DATASHEET

One Identity Safeguard for Privileged Analytics

Detect and prevent security breaches related to privileged access

Benefits

- Provides insight into what is happening in your IT system by tracking and visualizing user activity
- Continuous authentication through constant analysis of keystroke dynamics and mouse-movements
- Identifies unusual deviations from baseline activity with machine learning
- Shortens time to detect a security incident with contextual information and risk-based prioritization of recorded sessions
- Reduces the noise of security alerts so you can focus on what matters
- Enhances security by terminating any connection when an alert is thrown about potentially nefarious activity

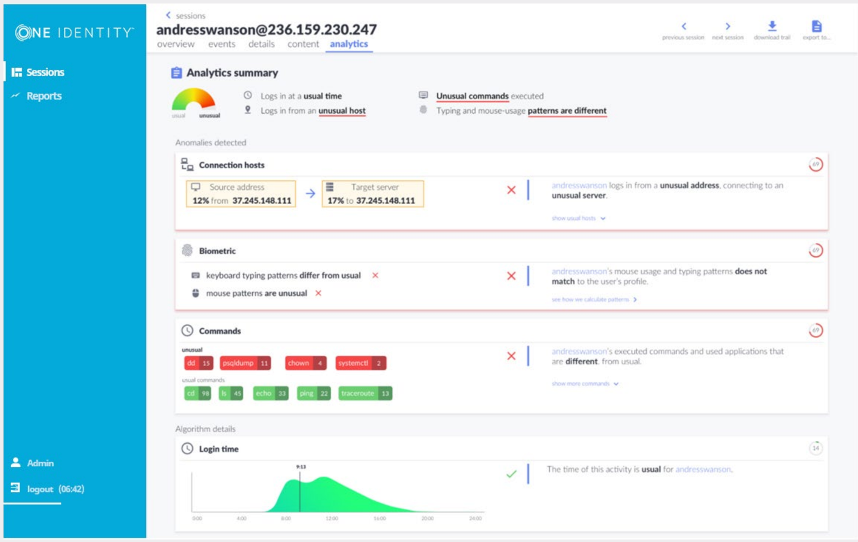
Overview

As an IT security manager, you know better than to think your company will never experience a privileged account breach. Today, it takes organizations an average of 206 days[1] to identify a breach. And time is money – and risk. So, whether the breach is from a hijacked privileged account or an admin gone rogue, the longer it goes undiscovered, the more time there is for the infiltrators to find and steal data, and for fines and more forensic expenses to add up.

You have probably had to provide privileged access beyond your trusted administrators. You might have expanded to include outsourced admins from outside consultants who could be based anywhere in the world. So how can you ensure that admins who have privileged access are using it for good and not evil?

With One Identity Safeguard for Privileged Analytics, you know who your most risky users are, you keep a constant lookout for new internal and external threats, and can detect unusual privileged behavior. This powerful solution gives you full visibility into your privileged users and their activities, and if there is an issue, you can take immediate action and be well positioned to prevent data breaches.

[1] Ponemon's 2017 Cost of Data Breach Study



andresswanson@236.159.230.247

Analytics summary

Logs in at a usual time
Logs in from an unusual host
Unusual commands executed
Typing and mouse-usage patterns are different

Anomalies detected

Connection hosts

Source address: 12% from 37.245.148.111 → Target server: 17% to 37.245.148.111

andresswanson logs in from a unusual address, connecting to an unusual server.

show usual hosts

Biometric

keyboard typing patterns differ from usual ✗
mouse patterns are unusual ✗

andresswanson's mouse usage and typing patterns does not match to the user's profile.

see how we calculate patterns

Commands

unusual: dd 15, psqldump 11, chown 4, systemctl 2
usual commands: cd 98, ls 45, echo 33, ping 22, traceroute 13

andresswanson's executed commands and used applications that are different. from usual.

show more commands

Algorithm details

Login time

✓ The time of this activity is usual for andresswanson.

Easily determine risky users and behavior

Quickly see if a user's activity is unusual and potentially risky with the analytics summary view. It contains a summary of unusual commands, biometric activity, and connection hosts.

Features

Identify risky users

Privileged Analytics evaluates entitlement grants against risk-classification rules to identify high-risk accounts. Proactive notifications are sent when changes to entitlement grants move a user's profile into a high-risk status. This eliminates risk from unnecessary or dormant entitlements before someone can abuse or exploit them.

Detect unknown threats in real-time

Rules-based security will fail to detect new external attack methods or malicious insiders. Safeguard for Privileged Analytics tracks and visualizes user activity in real-time for a better understanding of what is really happening in your IT environment. It doesn't require pre-defined correlation rules; it simply works with your existing session data.

Pattern free operation

Instead of using pattern-based matching to detect 'known bad' behavior - which is often incorrect - Safeguard for Privileged Analytics uses data collected from your IT environment. It creates a baseline of 'normal' behavior and detects deviations by using various machine learning algorithms.

Screen content analysis

By analyzing the screen content of privileged sessions and understanding the issued commands and window titles Safeguard for Privileged Analytics can enrich the baseline behavior profile of the regularly used commands and applications of your privileged users. This granular analysis facilitates the identification of typical behavior and the detection of privileged identity thefts.

Behavioral biometrics

Each user has its own idiosyncratic pattern of behavior, even when performing identical actions, such as typing or moving a mouse. The algorithms built into Safeguard for Privileged Analytics inspect these behavioral characteristics captured by Safeguard for Privileged Sessions. Keystroke dynamics and mouse movement analysis not only help you identify breaches, but also serve as a continuous, biometric authentication.

Reduce alert noise

Privileged Analytics reduces alert noise generated by SIEMs by categorizing user events based on risk and deviation levels, and highlighting the most suspicious events. Alerts can be sent to SIEMs or your security analysts can view a prioritized list of events on the intuitive user interface, enabling them to focus on the most important ones.

Automated response

In most attack scenarios, high-impact events are often preceded by a reconnaissance phase. So, detection and response during this phase is critical to preventing damaging activity. Seamless integration with Safeguard for Privileged Sessions enables automated session termination whenever a highly suspicious event occurs, or malicious behavior is detected.

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats. Learn more at OneIdentity.com