

# Insider threats

Is your organization at risk?






IP theft costs the U.S. economy more than

## \$250 billion annually<sup>1</sup>

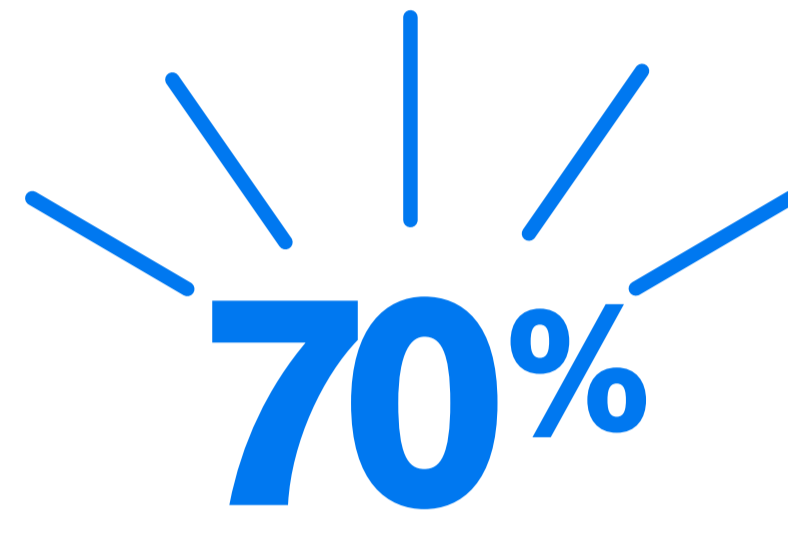
## The new insider threat

It's not what you think!

-  - Poorly secured, personal mobile devices
-  - Contractors, branch office employees and "trusted" partners
-  - Privileged insiders (executives and IT admins)

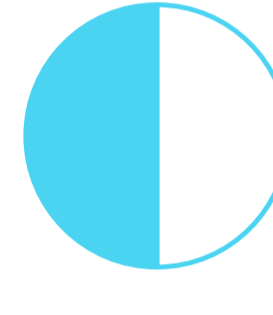
## The odds

are against you!  
According to a survey...



...of incidents were caused by "internal actors."<sup>2</sup>

And in another survey...<sup>3</sup>



50% email business documents to their personal accounts.



33% move corporate documents to unapproved file-sharing services.



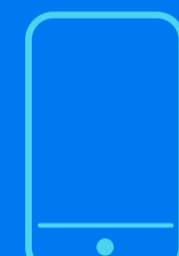
40% shuttle work files to their mobile devices.



## 8 signs you're in danger of insider threats.



1. Your BYOD strategy focuses on blocking users, not controlling their access.



5. You can't track and wipe mobile devices that leave the building.



2. Your top executives aren't bound by corporate security policies.



6. You don't manage how employees store things in hard-to-track places.



3. You grant access to third parties without control.



7. You don't review user access rights regularly.



4. Your security tools do not automatically revoke privileges.



8. You can't monitor the activities of privileged users.

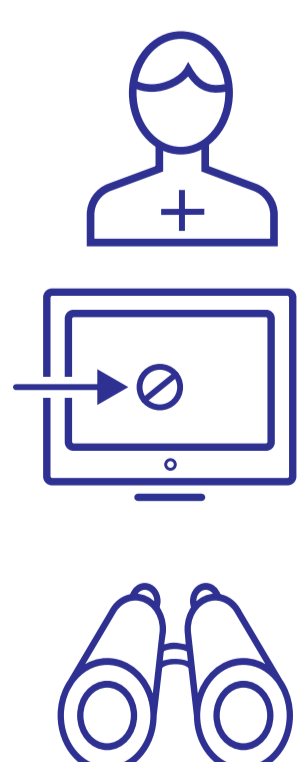
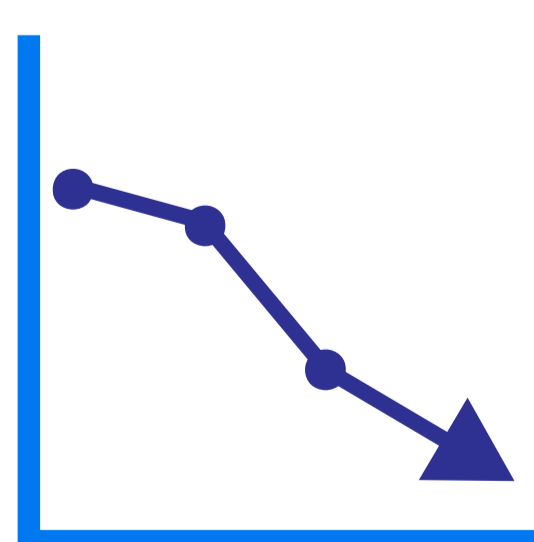
It's getting worse...

# 54%

of IT and Security Pros

believe that **insider threats** are more difficult to detect and prevent today than they were in 2011.<sup>4</sup>

## How can you reduce risk?



Reduce number of privileged users

Only grant access needed

Monitor privileged users activity

Learn how you can reduce your risk from insider threats.

Visit <https://www.netiq.com/solutions/identity-access-management/monitor-privileged-users.html>

Start reducing insider risk >