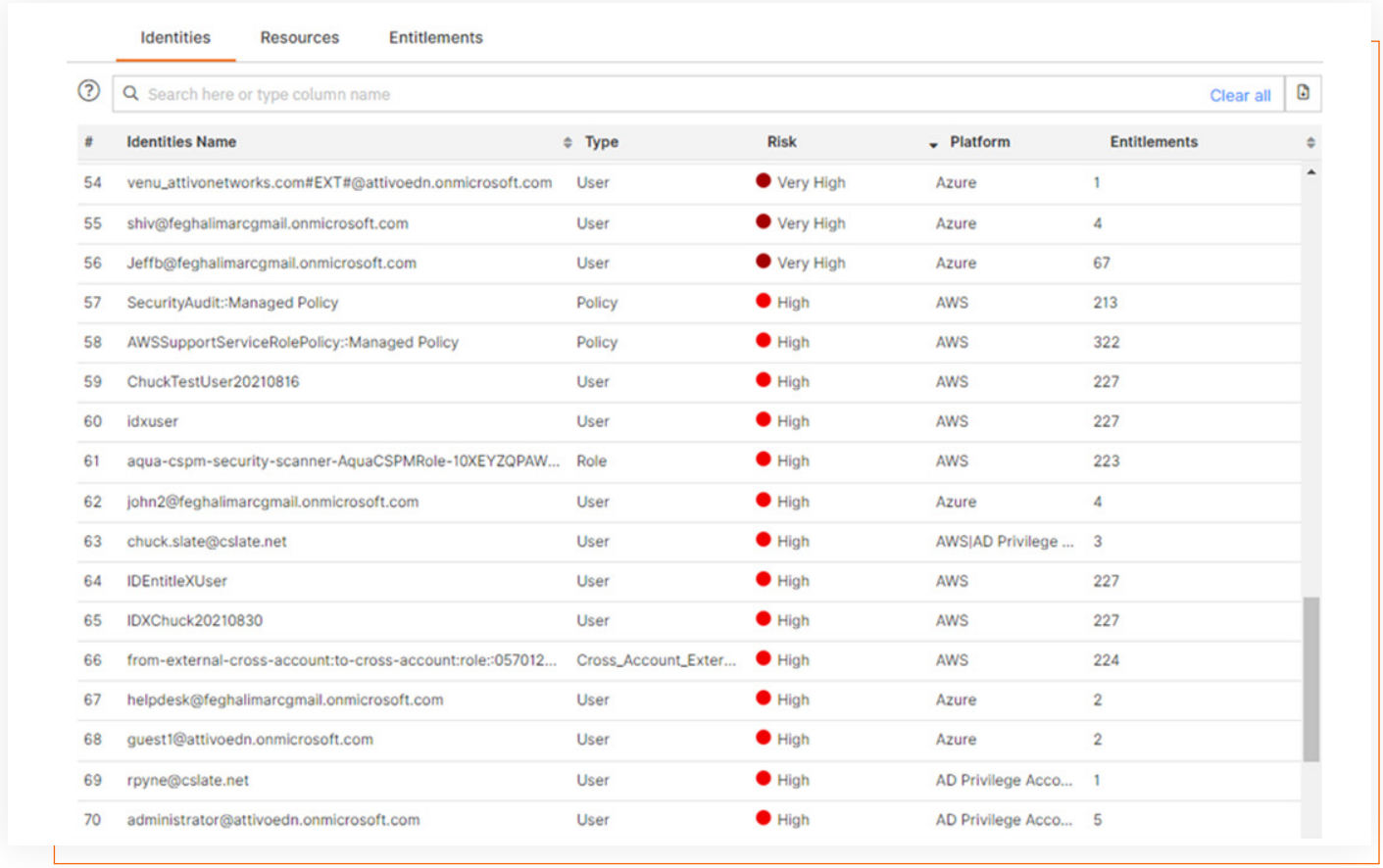
© 2022 Attivo Networks. All rights reserved.



Assess risk per platform and identity type



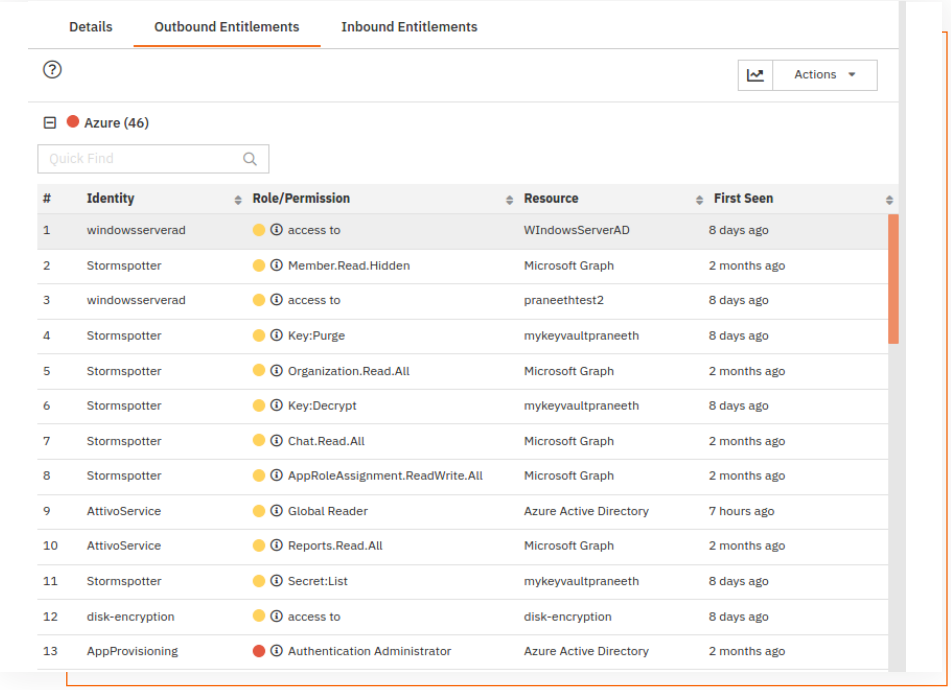
Monitor privileged identities and access to critical services



#	Identities Name	Type	Risk	Platform	Entitlements
54	venu_attivonetworks.com#EXT#@attivoedn.onmicrosoft.com	User	Very High	Azure	1
55	shiv@feghalimarcgmail.onmicrosoft.com	User	Very High	Azure	4
56	Jeffb@feghalimarcgmail.onmicrosoft.com	User	Very High	Azure	67
57	SecurityAudit::Managed Policy	Policy	High	AWS	213
58	AWSSupportServiceRolePolicy::Managed Policy	Policy	High	AWS	322
59	ChuckTestUser20210816	User	High	AWS	227
60	idxuser	User	High	AWS	227
61	aqua-cspm-security-scanner-AquaCSPMRole-10XEYZQPAW...	Role	High	AWS	223
62	john2@feghalimarcgmail.onmicrosoft.com	User	High	Azure	4
63	chuck.slate@cslate.net	User	High	AWS|AD Privilege ...	3
64	IDEntitleXUser	User	High	AWS	227
65	IDXChuck20210830	User	High	AWS	227
66	from-external-cross-account:to-cross-account:role::057012...	Cross_Account_Exter...	High	AWS	224
67	helpdesk@feghalimarcgmail.onmicrosoft.com	User	High	Azure	2
68	guest1@attivoedn.onmicrosoft.com	User	High	Azure	2
69	rpyne@cslate.net	User	High	AD Privilege Acco...	1
70	administrator@attivoedn.onmicrosoft.com	User	High	AD Privilege Acco...	5

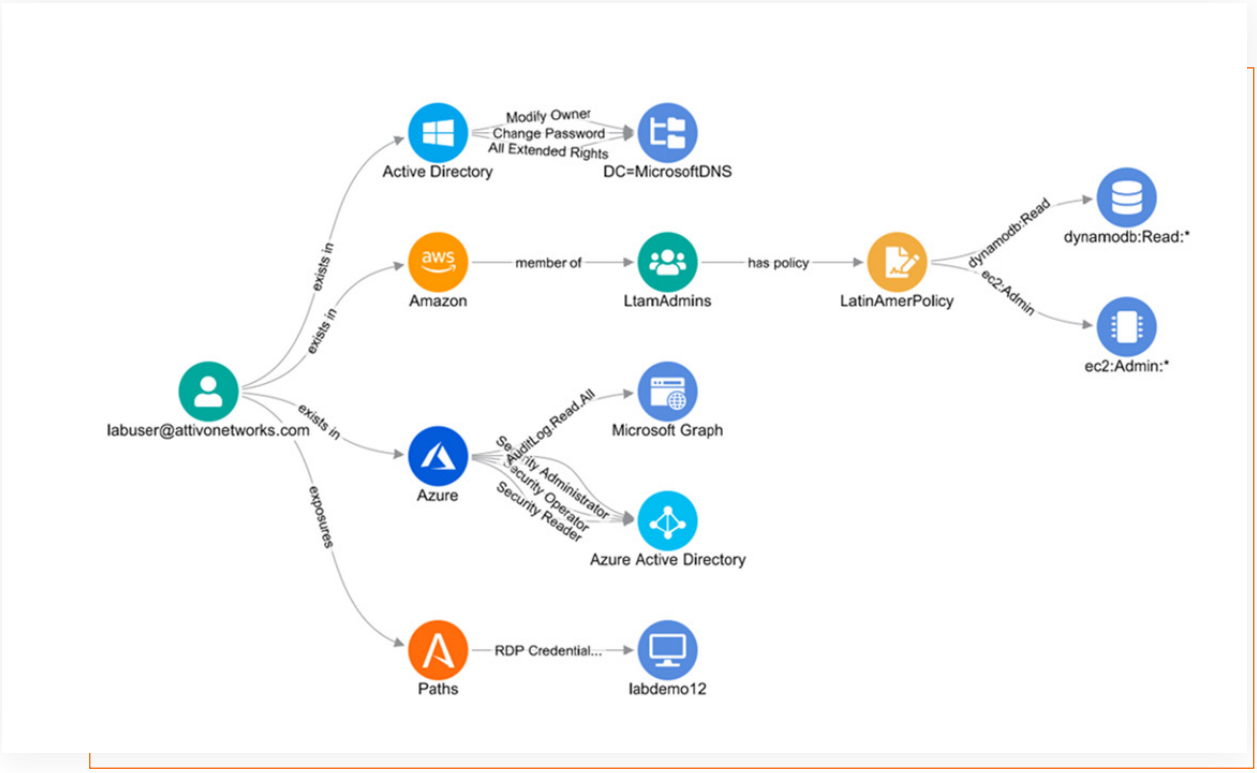
Isolate identities, resources, and entitlements by risk, type, platform, and number of entitlements

© 2022 Attivo Networks. All rights reserved.



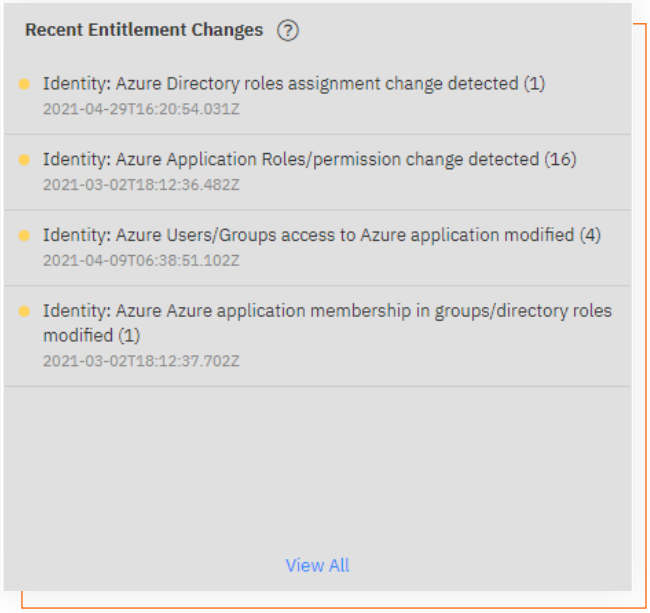
#	Identity	Role/Permission	Resource	First Seen
1	windowsserverad	access to	WIndowsServerAD	8 days ago
2	Stormspotter	Member.Read.Hidden	Microsoft Graph	2 months ago
3	windowsserverad	access to	praneethtest2	8 days ago
4	Stormspotter	Key:Purge	mykeyvaultpraneeth	8 days ago
5	Stormspotter	Organization.Read.All	Microsoft Graph	2 months ago
6	Stormspotter	Key:Decrypt	mykeyvaultpraneeth	8 days ago
7	Stormspotter	Chat.Read.All	Microsoft Graph	2 months ago
8	Stormspotter	AppRoleAssignment.ReadWrite.All	Microsoft Graph	2 months ago
9	AttivoService	Global Reader	Azure Active Directory	7 hours ago
10	AttivoService	Reports.Read.All	Microsoft Graph	2 months ago
11	Stormspotter	Secret:List	mykeyvaultpraneeth	8 days ago
12	disk-encryption	access to	disk-encryption	8 days ago
13	AppProvisioning	Authentication Administrator	Azure Active Directory	2 months ago

Investigate identity-specific entitlements, their risks, and assignment details



Visualize the whole relationship between an identity & its resources

© 2022 Attivo Networks. All rights reserved.



Track entitlement changes to critical identities & resources over time

CONCLUSION

As organizations continue to adopt cloud infrastructure at an ever-increasing rate and identities expand to match, CISOs should focus on identity-first security solutions that can keep pace with this growth.

The Attivo Networks IDEntitleX is a solution of choice for organizations seeking breadth and visibility depth to identity-based issues across the entire enterprise, whether on-premises at the endpoints, within Active Directory, remote sites, or in the cloud.

ABOUT ATTIVO NETWORKS

Attivo Networks®, a SentinelOne company, provides Identity Threat Detection and Response (ITDR) and cyber deception solutions for protecting against identity compromise, privilege escalation, and lateral movement attacks. Through data cloaking, misdirection, and cyber deception, the platform efficiently prevents attacks across Active Directory, cloud environments, and devices.

© 2022 Attivo Networks. All rights reserved.