

Account Compromises are now the #1 way that businesses lose money to cybercrime.

It's not just an enterprise problem anymore.
With automation, attackers target companies of all sizes.



\$50 billion

lost to BEC in last decade.
#1 most costly cybercrime.



90%

of breaches worldwide
are caused by phishing.



29%

Identity-based attacks
result in wire fraud.



\$137,000

is the average cost per incident.



Financial risk

Account Compromises are the #1 way that businesses lose money to cybercrime according to the FBI. A full 29% of attacks left unabated lead to wire fraud, and the average cost of a wire fraud incident was \$137,000. Attackers tend to steal these funds by sending fraudulent invoices to clients. Given enough time in the account, attackers will also steal payroll and divert employee salaries before anyone notices.



Data risk

Once inside an employee account, an attacker will access and exfiltrate sensitive emails and files. These often include invoices, financial statements, passwords, tax documents, or legal documents. In-fact, attackers will often go straight to these documents upon gaining access, so every minute counts. Data is often sold on the dark web or re-used in other attacks in order to commit fraud or extortion.



Reputational risk

Attackers will often use the compromised employee account to send phishing emails to your clients. These emails tend to bypass spam filters and email protection because they come from your domain. Therefore, they're highly likely to compromise your clients. If your client loses money as a result of that breach, your company could be held legally or contractually liable.



Most of today's successful attacks bypass traditional email security.

Today's attacks don't rely on suspicious links or Nigerian princes—most come from trusted colleagues' hacked accounts and sail through email filters.

By coming from hacked trusted colleagues, they bypass traditional email security

These hackers also often use U.S.-based IPs and social engineering to walk straight into your inbox.

Petra detects and stops these attacks that bypass email security filters, and even those that get past MFA.

Monitoring M365, we stop today's attacks **before** they cause damage.

By monitoring your M365 environment 24/7, we stop account compromises, today's #1 costliest cybercrime, before they cause data leaks, reputational damage, or financial damage such as wire fraud.



Stop threats that get past email security.

Monitoring your M365, we **identify account compromises within on average 3 minutes**, stopping attackers before they access sensitive files, send phishing emails to clients, or modify invoices.



Prevent client-facing fallout.

When attackers gain access, they send phishing emails from your domain. Monitoring your M365, we **stop attacks before clients are affected**, so you avoid legal risk and reputational fallout.



Stay secure without losing access.

Leveraging deep behavioral analytics, we can **avoid locking out employees** while they're traveling and using VPNs. Behavioral M365 monitoring is how we **keep your business secure while preventing disruption**.



75%

of today's successful attacks **bypass MFA**. Attackers prompt the user to enter their MFA code. **Monitoring M365, we can stop these attacks.**



73%

of today's successful attacks are **U.S.-launched**. Many don't even use a VPN. **Monitoring M365, we can stop these attacks.**



91%

of today's attacks are **automated**. Attackers are fast and go straight for the crown jewels. **Monitoring M365, we can stop these attacks.**



Why account protection matters

Attackers no longer rely on sloppy phishing emails. Many use compromised accounts from trusted colleagues, sending messages that appear completely legitimate to email filters, often containing Microsoft-laundered links to shared documents or invoice requests.

Others arrive by text or collaboration platforms. These messages don't trigger spam filters, and because they appear from trusted colleagues, your team is far more likely to click. By monitoring M365, we can stop these attacks before they cause damage.