IS Decisions®

USERLOCK

Secure access to your Windows
Network and Cloud Applications

WHO ARE WE?

IS Decisions makes it easy to manage and secure access to your Microsoft Windows Active Directory and Cloud Environments.

TRUST AND CONFIDENCE IN **IS DECISIONS**

PROVEN IT SECURITY SOLUTIONS

Used by some of the most regulated and security-conscious organizations.

FOR ALL SECTORS, REGARDLESS OF SIZE

Over 3,400 customers from 129 countries.

COST-EFFECTIVE CYBER RESILIENCE

Accurate and affordable security that reduces the risk of breaches and compliance fines.

DEPLOYS SWIFTLY, SCALES EFFORTLESSLY & INTUITIVE TO MANAGE

Non-disruptive technology that reduces complexity for both IT Teams and End-Users.

USERLOCK

UserLock reduces the risk of external attacks, internal security breaches and compliance issues

WHAT DOES **USERLOCK** DO?

MULTI-FACTOR AUTHENTICATION

Enable customized, multi-factor authentication on Windows logon, Remote Desktop (RDP & RD Gateway), IIS, VPN and Cloud Applications.

SINGLE SIGN-ON

Allow secure and frictionless access to Microsoft 365 and other leading Cloud Applications, from anywhere, using on premise Active Directory credentials.

CONTEXTUAL ACCESS RESTRICTIONS

Set restrictions using the contextual information around a user's logon, to help verify all user's claimed identity, and authorize, deny or limit network access.

SESSION MANAGEMENT & DETAILED AUDITING

Get real-time monitoring and risk detection tools that immediately alert on suspicious logon activity. A centralized audit provides detailed reports to support forensics and prove regulatory compliance.

MULTI-FACTOR AUTHENTICATION (MFA)

ON-PREMISE MFA FOR WINDOWS ACTIVE DIRECTORY

Enable MFA on all connections using **authenticator applications** which include Google Authenticator, Microsoft Authenticator and LastPass Authenticator, or **programmable hardware tokens such as YubiKey and Token2**.

Relying on cryptographic algorithms for Time-based and HMAC-based **One-Time Passwords** (TOTP and HOTP), all options offer strong and simple multi-factor authentication to better protect access across an entire organization.

- Offline-Available MFA needs no Internet connection
- MFA for Remote Users Not Connected to the LAN
- MFA and Windows Remote Desktop (RDP & RD Gateway)
- MFA and Virtual Private Network (VPN) Connections
- MFA and IIS Sessions such as Outlook on the Web
- MFA for Microsoft 365 and Cloud Applications

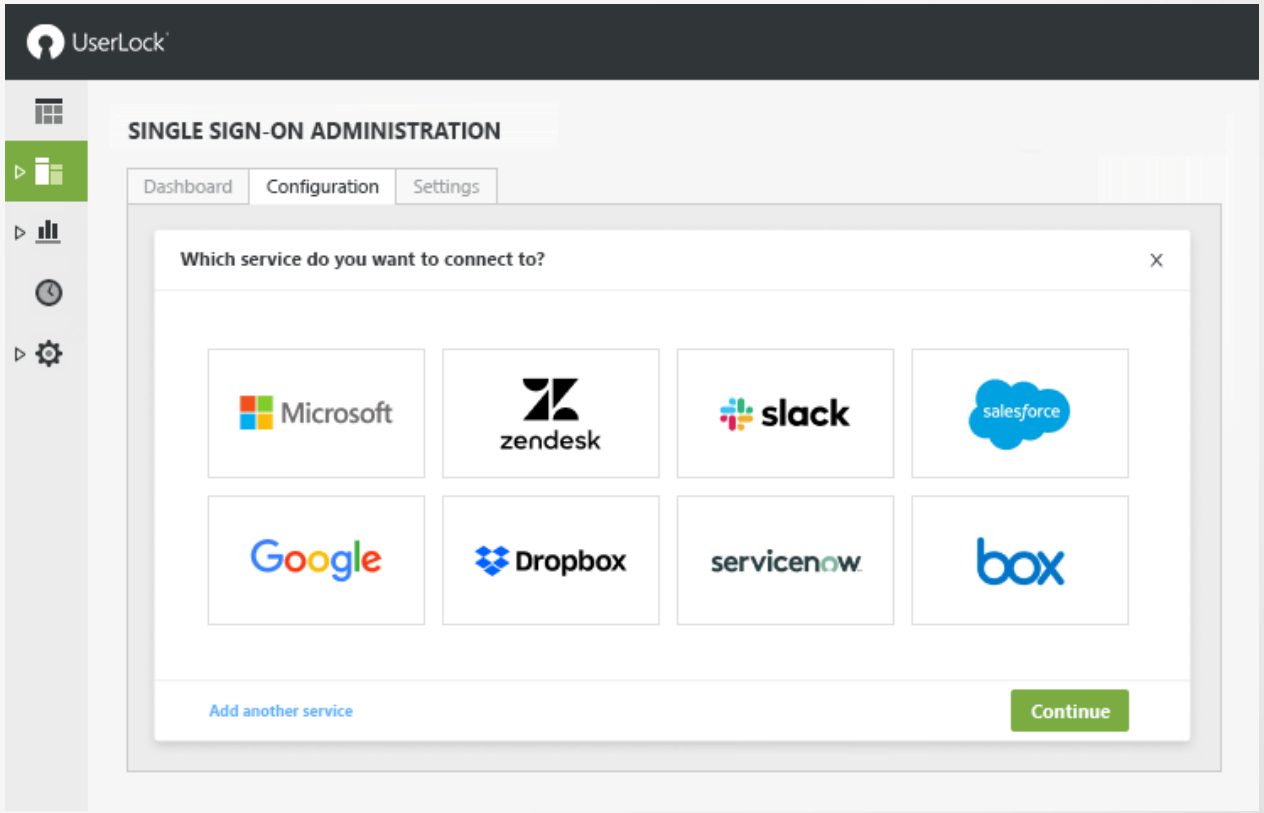
SINGLE SIGN-ON (SSO)

ONE SINGLE IDENTITY TO SECURELY ACCESS ALL RESOURCES

UserLock SSO supports SAML 2.0 protocol to enable **federated authentication** of Microsoft 365 and other cloud applications..

It allows each user to log in only once (with optional MFA) with their **existing Active Directory credentials** to seamlessly access all resources, from wherever they work.

Read more: Four (4) Key Advantages of SSO using Windows AD Identities



CONTROL & PROTECT

CONTEXT-AWARE RESTRICTIONS

Working alongside **Active Directory** to extend its security, UserLock can apply customized **login restrictions** by user, group or organizational unit (OU).

Any logon attempts that don't satisfy these conditions are automatically **blocked**.

ORIGIN

Limit access by location with controls at workstation, device, IP range, organizational unit (OU), department, and geolocation.

TIME

Limit access to specific timeframes and set daily, weekly or monthly time quotas, maximum session times and idle session time.

SESSION TYPE

Control workstation, terminal, Wi-Fi, VPN and IIS sessions to protect both interactive sessions and network access for remote and mobile users.

SIMULTANEOUS CONNECTIONS

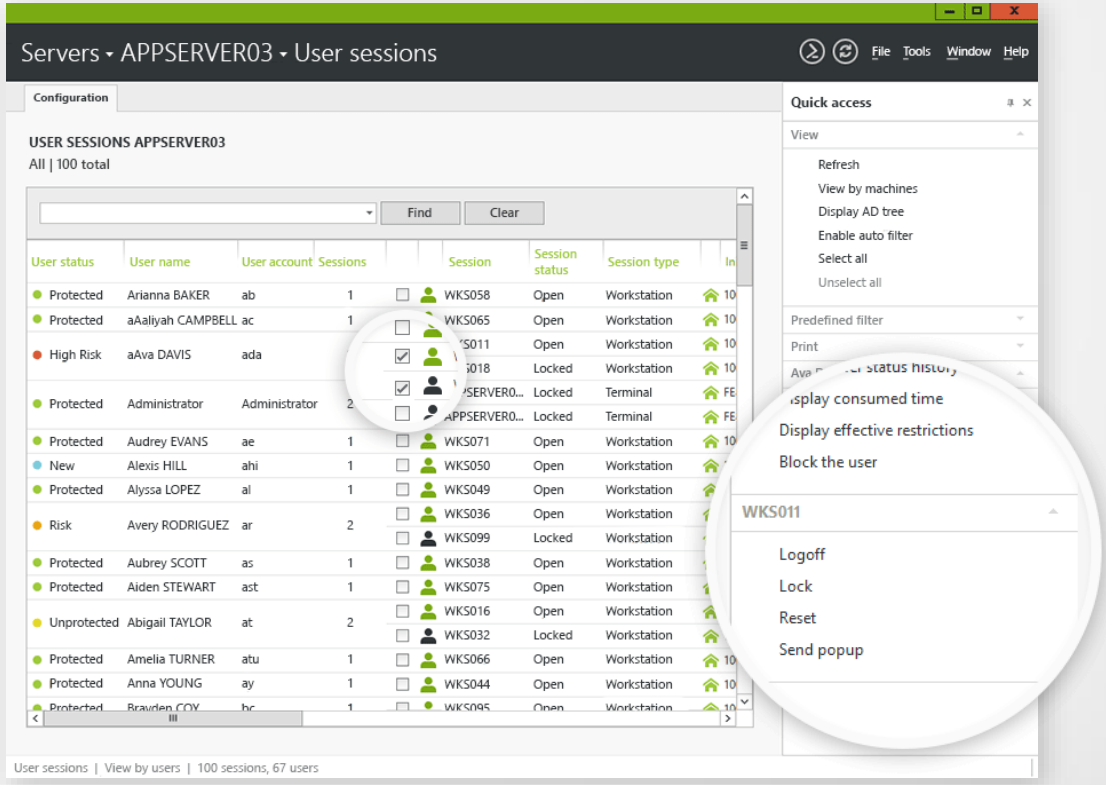
Limit the number of unique entry points and concurrent sessions to prevent simultaneous logins from a single identity.

DETECT & RESPOND

RESPOND TO SUSPICIOUS ACCESS BEHAVIOR

UserLock offers **real-time visibility** and **insight** into all users' logon and logoff activity across an entire Windows Server Active Directory network.

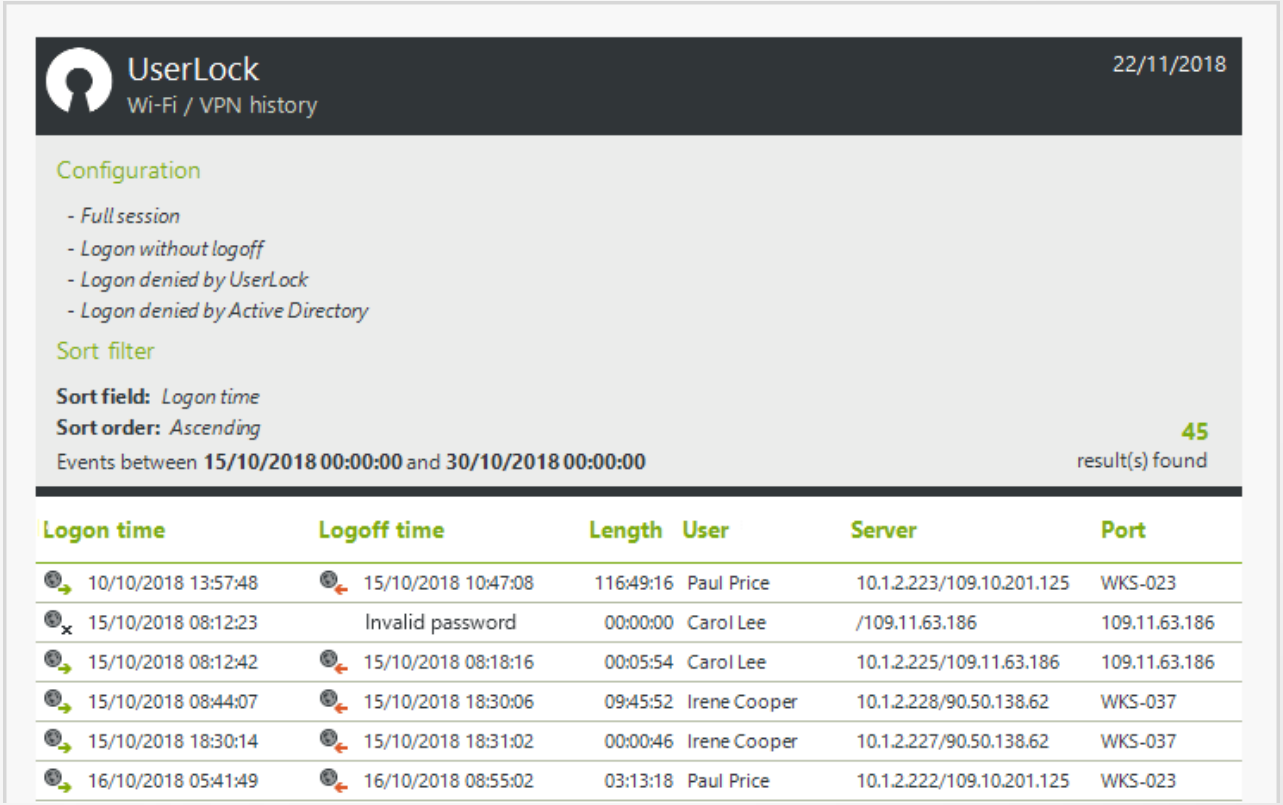
Get **real-time alerts** on specific connection events and **instantly react** to suspicious access behavior, direct from the console.



AUDIT & REPORT

AUDIT LOGON EVENTS

A **centralized audit** on all network logon events provides **detailed and accurate reports** to track down security threats, support forensics and prove regulatory **compliance**.



UserLock
Wi-Fi / VPN history
22/11/2018

Configuration

- *Full session*
- *Logon without logoff*
- *Logon denied by UserLock*
- *Logon denied by Active Directory*

Sort filter

Sort field: *Logon time*
Sort order: *Ascending*
Events between **15/10/2018 00:00:00** and **30/10/2018 00:00:00**
45 result(s) found

Logon time	Logoff time	Length	User	Server	Port
10/10/2018 13:57:48	15/10/2018 10:47:08	116:49:16	Paul Price	10.1.2.223/109.10.201.125	WKS-023
15/10/2018 08:12:23	Invalid password	00:00:00	Carol Lee	/109.11.63.186	109.11.63.186
15/10/2018 08:12:42	15/10/2018 08:18:16	00:05:54	Carol Lee	10.1.2.225/109.11.63.186	109.11.63.186
15/10/2018 08:44:07	15/10/2018 18:30:06	09:45:52	Irene Cooper	10.1.2.228/90.50.138.62	WKS-037
15/10/2018 18:30:14	15/10/2018 18:31:02	00:00:46	Irene Cooper	10.1.2.227/90.50.138.62	WKS-037
16/10/2018 05:41:49	16/10/2018 08:55:02	03:13:18	Paul Price	10.1.2.222/109.10.201.125	WKS-023

INFRASTRUCTURE

UserLock works alongside Active Directory
in a Microsoft Windows Environment

NON-DISTRUPTIVE TECHNOLOGY

No modifications are made to Active Directory or its schema. UserLock works alongside Active Directory to extend not replace its security.

FAST IMPLEMENTATION

Installed on any member server of the domain, UserLock is managed from any workstation or remotely through a web interface.

FAST AGENT DEPLOYMENT

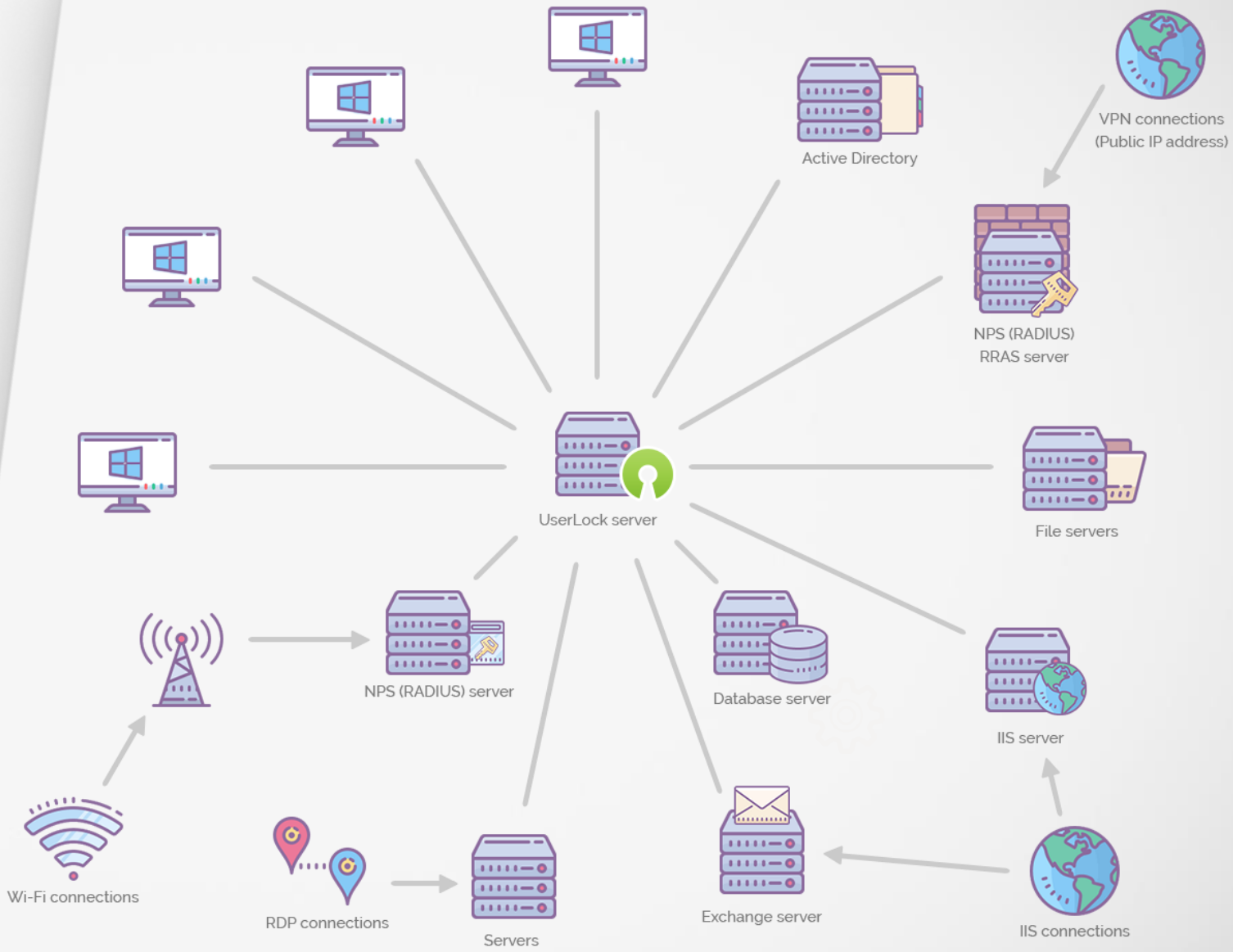
A micro agent is deployed automatically (or manually) on all machines. Once installed all access connections are detected and saved in the UserLock database.

ALL SESSION TYPES

UserLock offers a variety of agents according to the types of session it has to monitor, workstation, terminal, Wi-Fi & VPN and IIS.

INFRASTRUCTURE

UserLock is a **client server** application capable of **auditing** and **controlling** different types of user access connections.

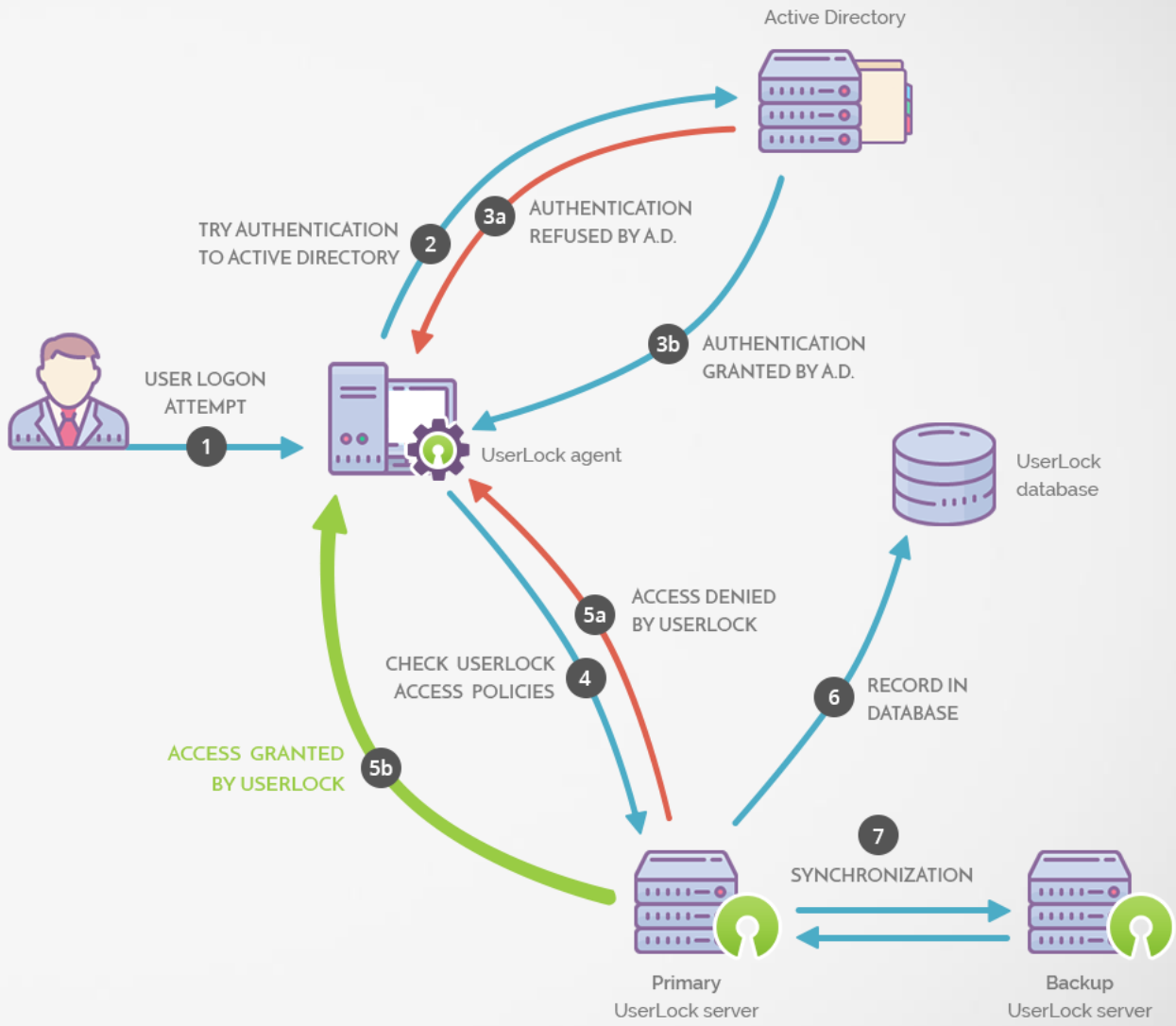


HOW **USERLOCK** WORKS

GENERAL PROCESS DESCRIPTION (1/2)

The user enters their credentials to log on or to **establish a connection** to the domain network. These credentials are verified and validated against Active Directory. If the **authentication process fails**, the connection will be refused by Windows and **UserLock does not intervene**. The agent will however notify the UserLock server about this logon failure.

Different agents are available depending on the connection type to be audited and the technology used to configure these connections. The general process is the same regardless of the agent type.



HOW **USERLOCK** WORKS

GENERAL PROCESS DESCRIPTION (2/2)

If the **authentication is successful**, the UserLock agent will transmit to the UserLock server all information about the **context of the connection** requested. The UserLock server will then **process and analyze the data** transmitted by the agent to check access control rules, trigger any alerts, refresh session information and save the user connection event in the database. **The server then communicates its decision** to the agent regarding the acceptance or refusal of the connection requested.

WHY YOU NEED USERLOCK?
AVOID NETWORK & DATA BREACHES

UserLock prevents unauthorized and unwanted access to the corporate Windows Network and Cloud Applications.

STOP EXTERNAL ATTACKS AND LATERAL MOVEMENT

Stop an attacker's ability to use compromised credentials.

DETER MALICIOUS BEHAVIOR

Hold individual users accountable for their access and actions on the network.

ERADICATE CERTAIN CARELESS USER BEHAVIOR

Such as password sharing, shared workstations left unlocked…

Review by Gov't Network Tech

★★★★★

Gartner peerinsights

Awesome Tool For Securing Logons

Userlock has been a great tool and helped us tighten up our user security. It's used in conjunction with Active Directory and Group Policy to secure all logon types in the domain.

WHY YOU NEED USERLOCK?
MANAGE ACCESS FOR ALL USERS

UserLock helps enforce the legitimate access needs for all users to the corporate Windows Network and Cloud Applications.

SECURE ANY KIND OF PRIVILEGED ACCESS

Every user is some sort of privileged user. UserLock makes it easy to manage and protect all users.

MANAGE A ZERO-TRUST ACCESS POLICY

Set different login controls to verify all access attempts without unnecessarily impeding employees.

ADDRESS COMPLIANCE AND AVOID FINES

Requirements exist to ensure all access is protected by MFA and is always identifiable, audited and attributed to an individual user.

Review by Bob B.

★★★★★

Capterra

An Administrators Premier Management Tool!

In a flash, I can control my users' login experience, find/identify users computers and remote in for support. It's just always there for me. I can't imagine working without it now.

ADVANTAGES OF **USERLOCK** (1/2)

EASY TO USE

No training is necessary

FAST & SIMPLE TO INSTALL

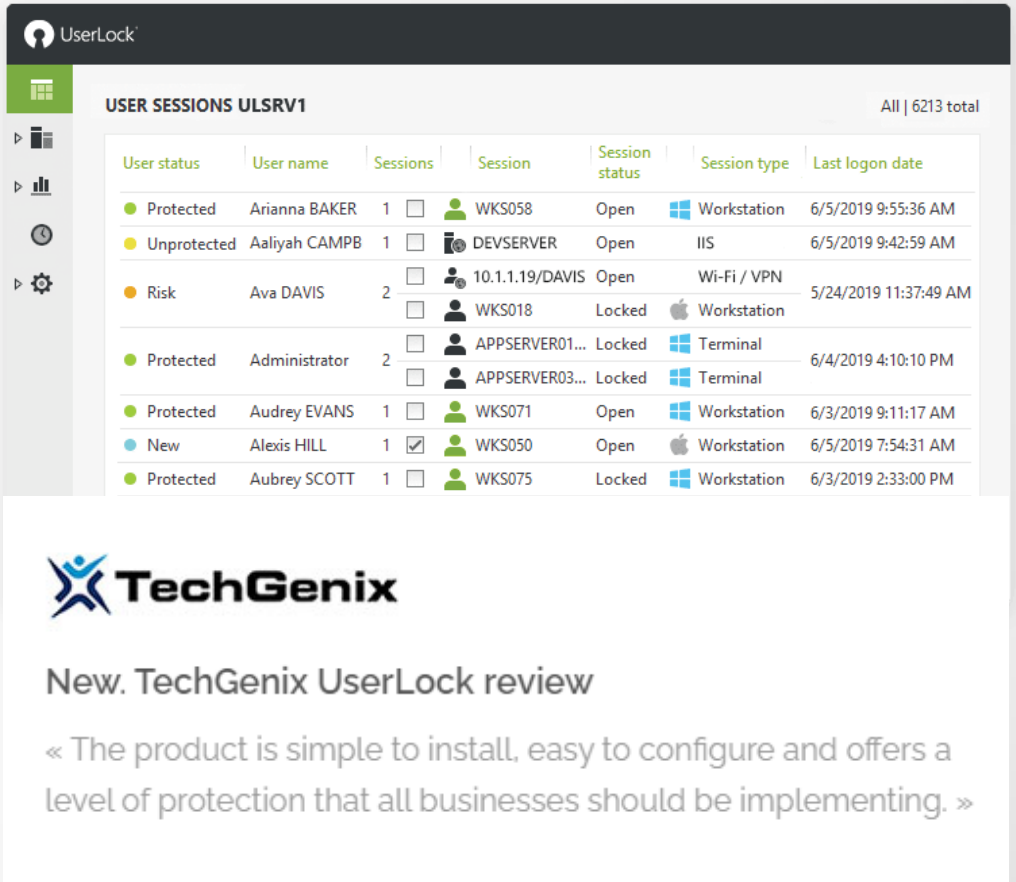
Ready to use in minutes

NON-DISRUPTIVE TECHNOLOGY

No modifications are made to Active Directory

TRANSPARENT FOR THE END USER

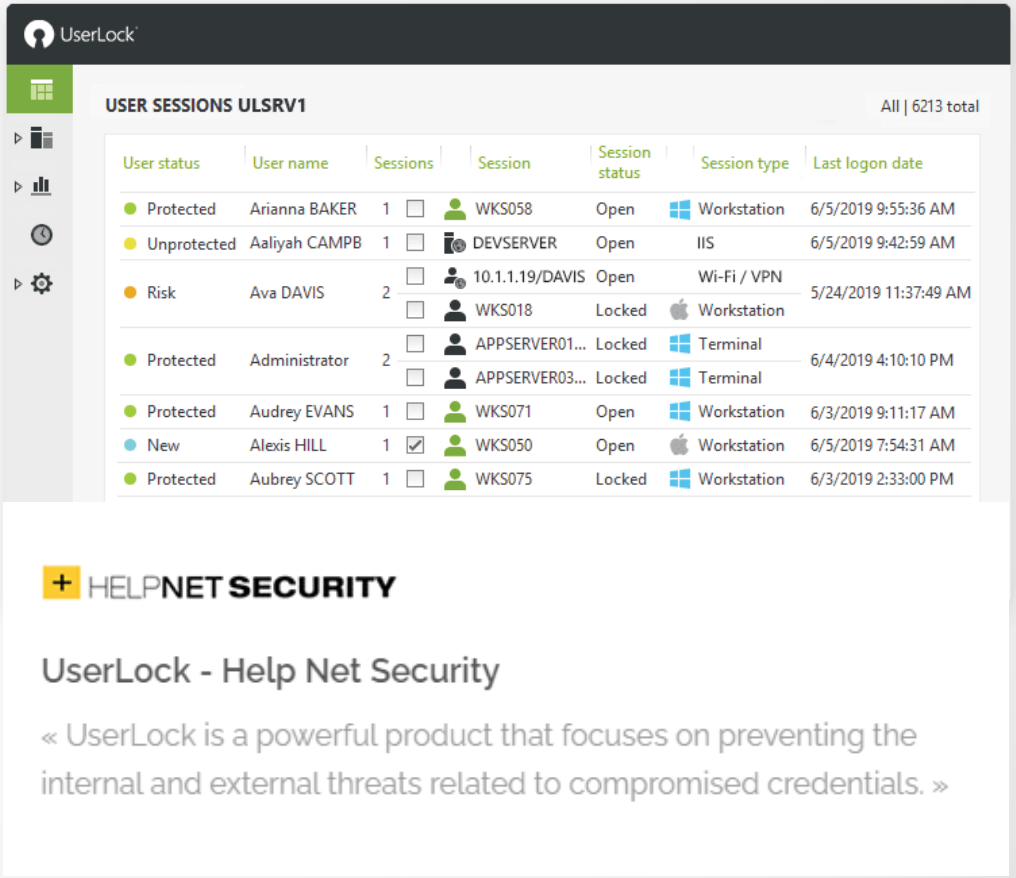
UserLock does not impede with productivity



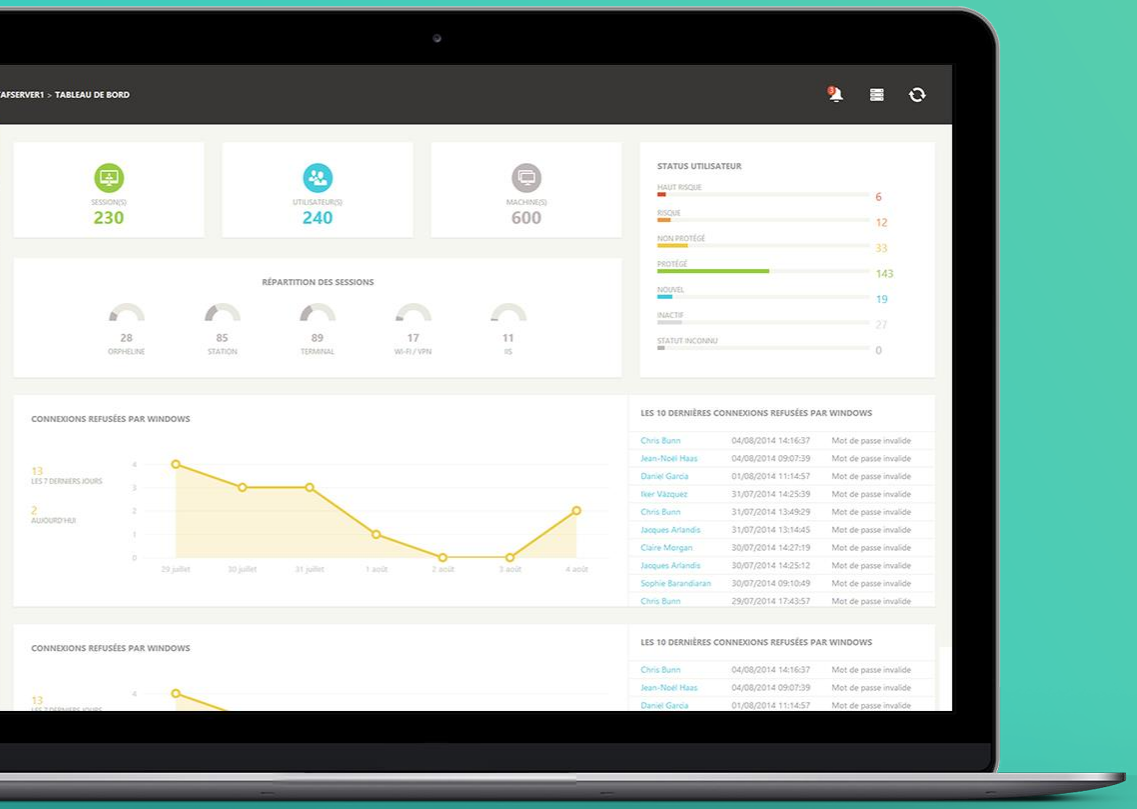
ADVANTAGES OF **USERLOCK** (2/2)

GET SECURITY FAR BEYOND NATIVE ACTIVE DIRECTORY & GROUP POLICIES

- ✓ Granular Multi-Factor Authentication
- ✓ Secure Single Sign-On to Cloud Applications
- ✓ Set restrictions by Group and OU
- ✓ Identify Initial Access Point from a nested session
- ✓ Concurrent login control
- ✓ Force logoff when allowed time expires
- ✓ Remotely logoff, lock or reset any user session
- ✓ Warn users themselves of suspicious login activity
- ✓ Display notifications of previous logon
- ✓ Set temporary logon controls



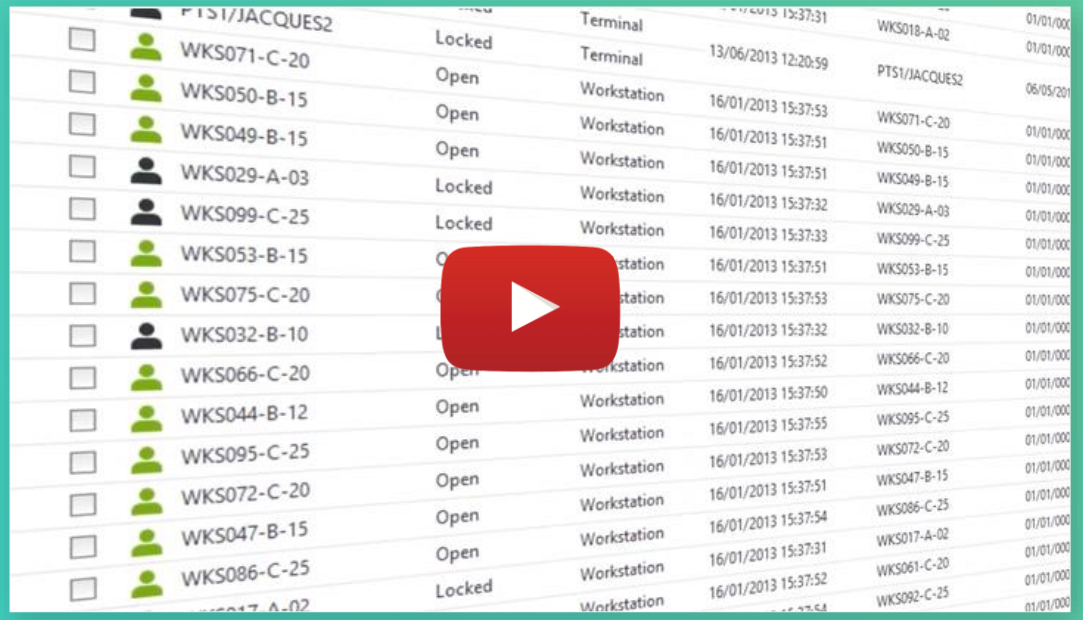
« The perfect access security partner for Windows Active Directory environments. »



After analyzing several other options, we found UserLock gave us the most accurate visibility on all user's logon and logoff activity. In addition, its ability to easily enforce logon restrictions allows us to not only detect and react to abnormal logon activity but prevent the inappropriate use of credentials.

Wilde Ho
IT Manager at Angliss

LEARN MORE ABOUT USERLOCK



IS Decisions®

www.isdecisions.com

info@isdecisions.com