

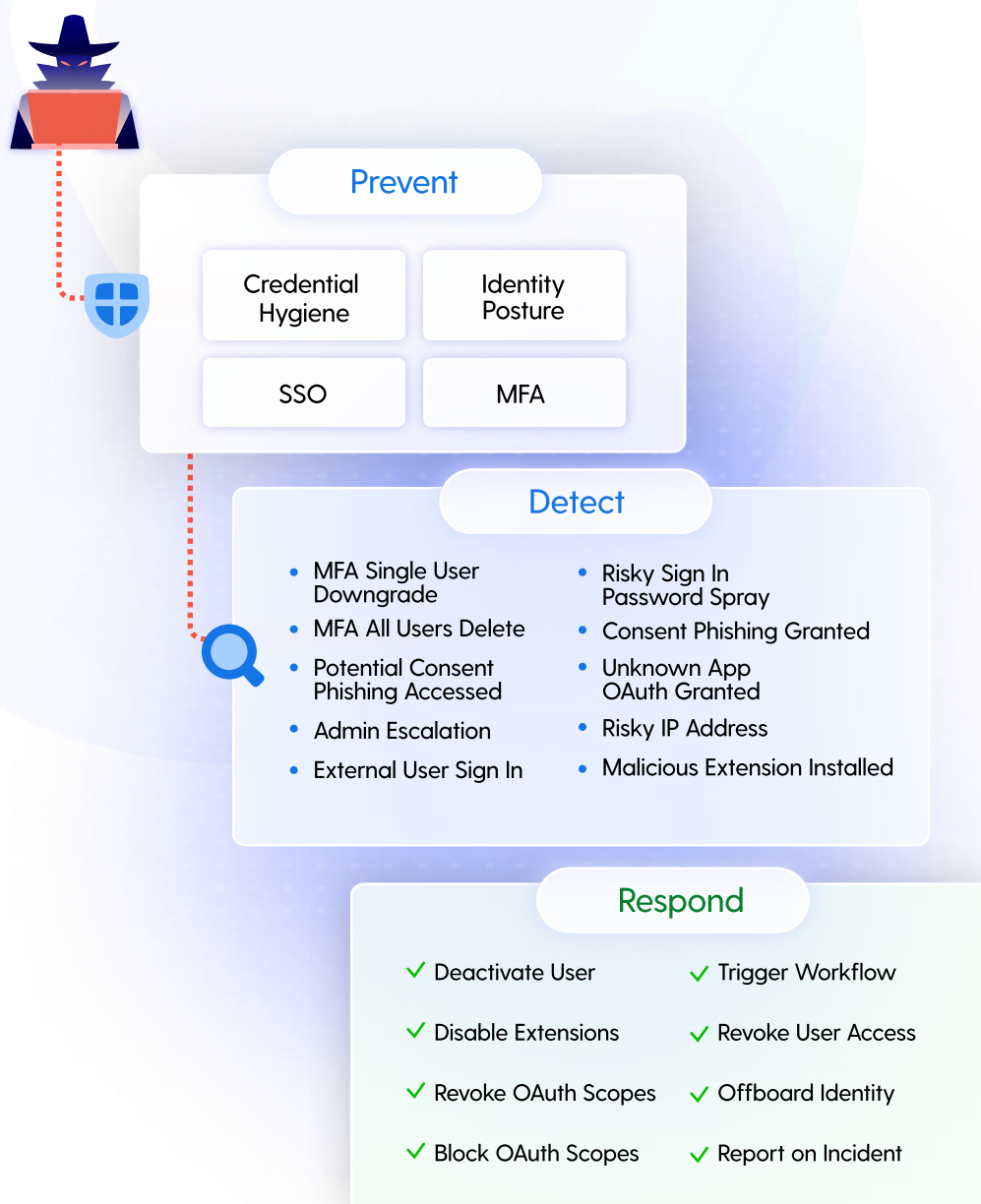


Grip Identity Threat Detection and Response 2.0

Grip ITDR 2.0: Next-Gen Identity Threat Detection & Response

Grip ITDR 2.0 helps SecOps teams not only detect and respond to identity threats but prevent them before they lead to breaches.

- **Proactive prevention** – Reduce risk before it becomes a threat by eliminating unused access, strengthening access controls, and mitigating posture gaps that attackers exploit.
- **Smarter threat detection** – Prioritize the most critical identity threats to reduce alert fatigue and provide rich identity context to aid investigation efforts.
- **Faster response** – Take immediate action. Terminate access, revoke or block OAuth scopes, disable malicious browser extensions, and contact users directly via the browser extension.
- **Seamless workflows** – Integrate natively with SIEM, SOAR, or ticketing tools to streamline containment and reduce manual effort.



Outcomes Achieved:

- **Prevent threats**—Enable SecOps to proactively reduce risks before they lead to breaches.
- **Accelerate Threat Detection (MTTD)** – Detect identity threats across all SaaS, including unmanaged and shadow apps in one place.
- **Accelerate Response (MTTR)** - Quickly respond to threats by blocking access, revoking OAuth scopes, quarantining users, terminating IdP sessions, and disabling malicious browser extensions.
- **Stop Lateral Movement & Data Loss** - Shut down credential abuse and identity threats before attackers can pivot or exfiltrate data.
- **Enforce Least Privilege Access** - Prevent unauthorized privilege escalation and shared account misuse.
- **Reduce Account Takeover** - Identify and remediate weak, reused, or compromised credentials across all identities.
- **Shrink the SaaS Attack Surface** – Eliminate risky OAuth connections and browser extensions that attackers exploit to escalate access.

Key Features:

- Real-Time Threat Detection Across all SaaS
- Detection of Malicious SaaS to SaaS OAuth Grants
- Detection of Malicious Browser Extension Installations
- Investigation Panel with Blast Radius Mapping
- One-Click & Automated Response Workflows
- Continuous Monitoring & Detection Tuning
- Identity Attack Surface Management (IASM)
- Identity Security Posture Management (ISPM)

Grip ITDR 2.0 is built on a foundation of deep visibility—something other solutions lack. It delivers unmatched insight and control across the modern SaaS portfolio, including unmanaged applications, shadow identities, risky OAuth grants, malicious browser extensions, and more. This visibility gives SecOps teams the context they need to detect, prevent, and respond to identity threats with precision and confidence.

Why Grip ITDR 2.0?

SecOps Speed and Precision

Grip ITDR 2.0 is purpose-built to accelerate SecOps workflows while actively reducing identity risk. It enriches alerts with identity-specific context, recommends the next best action, and enables instant remediation—manually or via automation. But it doesn't stop at response. Grip prevents threats before they escalate by continuously identifying and eliminating risky access, stale accounts, and vulnerable integrations. Less time spent triaging and guessing means more time stopping and preventing real threats.

Broader Detection Across the Identity Attack Surface

Other ITDR tools only monitor what your IdP manages. Grip ITDR 2.0 goes further, covering IT-managed apps, shadow SaaS, user-created accounts, and SaaS-to-SaaS integrations. It detects weak or reused credentials, risky OAuth scopes, and abnormal behaviors that traditional solutions overlook. By monitoring the full identity attack surface, Grip gives SecOps teams earlier, more actionable signals—and a chance to shut down threats before damage is done.

Visibility Beyond the Login

Most ITDR platforms focus on login anomalies like impossible travel or geo-location mismatches. Grip ITDR 2.0 goes far beyond that. It detects threats post-authentication, including malicious OAuth grants, credential-harvesting browser extensions, and privilege abuse within SaaS apps. This depth of visibility enables not just detection, but early intervention and preemptive control—essential for stopping identity threats before they become breaches.

Category	Capability	Traditional ITDR	Grip ITDR 2.0
Prevention	Monitors identity posture to flag risky identities and recommend mitigations	Limited	Yes
	Identifies critical misconfigurations in SaaS and IdPs with guided remediation	No	Yes
Threat Detection	Detects anomalous login activity (IP, device, location)	Yes	Yes
	Detects identity threats beyond login (OAuth, extensions, privilege escalation)	No	Yes
	Uses data sources beyond IdP (e.g. browser extension)	Limited	Yes
	Detects malicious browser extension installations	No	Yes
	Detects unmanaged / shadow SaaS apps	No	Yes
	Detects non-human identity threats (e.g., SaaS-to-SaaS integrations)	Limited	Yes
	Tracks risks from external identities	Limited	Yes
Investigation	Maps downstream impact with blast radius visualization	No	Yes
	Visualizes identity attack surface (internal + external)	Limited	Yes
	Correlates multiple behaviors into multi-stage attack narratives	No	Yes
Response	Supports one-click and automated remediation	Limited	Yes
	Integrates with SIEM, SOAR, and ticketing systems	Yes	Yes
	Tracks threat lifecycle from detection to resolution	Limited	Yes
Continuous Monitoring	Automates detection tuning through behavior learning	Limited	Yes
	Continuously correlates new events with historical threats	Limited	Yes
	Identifies attack stages and adapts detection patterns	Limited	Yes

Grip ITDR 2.0 Key Capabilities

Real-Time Threat Detection Across all SaaS

Detect live identity threats live across the full SaaS ecosystem, including shadow apps. Go beyond login telemetry to detect deeper identity threats:

- Correlate signals from IdPs, OAuth, email, Grip Extend (browser), and more.
- Detect threats like:
 - Risky logins (unusual geo/device/IP).
 - Password spray attempts.
 - Removal of MFA (individual or org-wide).
 - OAuth consent phishing.
 - Admin privilege escalation.
 - OAuth scopes granted to unknown apps.
 - Malicious browser extension installations.
 - External users accessing sanctioned SaaS.

Identity Threat Detection & Response

Severity	Threat Type	Related Identity	Related App	Detection Date ↓	Status	
Low	Unknown App OAuth t	DG Debby Geldens debby.geldens@acme.co...	N/A	Apr 28, 2025 05:32	New	Block OAuth Scopi
Critical	Consent Phishing Grar	DG Debby Geldens debby.geldens@acme.co...	N/A	Apr 28, 2025 05:32	New	Revoke All OAuth Scopi
Low	Potential Consent Phis	DG Debby Geldens debby.geldens@acme.co...	N/A	Apr 28, 2025 05:31	New	Quarantine Us
Critical	Malicious Extension In:	DG Debby Geldens debby.geldens@acme.co...	N/A	Apr 28, 2025 05:27	In Progress	Disable Extensic
Critical	Malicious Extension In:	HC Honor Crespi honor.crespi@acme.com	N/A	Apr 24, 2025 07:55	New	Disable Extensic
Critical	Malicious Extension In:	HC Honor Crespi honor.crespi@acme.com	N/A	Apr 24, 2025 07:38	New	Disable Extensic
Critical	Consent Phishing Grar	HC Honor Crespi honor.crespi@acme.com	N/A	Apr 24, 2025 07:16	Under Investigation	Revoke All OAuth Sco ?

Detection of Malicious SaaS to SaaS OAuth Grants

Uncover and control risky app-to-app integrations created through OAuth without needing direct API access.

- Discover OAuth grants between third-party apps and evaluate their risk
- Detect consent phishing and unauthorized scope grants to unknown or unvetted apps
- Automatically revoke or block suspicious OAuth scopes before they can be exploited

SaaS to SaaS

Prioritize and respond to risky OAuth app activity across your environment

Active OAuth Alerts

2 Alerts

Critical

View All →

Automated Actions

6 Actions

Revoked Blocked Verified

Create New → View All →

Top OAuth Alerts

Severity	Type	Detection Time	Action
Critical	Consent Phishing Granted	Apr 24, 202...	Revoke All OAuth Scopes
Critical	Consent Phishing Granted	Apr 24, 202...	Revoke All OAuth Scopes

View All →

Detection of Malicious Browser Extension Installations

Expose and respond to browser extensions that pose a threat to SaaS security—a growing and often overlooked attack vector.







- Identify newly installed extensions that can intercept sessions or exfiltrate data
- Mitigate threats by uninstalling extensions, alerting users, or blocking future installs

Extensions Portfolio

Total Extensions

16

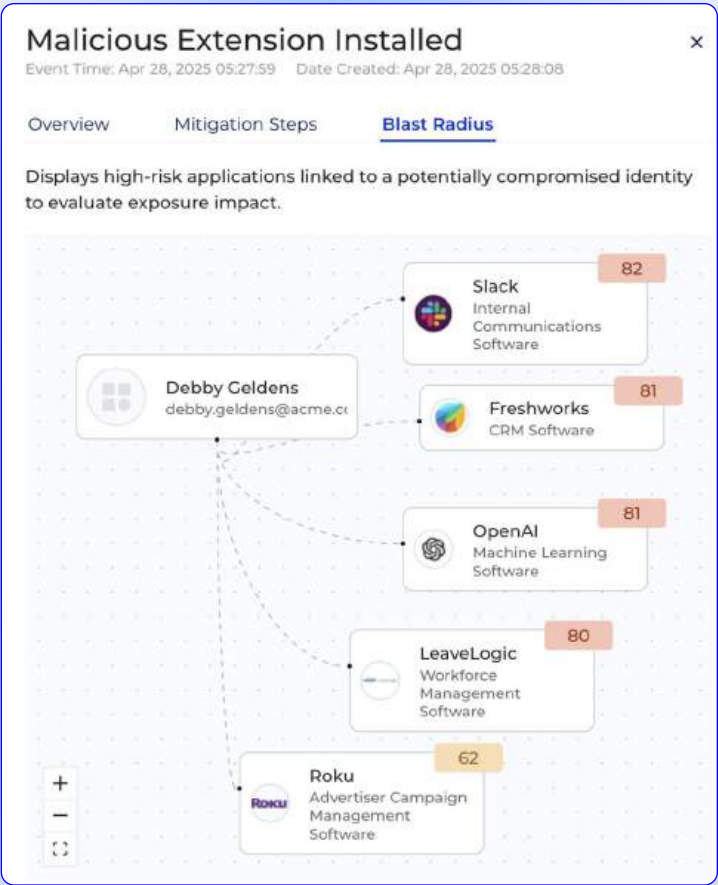
+ 15 from last week

Extension Name	Score ⓘ	Sanction	Total Accounts	First Detection	Permissions
 uBlock Origin Privacy	90	+1 New	1	Apr 24, 2025	tabs +5
 Todoist for Chrome Workflow	50	- Tolerated	2	Apr 22, 2025	tabs
 Sider: Chat with all AI models ... Tools	70	- Tolerated	1	Apr 23, 2025	tabs +2
 Shazam: Find song names fro... Tools	50	+1 New	1	Apr 24, 2025	capture +2
 Session Buddy Workflow	50	+1 New	3	Apr 24, 2025	tabs
 React Developer Tools Developer	70	+1 New	1	Apr 24, 2025	tabs +3

Investigation Panel with Blast Radius Mapping

Investigate identity threats in depth with rich context and visibility into downstream risk.

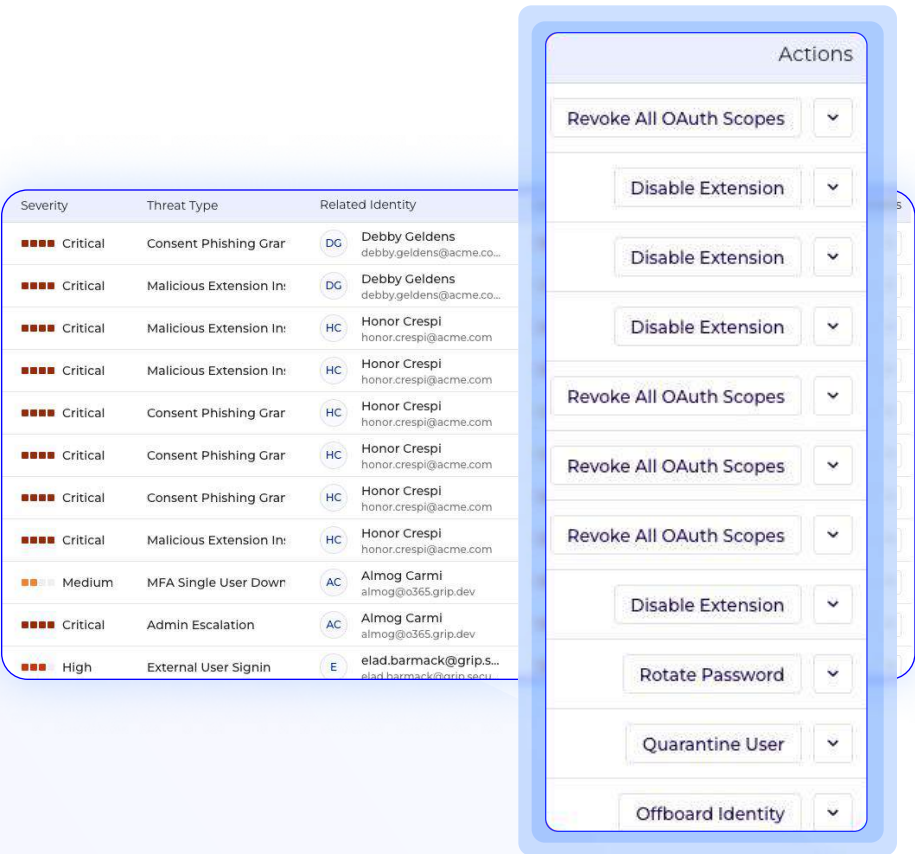
- Use the Investigation Panel to analyze affected identities, SaaS assets, behavioral anomalies, and source signals
- Visualize impact with the Blast Radius Map, highlighting exposed users and apps
- Filter investigations by threat traits and behavioral patterns
- Correlate discrete events into multi-stage attacks for full situational awareness



One-Click & Automated Response Workflows

Quickly contain and remediate identity threats with manual or automated actions tailored to the threat.

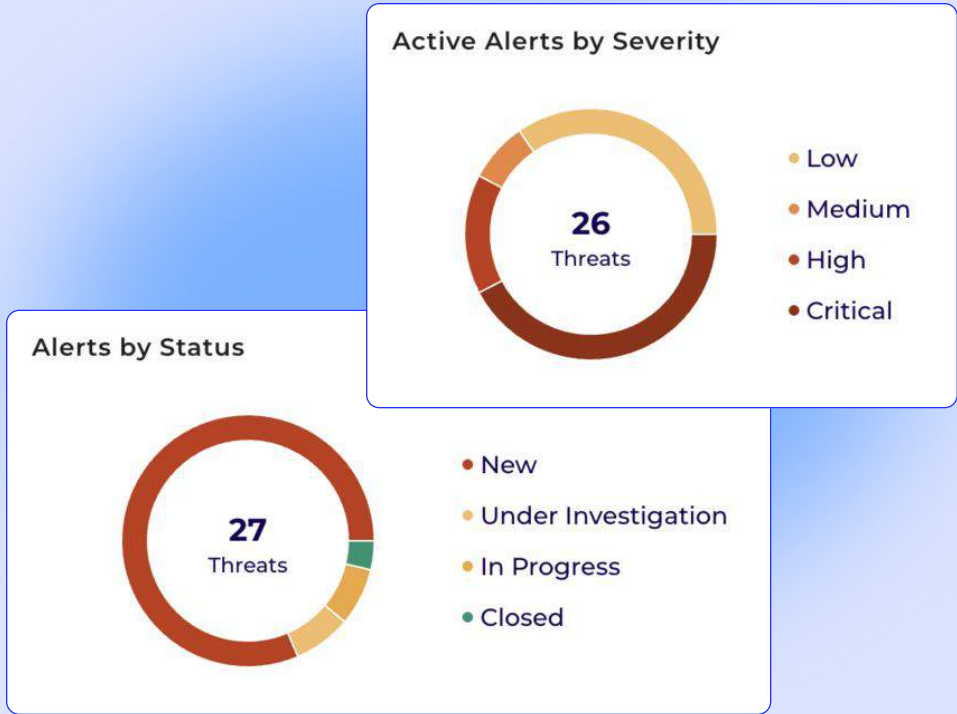
- Respond instantly with one-click actions or policy-driven automation:
 - Quarantine compromised identities.
 - Revoke or block OAuth grants.
 - Reset passwords.
 - Terminate active sessions.
 - Remove malicious browser extensions.
- Automate responses based on threat type, severity, or behavioral patterns.
- Integrate seamlessly with SIEM, SOAR, and ticketing systems.
- Track threat status through the full lifecycle:
 - New → Under Investigation → Remediated → Policy-Handled.



Continuous Monitoring & Detection Tuning

Stay ahead of evolving threats with real-time monitoring and adaptive detection improvements.

- Correlate new activity with past threats for deeper context
- Identify attack stages and build detection patterns over time
- Continuously refine detection accuracy and response effectiveness behind the scenes



Identity Attack Surface Management

Gain visibility into the identities most vulnerable to exploitation across your SaaS environment—and take action to reduce risk.

- Identify internal risks like stale accounts, admins using personal emails, shared credentials, and dormant high-risk users
- Surface external risks including third-party users with access to corporate apps or unintended SSO privileges
- Act immediately from a centralized dashboard to disable users, revoke access, offboard accounts, and more

External Users

Identity	Identity Risk	Total Accounts	Action
Laure Purse laure.purse@acme.com	N/A	20	Disable User
Carla Megan carla.megan@acme.com	N/A	11	Disable User

Admins using non-corporate emails

Admins who've signed up to SaaS apps using personal email addresses (e.g., gmail.com)

Identity	Personal Accounts	Action
Agna Tham agna.tham@acme.com	1	Contact User
Jessa Cornel jessa.cornel@acme.com	1	Contact User
Dory Mesics dory.mesics@acme.com	1	Contact User
Zenia Reedy zenia.reedy@acme.com	1	Contact User
Donnie Jepson donnie.jepson@acme.com	1	Contact User

Top Identities with Stale Accounts

Identify and manage identities with stale accounts to reduce security risks and enforce access policies.

Identity	Stale Accounts	Oldest Account	Action
Anastasia Nido... anastasia.nidorf...	6	Instagram Over 5 months	Revoke Access
Nadeen Moon... nadeen.mooney...	6	Blaze Over 5 months	Revoke Access
Christyna Blas christyna.blas@...	6	Alight Over 6 months	Revoke Access

Identity Posture

See a breakdown of the most risky identities in your organization, all the possible attack surfaces and get recommendations for mitigation and prevention.

Identity Attack Surface: [Identity Security Posture](#)

Admin Posture Policies

Policy	Severity	Requirement	Module	Status	Action
Common Controls B1	Medium	Account self-recovery for super admins is disabled.		Fail	Mitigate
Slack 1.2	High	Ensure admins have MFA.		Fail	Mitigate
Entra ID 7.8	High	Global Administrator role activation triggers an alert.		Fail	Mitigate
Okta 3.1	High	Restrict super-admin privileges to essential users.		Fail	Mitigate
Salesforce 4.1	Medium	Administrators Can Log in as Any User is disabled.		Fail	Mitigate

Credential Posture Policies

Policy	Severity	Requirement	Module	Status	Action
Zoom 1.1	High	Enforce two-factor authentication (2FA) for all users.		Fail	Mitigate
Common Controls 1.1	High	Phishing-resistant MFA is required for all users.		Fail	Mitigate
Slack 1.1	High	Ensure all users use MFA.		Fail	Mitigate
Entra ID 3.6	High	Phishing-resistant MFA is mandatory for roles with high privileges.		Fail	Mitigate
Okta 2.1	Medium	Enforce a minimum password length to strengthen password against brute force.		Fail	Mitigate

Identity Security Posture Management

Continuously monitor and improve identity configurations across your SaaS and identity systems to reduce breach risk.

- Gain visibility into posture gaps like weak credentials, incomplete MFA coverage, and risky admin settings
- Uncover issues tied to external sharing policies and session settings with full identity context
- Strengthen posture with built-in, app-specific remediation guidance tailored to each misconfiguration



Grip Security is a pioneer in SaaS identity risk management, providing innovative solutions to help enterprises address the security risks associated with widespread SaaS adoption.

Contact Us

- ✉ info@grip.security
- 🌐 [@GripSecurity](https://www.grip.security)
- 🌐 [grip.security](https://www.grip.security)



SOC 2 Type II
Certified



ISO 27001
Certified