Flotek group

Introducing

FloCDR

Cloud Detection & Response, Powered by AI

24/7 Microsoft 365 & SaaS Security–Fully Managed by Flotek

Ai Changing The Threat landscape

62%

of all reported, cybercrime is identify based attacks.

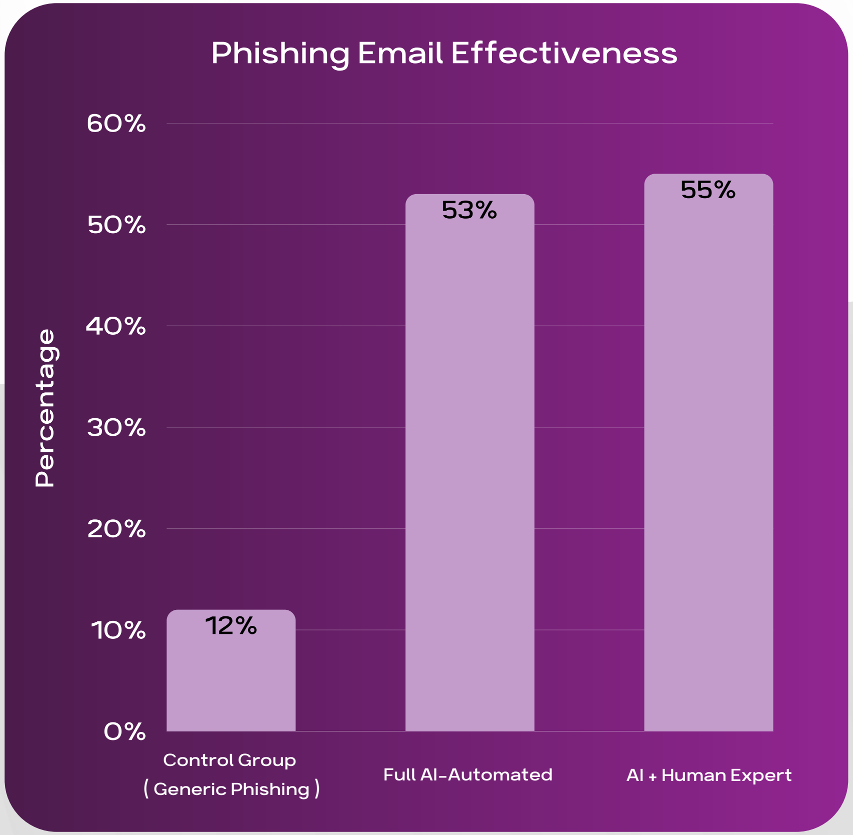
98.68%

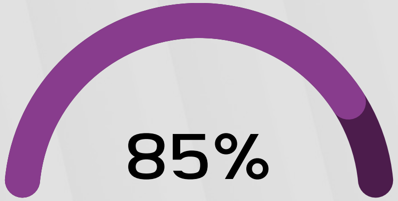
of inbox threats are email impersonation.

£12 Billion

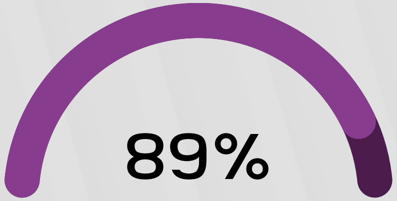
in losses because of BEC in 2024.

Using only AI, sophisticated phishing campaigns can be built in under **10 minutes** Achieving a staggering **56%** click rate.





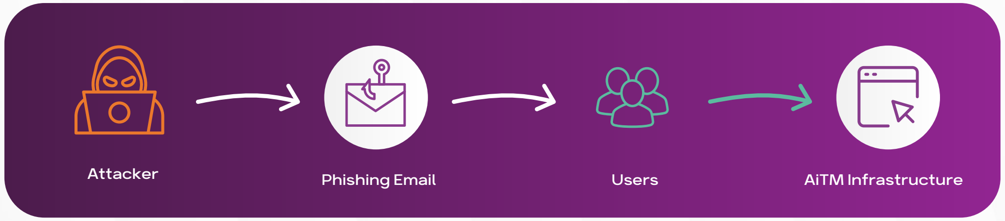
of business applications are SaaS-based



of business are 'digital first'

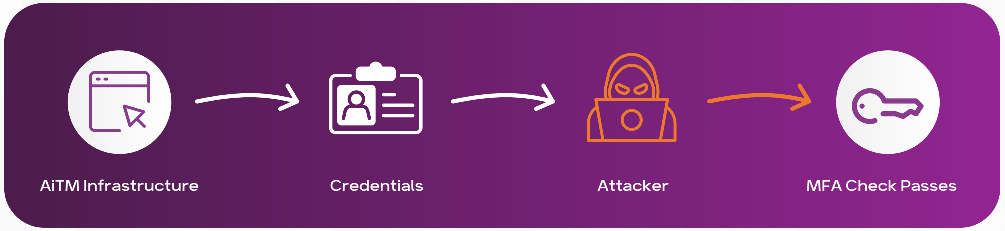
How Attackers Exploit Your Weakness

Attackers use tools and malware to steal tokens, bypassing MFA and gaining access.



Part 1) Gaining Access

- Attacker crafts a phishing email
- User interacts with the phishing email
- Attacker gains access to the user's (AiTM) infrastructure



Part 2) Accessing Platform

- User credentials are harvested
- Attacker uses the stolen credentials to bypass (MFA)
- Attacker successfully accesses the target platform

Your account, your responsibility: one mistake could cost more than you think

Microsoft is not liable for any losses resulting from unauthorised use, whether you’re aware of it or not.

However, you may be held accountable for damages caused to Microsoft or others.

Official Microsoft T&C’s

The SaaS Security Landscape

Microsoft 365 picks up on over 6 million security alerts for every 100 users each month.

That gives you an idea of just how much activity it's monitoring behind the scenes to help keep things secure!

See below for why security matters:

SaaS Adoption is Surging

- SaaS adoption is rising.
- Attack surfaces are growing.
- Cyber threats are increasing.

Unauthorised Logins

- 50%+ of unauthorised logins came from global hotspots.
- Highlights need for geo-aware security.

Successful Logins

- 45% of breaches came from five regions.
- Involves stolen credentials & unapproved access.

Critical Alert Categories

- IAM anomalies, policy changes, and data exports were top alert triggers in 2024.

High-Risk SaaS Applications

- Microsoft 365 triggered most critical alerts for Misconfigs and weak user practices.

Emerging Threats Last 12m

- Rising threats: Phishing-as-a-Service, token hijacking, VPN IP spoofing.

Real-Time Monitoring

- Automated detection and response are now essential for SaaS threat defence.

Data-Driven Security

- 2025 SASI Report helps benchmark risk and guide security investments.

Meet the Challenge: Why CDR + Fortify

See The Difference

Unmanaged Environment		Flotek's CDR + Fortify
Manual Monitoring Security teams must sift through thousands of alerts manually.	→	**7 Day Monitoring by Experts** Flotek's Pro Active Security Team watches your environment every day.
Underused Secure Score Most businesses don't act on Microsoft's recommendations.	→	**Secure Score Optimisation** Continuous improvement based on Microsoft's best practices.
Delayed Response Threats often go undetected for hours or days.	→	**Automated Threat Response** Immediate action on suspicious logins, inbox rule changes, and more.
Alert Fatigue Teams overwhelmed by false positives and noise.	→	**Integrated with RMM** Links SaaS activity to known devices – reducing false positives.

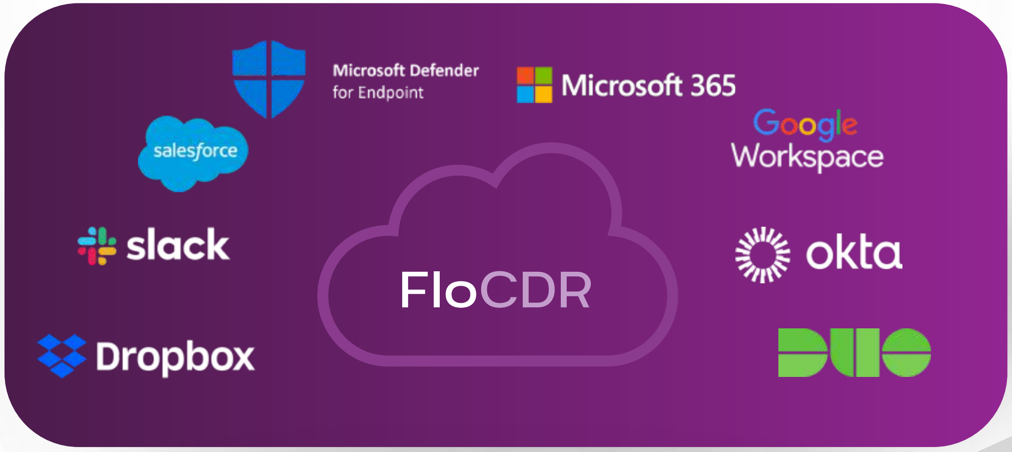
What is Cloud Detection & Response(CDR)?

Did you know?

CDR tools can spot risky behaviour in the cloud and tell if it's legit—helping stop threats before they spread!

SaaS Security That Thinks Like a Human & Reacts Faster!

Our system uses machine learning to monitor SaaS behaviour and instantly respond to unusual activity, stopping threats before they spread.



How does SaaS security protect data across cloud-based applications?

Our CDR system doesn't just monitor, it acts fast! It locks compromised accounts, blocks suspicious logins, and stops threats.

You get clear reports and guidance to stay secure, 24/7.

Continuous Monitoring / Alerts

Automated Remediation

Continuous Security Hardening*

What is Cloud Fortify?

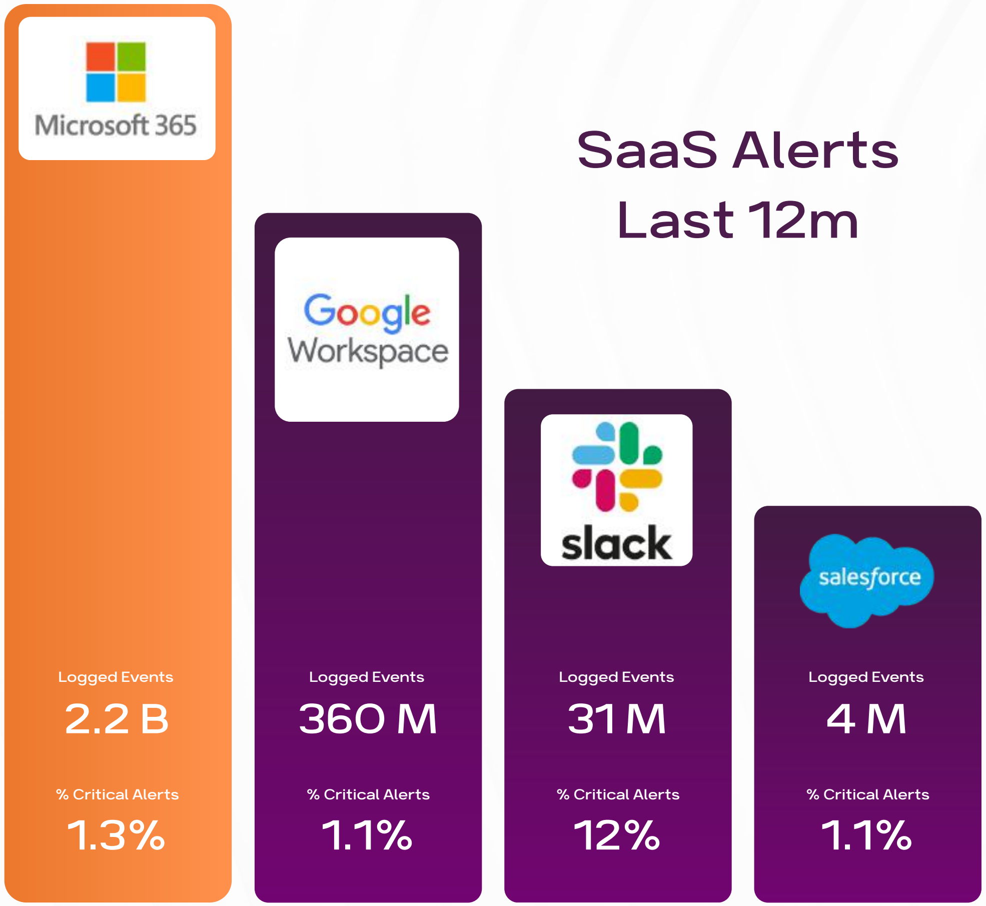
Cut through the noise.

Act on what matters.

Fortify simplifies Microsoft security, helping you protect Microsoft 365 faster and with less effort.

Cyber threats are increasingly targeting small and medium-sized businesses through Microsoft 365, securing your tenant has never been more **urgent**.

Fortify empowers you to apply Microsoft's best-practice security settings across your environment in just minutes—saving time, reducing risk, and giving you peace of mind.

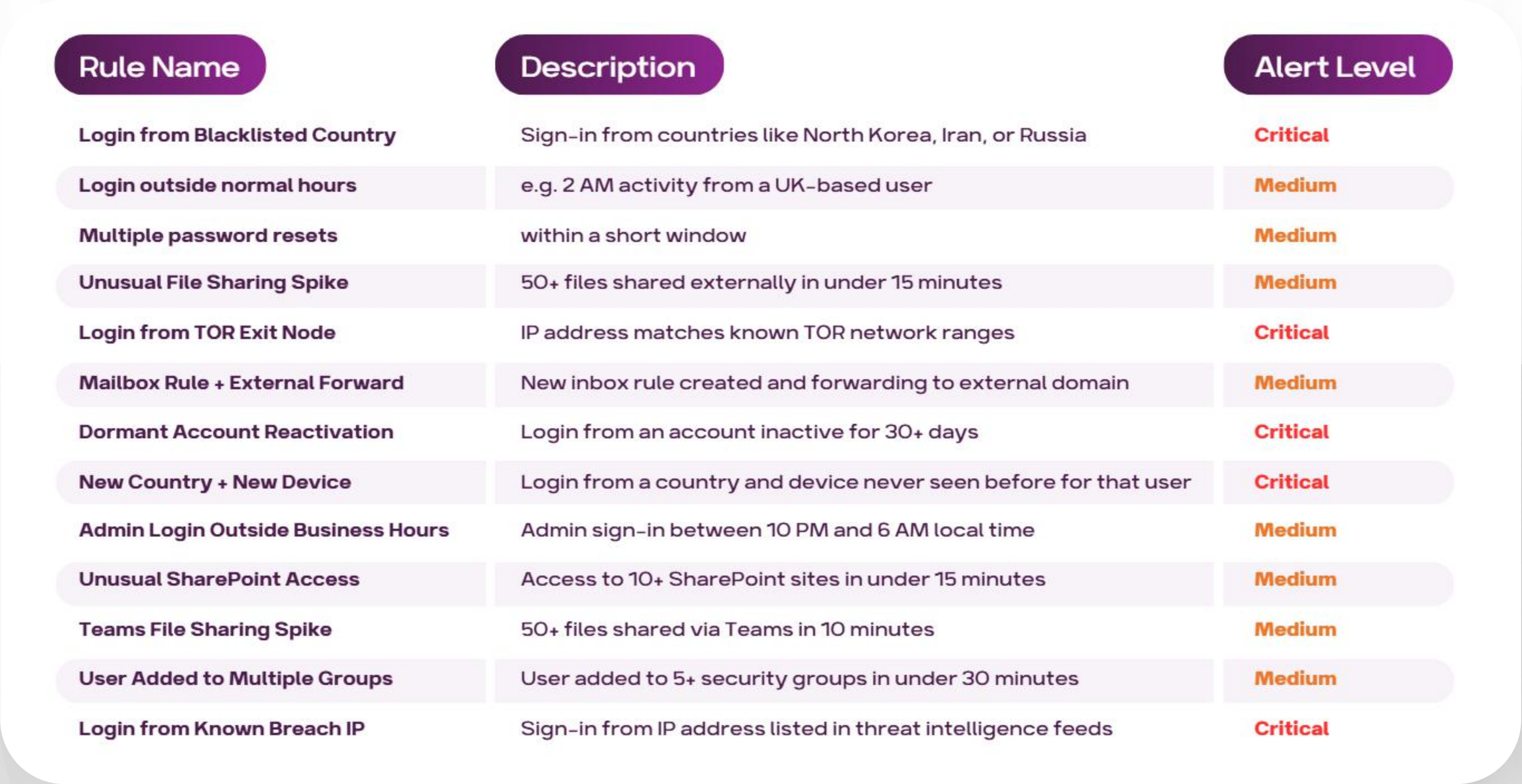


Organisation Vulnerability Assessments
Fortify helps teams share Microsoft Secure Scores and custom security tips with ease.

Streamline Microsoft Security Recommendations
Fortify speeds up security by applying Microsoft recommendations across tenants fast

Tailored To You – 50+ Automated Rules

Fortify applies Microsoft security rules across tenants in minutes—boosting protection and saving time. New automated actions are added daily to detect threats faster, trigger instant responses, and guide setup with clear rule descriptions.

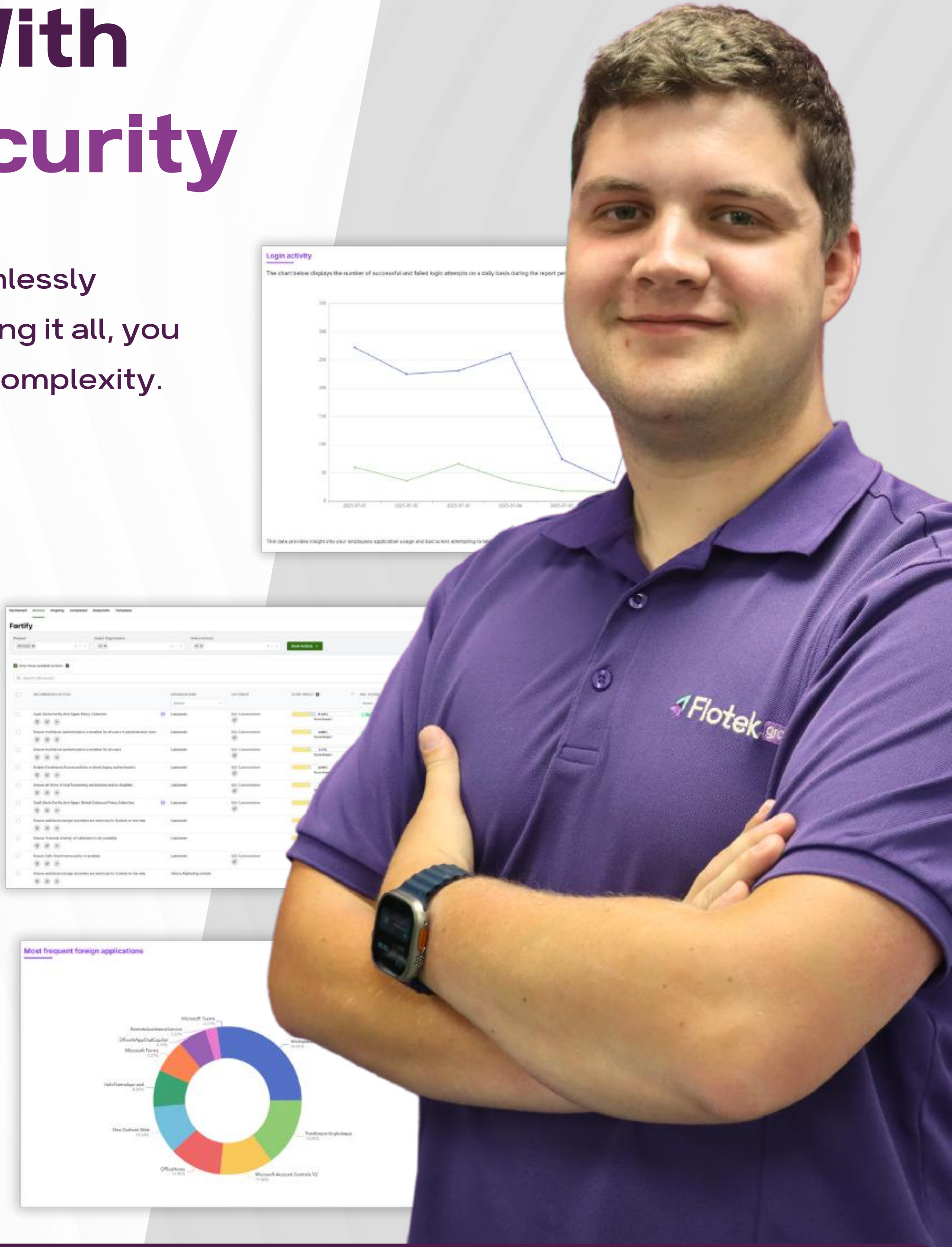


Rule Name	Description	Alert Level
Login from Blacklisted Country	Sign-in from countries like North Korea, Iran, or Russia	Critical
Login outside normal hours	e.g. 2 AM activity from a UK-based user	Medium
Multiple password resets	within a short window	Medium
Unusual File Sharing Spike	50+ files shared externally in under 15 minutes	Medium
Login from TOR Exit Node	IP address matches known TOR network ranges	Critical
Mailbox Rule + External Forward	New inbox rule created and forwarding to external domain	Medium
Dormant Account Reactivation	Login from an account inactive for 30+ days	Critical
New Country + New Device	Login from a country and device never seen before for that user	Critical
Admin Login Outside Business Hours	Admin sign-in between 10 PM and 6 AM local time	Medium
Unusual SharePoint Access	Access to 10+ SharePoint sites in under 15 minutes	Medium
Teams File Sharing Spike	50+ files shared via Teams in 10 minutes	Medium
User Added to Multiple Groups	User added to 5+ security groups in under 30 minutes	Medium
Login from Known Breach IP	Sign-in from IP address listed in threat intelligence feeds	Critical

Take Back Control With Intelligent Cloud Security

AI-driven threat detection and rapid response—now seamlessly integrated into CDR as a core module. With Flotek managing it all, you get peace of mind and powerful protection, without the complexity.

- ✓ 24/7 Detection & Response
- ✓ Monitoring & Alerting
- ✓ Monitor More Applications
- ✓ RMM & IT Docs Tool Monitoring
- ✓ Shareable Reports
- ✓ Security Configurations



Login activity

The chart below displays the number of successful and failed login attempts on a daily basis during the report pe

This data provides insight into your employees application usage and bad actors attempting to

Fortify

Most frequent foreign applications

FloCDR Package

Best In Market
24/7 Monitoring

Microsoft 365

Our pricing is per integration. All remediation is included in our premium IT support or available as project work.

We cover everything needed—making it aligned, scalable, and affordable for businesses of all sizes.

FloCDR License

£3.00 per month

Setup & Training Included

Free Microsoft 365 Security Report

Now Includes our Fortify add-on

Cloud Detection & Response (CDR) Licence

What's Included

- ✓ **Microsoft Integration**
- ✓ **Microsoft Defender**
- ✓ **Google Workspace**
- ✓ **Salesforce**
- ✓ **Okta**
- ✓ **Dropbox**
- ✓ **Slack**
- ✓ **CDR Alerts**
- ✓ **CDR Respond**
- ✓ **CDR Unify**
- ✓ **CDR Fortify**
- ✓ **Fortify Security Reports**
- ✓ **M365 Remediation****
- ✓ **Onboarding & Setup***

* Included on a minimum term of 36 months

**Included on Flo 360 & above support plans or charged as project work.

Flotek group

T: 0292150 8000

E: Hello@Flotek.io

W: www.Flotek.io

Unit 4,
Bocam Park,
Pencoed,
Bridgend
CF35 5LJ

Flotek Group Limited is Registered in England & Wales.
Company Number: 13882299
VAT Registration Number: GB 4060 18239