bitglass

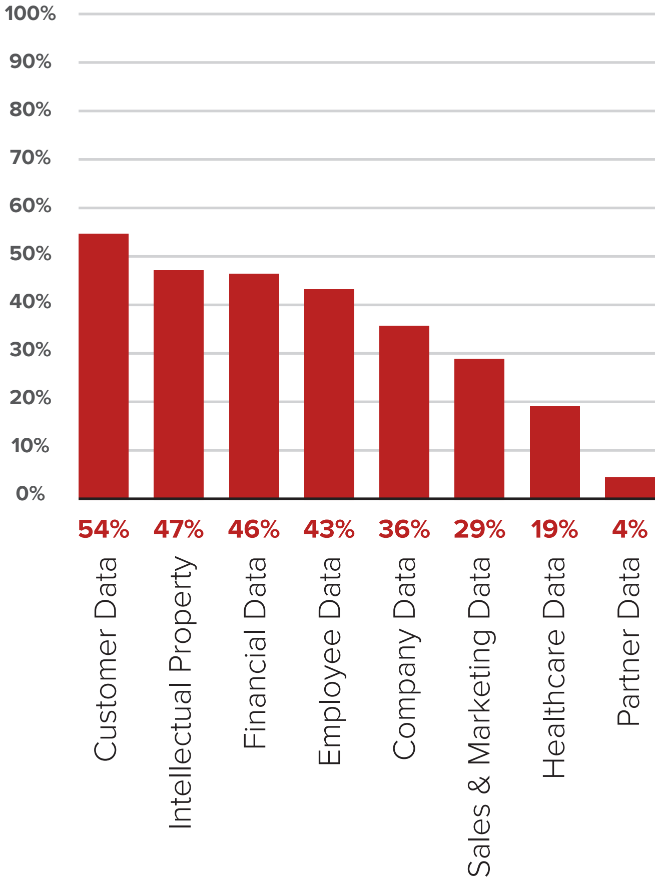
2020 Insider Threat Report

Insider threats are a significant danger to any organization. Disgruntled or careless employees as well as hackers who gain access to valid credentials can do massive damage to an enterprise. Consequently, IT and security teams are forced to balance budgetary and business concerns with the need for comprehensive data and threat protection. Unfortunately, as the IT ecosystem evolves and organizations migrate to the cloud, shift to remote work, and enable BYOD policies, defending against insider threats can become highly challenging. To uncover the state of security when it comes to insider threats, Bitglass partnered with a leading cybersecurity community to survey IT and security professionals about their organizations.

Data and the Cloud

54% of survey respondents said customer data was the most vulnerable to insider attacks. This is sensible given the massive compliance and privacy concerns associated with customer information, as well as the fact that it is desirable for malicious parties looking to sell it to make a profit. Unfortunately, 50% of firms find it harder to detect insider threats after migrating to the cloud. Traditional on-premises tools don't translate well to the cloud, calling for a new approach to security to keep information like customer data safe from insider threats.

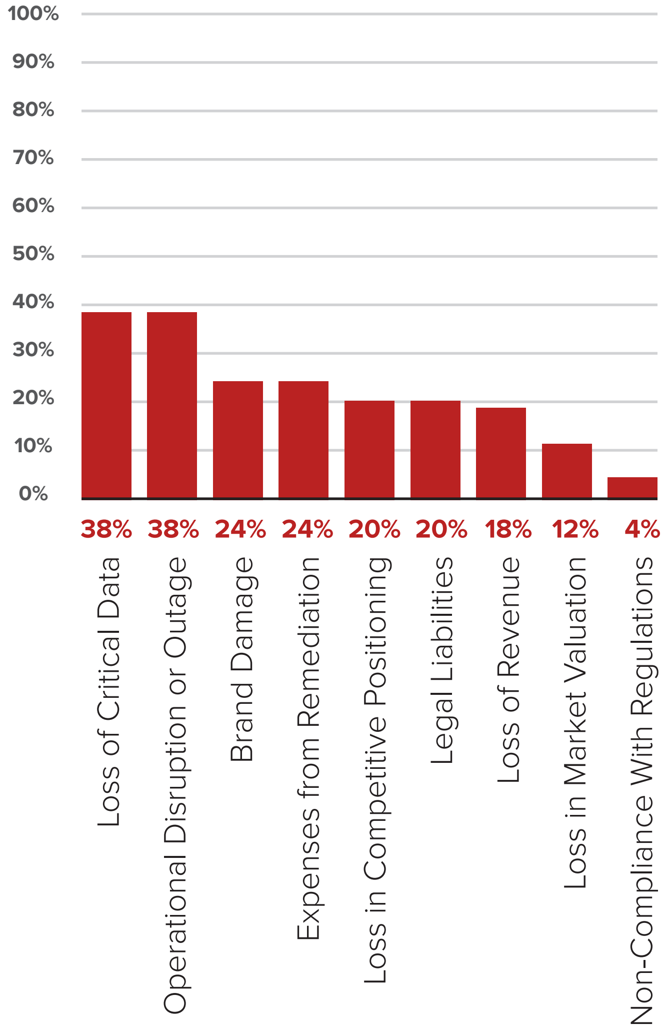
What types of data are most vulnerable to insider attacks?



The Effects of Insider Attacks

Loss of critical data is the most obvious repercussion of insider attacks, but disruption to business operations is tied with it at 38% as the most commonly cited outcome. While some enterprises overlook this aspect of security in favor of more salient items like brand damage (24%), legal liabilities (20%), and loss of revenue (18%), having operations grind to a halt can be just as damaging. Unfortunately, 61% of those surveyed experienced an insider attack in the last 12 months (22% reported at least six). It is for these reasons that organizations need security solutions that boast maximum uptime and performance and stop threats around the clock.

What impact have insider threats had on your organization?

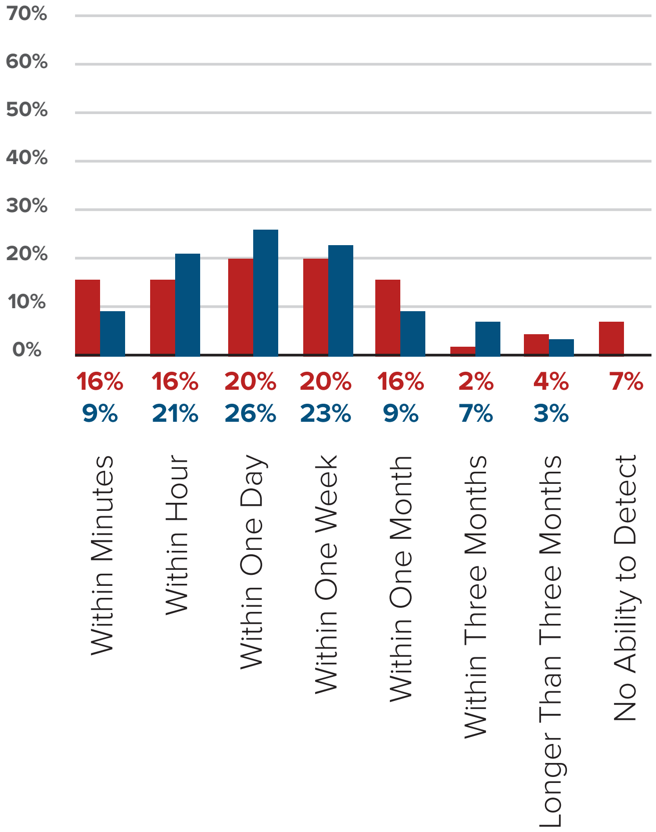


Detection & Recovery

Due to the potential for data leakage and, consequently, noncompliance in the cloud, organizations need to maintain real-time visibility and control over data that has gone beyond the reach of on-premises security tools; this is key for any business' livelihood. However, 49% of respondents stated that at least a week typically goes by before insider attacks are detected. Additionally, 44% said that it would take another week or more to recover from such an attack. Reactive security tools and strategies are not able to keep pace with today's dynamic business environment; instead, organizations require automated, real-time protections.

How long would it typically take your organization to detect an insider attack?

How long would it typically take your organization to recover from an insider attack?



The Finances of Security

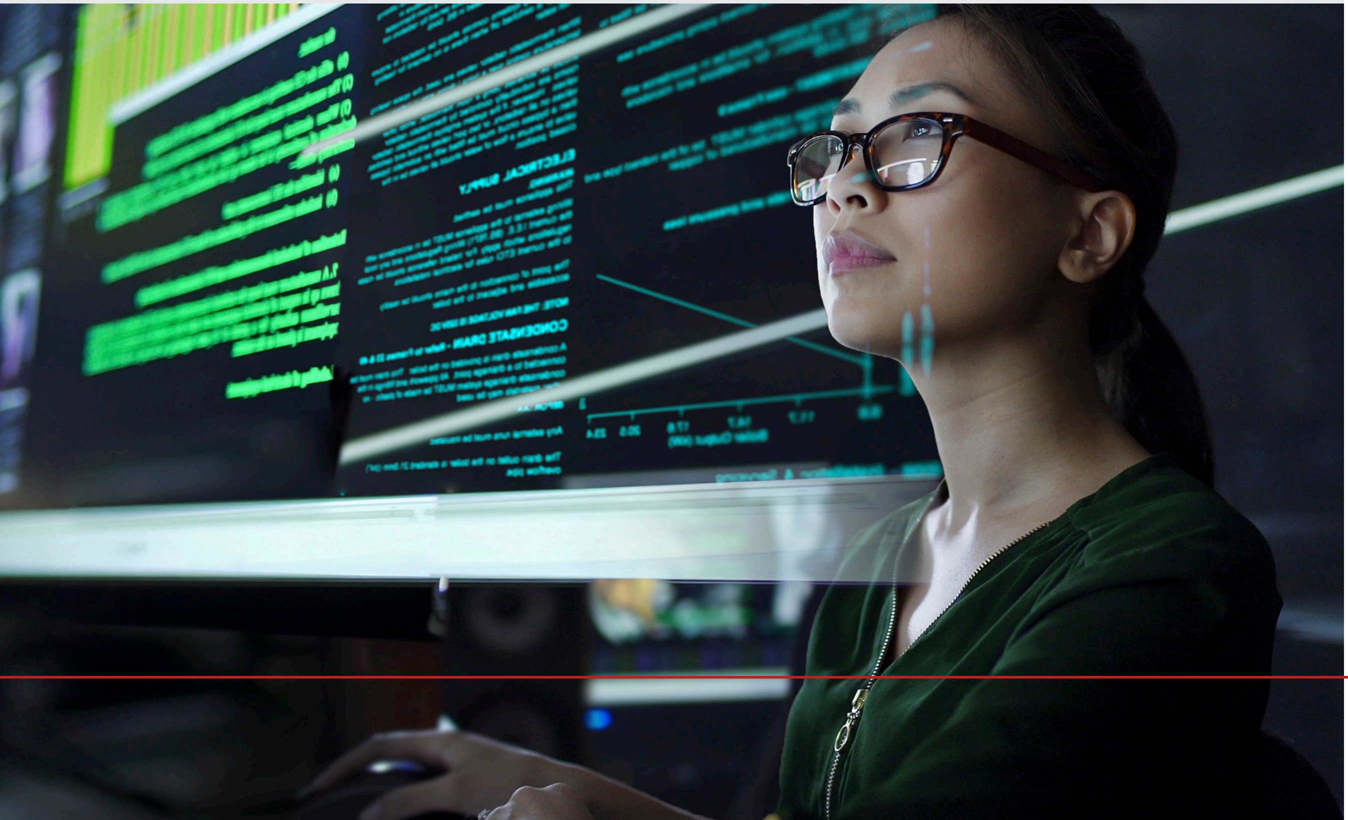
By preventing breaches in a proactive fashion, organizations are able to save significant sums of money that would otherwise be used for legal fees, compliance penalties, and reclaiming their reputational footing. 32% of surveyed organizations affirm that the average cost of remediation after an insider attack is $100K to $2M. Even when costs are less than $100K, they can add up quickly when multiple attacks occur. With 73% of respondents saying that their security budgets are staying flat (57%) or decreasing (16%) next year, organizations are being tasked to do more with less. In other words, they need cost-effective security measures now more than ever; compliance, security, and business success depend on it.

32% of companies volunteered that the cost per insider attack is between $100K and $2M.

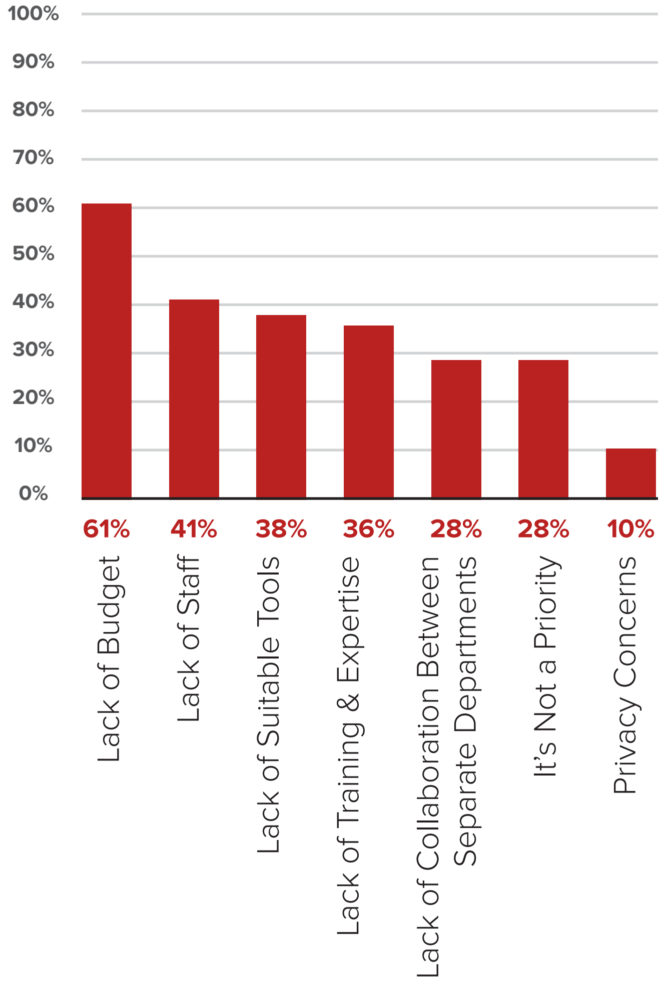
73% of security budgets are decreasing or staying flat over the next twelve months.

Challenges to Proper Security

81% of organizations find it difficult to assess the impact of insider attacks. This suggests that most firms lack the needed levels of visibility and control. Unfortunately, according to survey respondents, the top three barriers to better insider threat management are lack of budget (61%), lack of staff (41%), and lack of tools (38%). These items highlight the challenge faced by IT and security teams: they are tasked with complex security use cases that must be addressed continuously despite significant budgetary constraints. These teams would benefit greatly from easily manageable, cost-effective platforms that meet a breadth of security use cases.



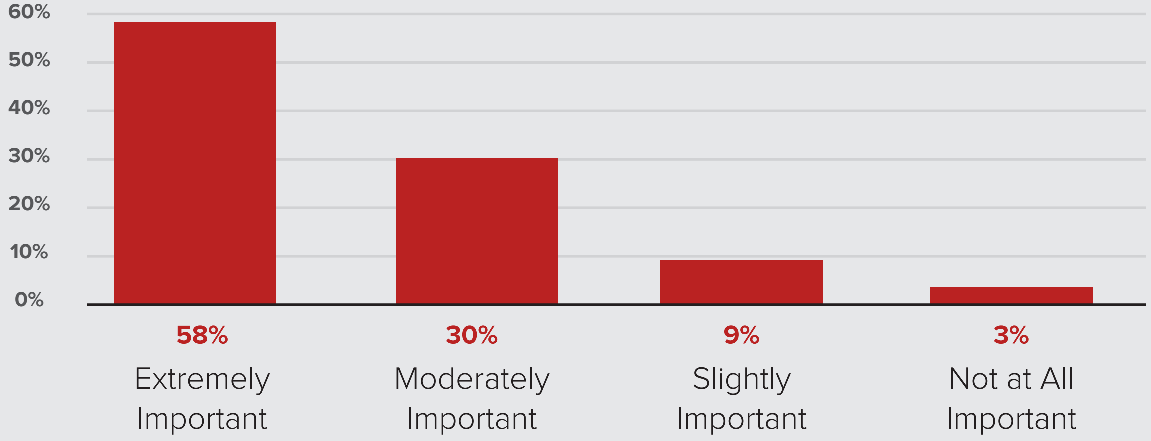
What are the biggest barriers to better insider threat management?



Consistent Visibility & Control

88% of respondents recognize that unified security across apps, devices, on-prem resources, infrastructure, and the web is important for counteracting insider threats. Unfortunately, 61% of respondents lack unified or comprehensive security, and are tasked with managing multiple, disjointed solutions that provide varying levels of protection. This means that most security professionals have to spend inordinate amounts of time managing a number of unintegrated products, and lack the comprehensive, consistent security that they need to protect data and defend against threats.

How important is unified visibility and control across all apps, devices, web destinations, on-premises resources, and infrastructure when it comes to insider threats?



What level of unified visibility and control do you currently have across all apps, devices, web destinations, on-premises resources, and infrastructure to detect insider threats?

6% A single product/dashboard delivers completely unified visibility and control wherever data goes

33% Multiple but integrated products provide unified visibility and control wherever data goes

27% We have partially unified security, but still have to manage disjointed solutions from different dashboards

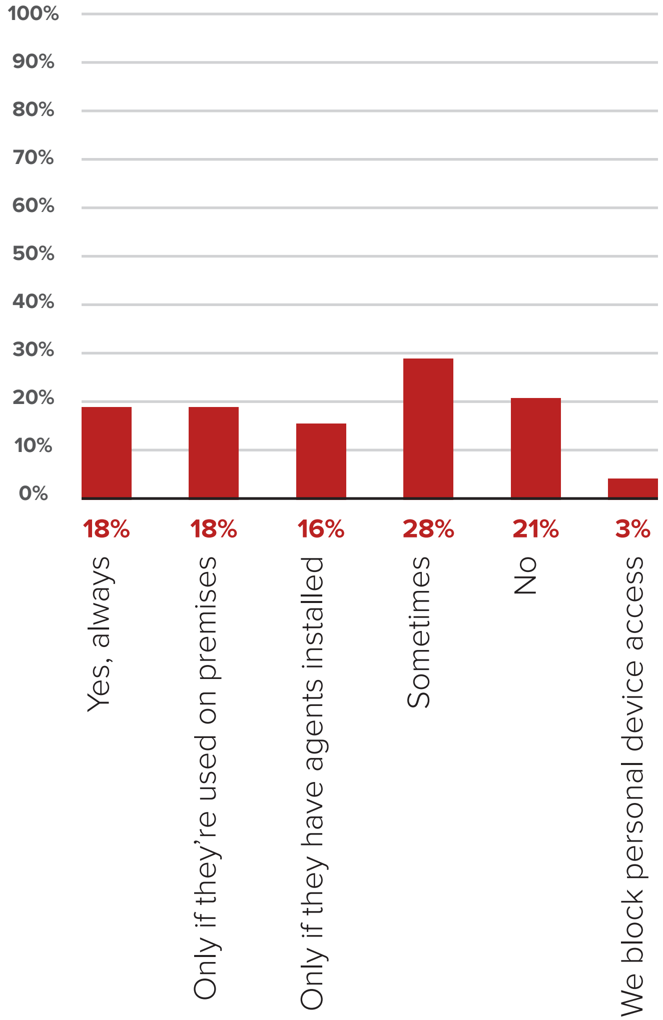
15% We have completely disjointed and disparate security solutions monitoring each of the above areas

18% We don't have the proper tools for securing all of the above areas—let alone integrated tools

Threats on Personal Devices

The rise of the remote workforce and the resulting surge of unmanaged devices syncing corporate data in 2020 have served as catalysts for BYOD (bring your own device) adoption. Unfortunately, 82% of organizations cannot guarantee that they can detect insider threats stemming from personal devices. Often, other criteria need to be met in order for them to do so; for example, having the personal devices on premises (18%) or ensuring that they have agents installed (16%). Additionally, half of organizations don’t have visibility into messaging and file sharing apps on BYO endpoints. Lacking personal device oversight makes it highly challenging to defend against insider attacks which often take advantage of BYOD policies. Notably, only 3% of organizations block personal device access altogether; this is because of the manifold productivity and flexibility gains that BYOD provides.

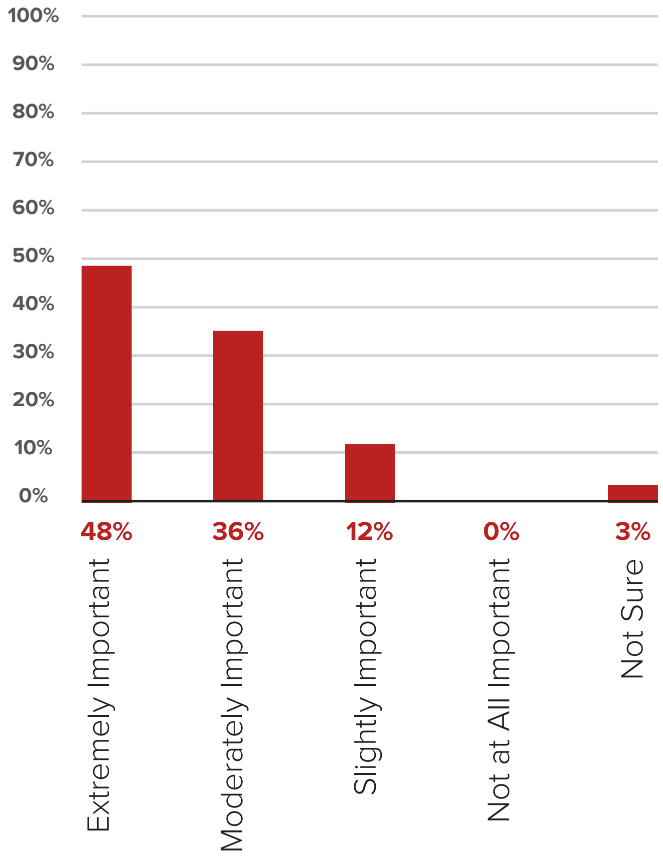
Can you detect insider threats stemming from personal mobile devices?



The Importance of Performance

84% of surveyed organizations agree that security performance and uptime are essential for preventing insider threats; not to mention the fact that security downtime typically disrupts business continuity and prevents employees from doing their jobs. As security solutions' architectures invariably affect their uptimes, organizations need to leverage tools that are designed for the highest levels of performance. Typically, such solutions will be deployed in the public cloud, taking advantage of the world's fastest and most reliable networks, and will forgo the use of costly hardware appliances that become performance bottlenecks as companies grow or their load profiles shift.

How important is security solution uptime and performance for stopping insider threats in the cloud (for SASE, CASB, SWG, etc.)?



Wrap-Up

In order to thrive in a highly remote and dynamic business environment, organizations must ensure that they are deploying sound security solutions. These tools must stop insider threats, extend secure access to sensitive data, and be performant, scalable, and cost effective--around the clock and across the globe. Unfortunately, many organizations are still struggling to deploy security platforms that can meet the demands of modern business. These enterprises need multi-faceted security solutions that provide items like the following:

- User and entity behavior analytics that use machine learning to baseline user behavior and identify suspicious departures from the norm
- Step-up, multi-factor authentication for users in unusual locations or for those who are engaging in unusual activities
- Real-time data loss prevention capabilities like digital rights management and redaction that can prevent data leakage
- Cloud encryption for sensitive files and fields in order to keep confidential or regulated data safe from prying eyes
- Agentless deployment modes that don't require software installations on endpoints; critical for BYOD security

At Bitglass, we pride ourselves in our Total Cloud Security Platform and its ability to secure any interaction between any device, app, on-premises resource, web destination, or infrastructure. Our SASE offering provides all of the above functionality in a cost-effective, cloud-based architecture that delivers maximum uptime, scalability, and performance. Want to see it in action? Request a free trial today.

2020 Insider Threat Report

Phone: 408.337.0190
Email: info@bitglass.com

www.bitglass.com

About Bitglass

Bitglass' Total Cloud Security Platform is the only secure access service edge offering that combines a Gartner-MQ-Leading cloud access security broker, the world's only on-device secure web gateway, and zero trust network access to secure any interaction. Its Polyscale Architecture boasts an industry-leading uptime of 99.99% and delivers unrivaled performance and real-time scalability to any location in the world. Based in Silicon Valley with offices worldwide, the company is backed by Tier 1 investors and was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution.