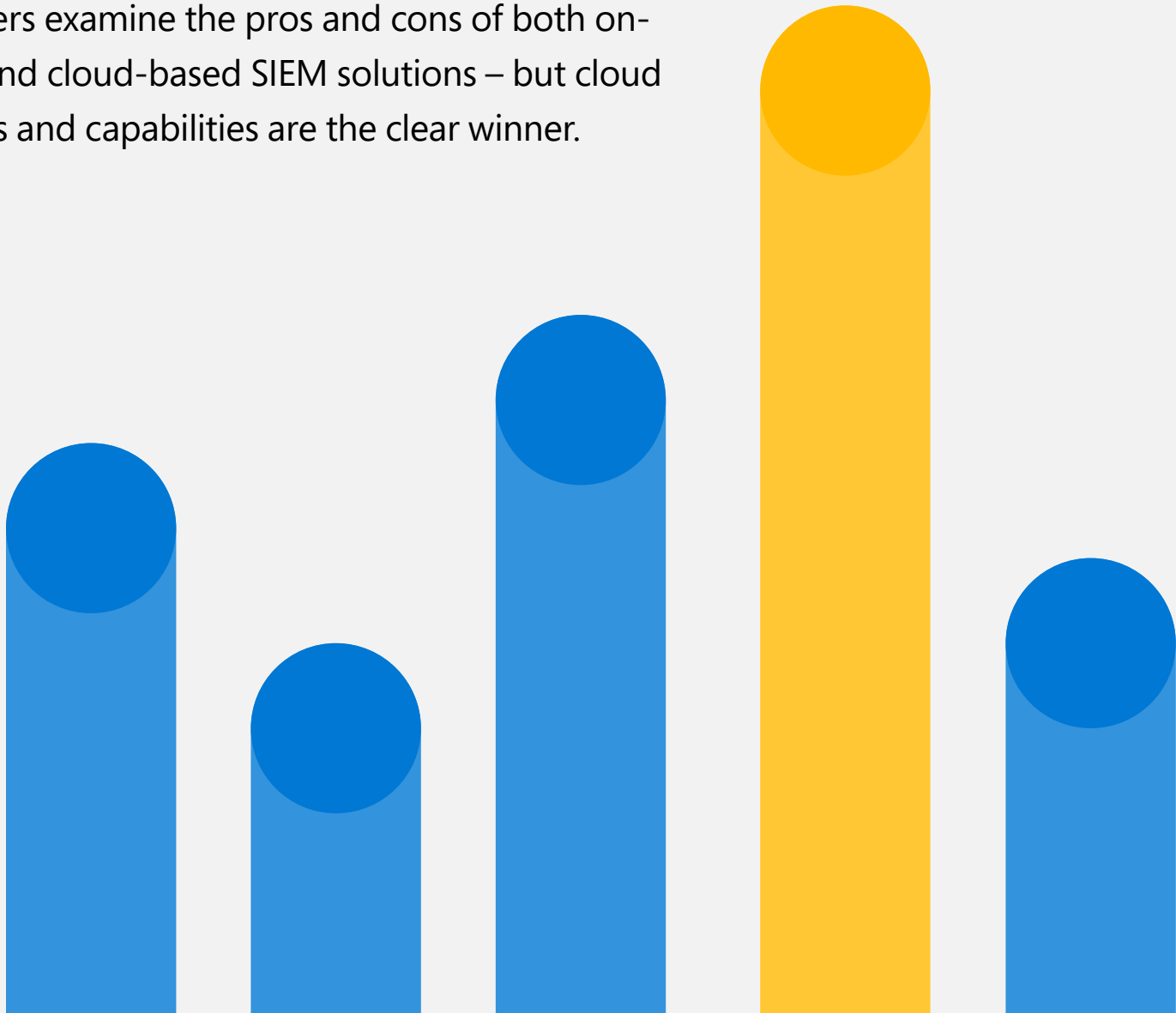
Microsoft Security

SIEM Shift:

# How the Cloud is Transforming Security Operations

IT leaders examine the pros and cons of both on-prem and cloud-based SIEM solutions – but cloud services and capabilities are the clear winner.



## IT security is always a top priority among CSOs and CISOs. However, it's becoming more urgent and challenging.

Threats are evolving just as quickly as data-volume growth, with bad actors exploiting every possibility and technique to gain access to the corporate network. At the same time, the risk surface has widened as companies shift to hybrid-cloud environments, adopt DevOps and Internet of Things (IoT) technologies and expand their remote workforces.

Amid this landscape, CSOs and CISOs require a bird's-eye view of security posture across the enterprise. And they're trusting their security information and event management (SIEM) systems to carry the day.

Yet, to mitigate a myriad of challenges associated with on-premises SIEM solutions, there is an emerging shift toward cloud-based SIEM models, according to new quantitative and qualitative IDG research conducted among security and IT leaders.

"**There are a lot of benefits [to cloud SIEM]… stability, providing additional load without performance tradeoff, scalability and maintenance**," said the senior security solutions architect of a telecom company, which two years ago migrated from an on-prem SIEM solution to the cloud.

The IDG survey revealed numerous considerations around how SIEM – both on-prem and cloud-based – addresses organisational challenges. This report examines the results, including:



> **There are a lot of benefits [to cloud SIEM]… stability, providing additional load without performance tradeoff, scalability and maintenance."**
>
> – Senior security solutions architect, telecom company

# Cost Factors

Organisations have made significant investments in security technologies and practices (see Figure 1). IDG found the overall average annual security budget is USD $8.7 million; companies with less than 10,000 employees are averaging USD 3.7 million and that rises to USD 19.7 million for larger enterprises.

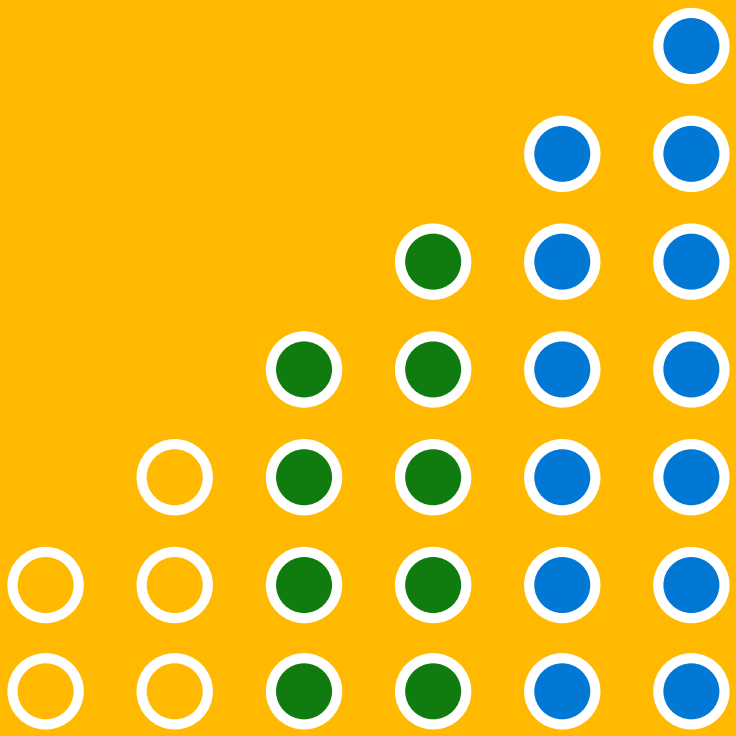


Figure 1.

## Security in Numbers

**97%** — **Encrypt sensitive data**

**68%** — **Deployed SIEM solutions three plus years ago**

**91%** — **Replicate sensitive data to secondary systems**

**45** — **Average number of SOC employees**

Source: IDG

Specifically, organizations are heavily investing in SIEM, averaging USD 580,000 per year for staffing, infrastructure, licensing and ongoing software costs.

Results show the shift toward SIEM in the cloud has begun. Today, 68% of respondents use an on-prem solution. Among the cloud SIEM deployments, the majority (57%) made the migration in the past two years. It appears that a primary reason for this migration is cost.

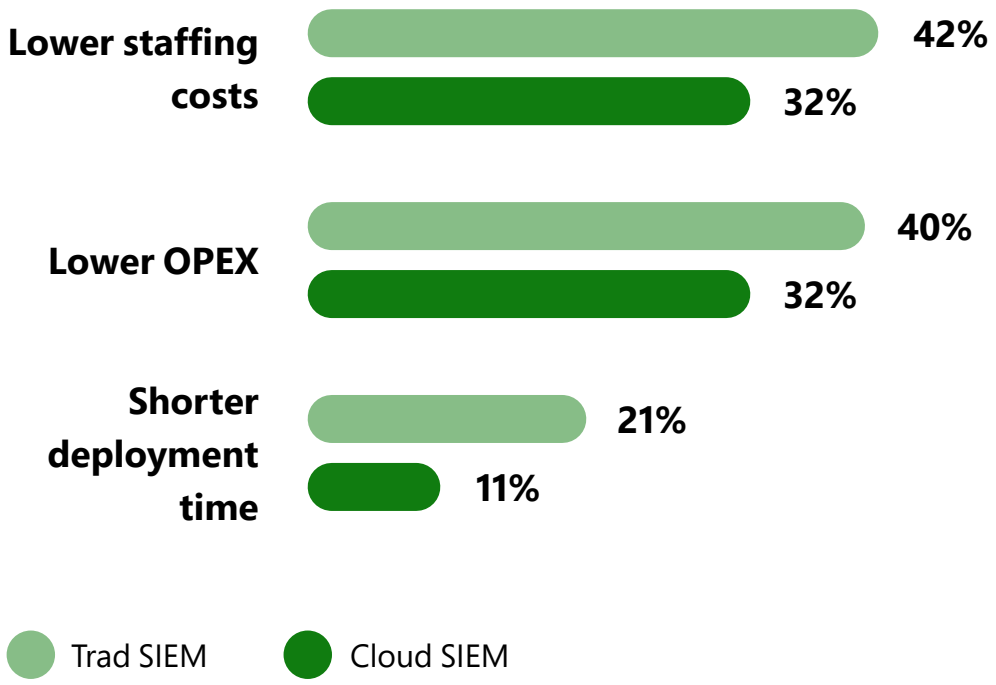
On-prem users are averaging USD 607,000 per year for maintenance, staffing, infrastructure, ongoing software costs and licensing. Cloud-based SIEM solutions cost substantially less to support: an annual average of USD 541,000, or 11% less than on-prem.

So, it's not altogether surprising that cost was the top answer – particularly among on-prem users – when respondents were asked: Assuming you could change your SIEM solution tomorrow, which outcomes would you most like to realise? (see Figure 2).

> **Overall, I think that the biggest challenge [with on-prem] is cost. It's more expensive."**
>
> – VP of technology, financial firm

Figure 2.

## Desired SIEM Outcomes



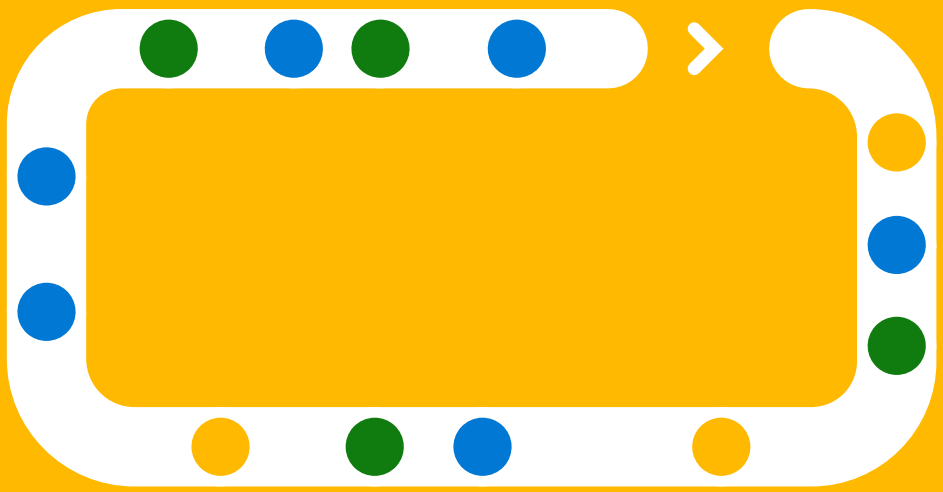

Source: IDG

"Overall, I think that the biggest challenge [with on-prem] is cost," said a VP of technology, whose financial firm is using an on-prem solution. "It's more expensive. The SIEM doesn't typically have a tremendous amount of infrastructure but the licensing fee… that's large. Also, to get people to maintain it… that's pretty expensive."

As with any move to the cloud, there are cost efficiencies to be gained – particularly when companies don't have to build out and then manage/maintain a supporting infrastructure. "For example, we found out that when you move from on-prem to cloud, the overhead and administration and regularly refreshing the technology is pretty much mitigated," said the head of architecture, security and privacy for a digital media services company.

# Performance Efficiencies

Given the increase in data volume, applications and devices, it's no surprise this growth is also straining other areas, creating concerns around performance, resiliency and capacity.



The financial services VP of technology explained that his on-prem SIEM solution, "becomes a potential single point of failure if it were to experience an issue. If you were to have a performance challenge when you have your own environment, that means that you can't just turn on additional compute power. If you're having a storage challenge, you can't just magically automatically add more."

In other cases, companies struggle to easily make meaningful correlations. The inefficiencies and risks around not being able to aggregate reports became critical factors behind the digital media company's move to cloud-based SIEM two years ago.

"That's where the investment [in cloud SIEM] justifies itself," said the company's head of architecture, security and privacy. "Think about the delay that gets introduced when you have to compare data you're gathering on-prem to data that is available on the cloud. You now have introduced two network hops. If it's on-site, you can hit the most targeted use cases, but you cannot have that aggregated intelligence that will help you prevent really big incremental strategic attacks that people always launch on you."

**In addition, the telecom senior security solutions architect sees several other performance efficiencies with his cloud SIEM solution:**

- ✓ **Improved response times.** This can be managed and enforced through service-level agreements, he said, adding: "The closer the ingestion point, the better performance there is."
- ✓ **Better user experience.** "[With on-prem SIEM], we had to make sure we were not running real-time data searches and restrict the number of searches. Now, that's no longer the case. As a user, definitely performance improvement."

> **[With on-prem SIEM], we had to make sure we were not running real-time data searches and restrict the number of searches. Now, that's no longer the case. As a user, definitely performance improvement."**

– Head of architecture, security and privacy, digital media company

# Handling Alert Fatigue

No matter which SIEM model they're using, respondents are worried about burnout from handling a growing volume of alerts. Across the board, alert fatigue is causing longer response times. However, it has a disproportionate impact on on-prem SIEM users (see Figure 3).

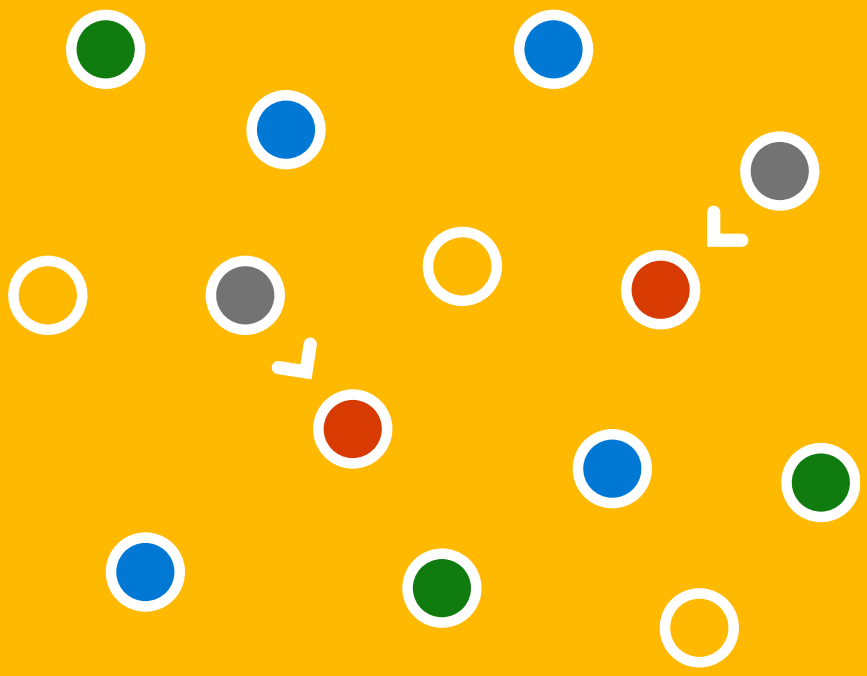
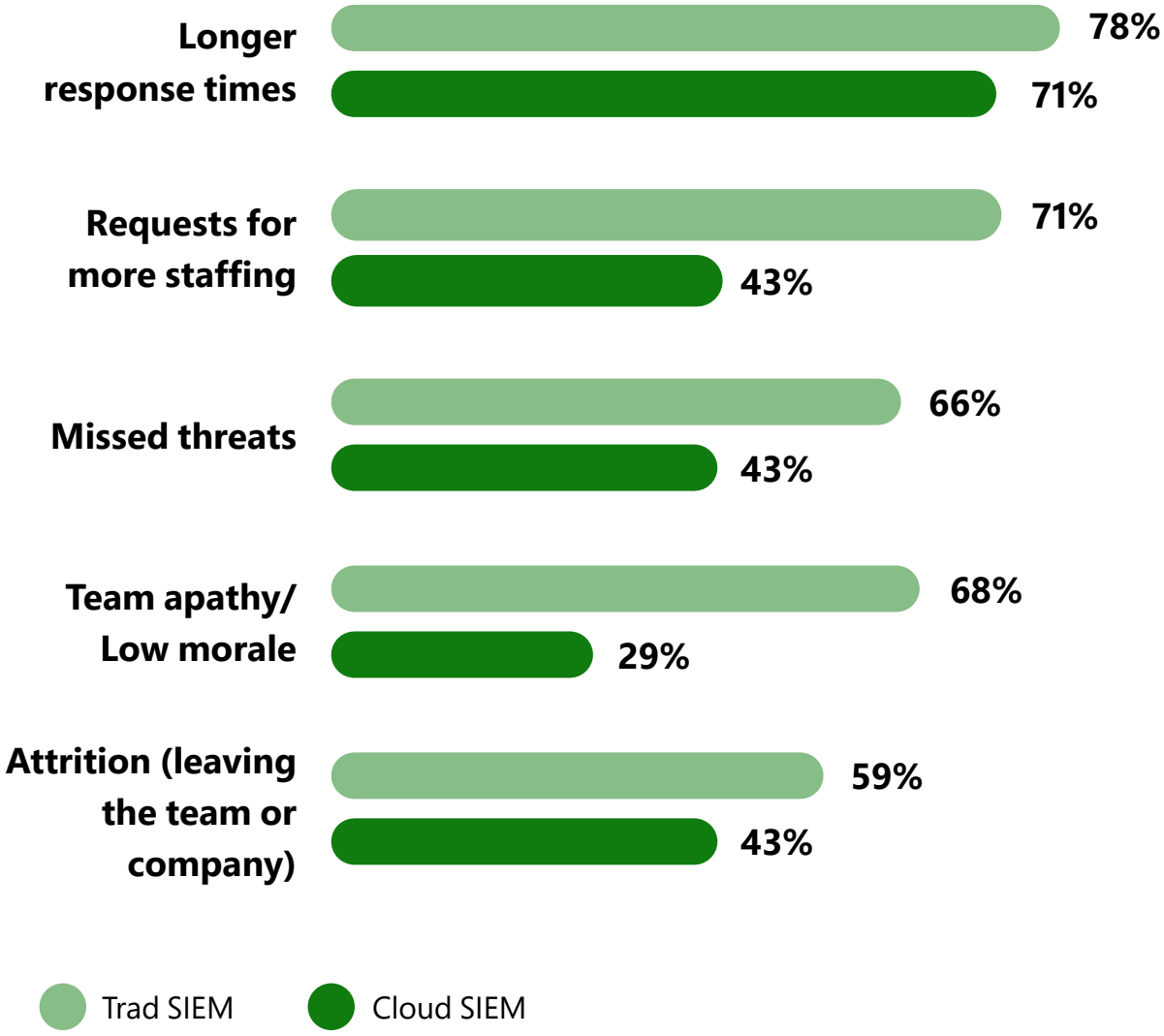


Figure 3.

# The Effects of Alert Fatigue on IT Staff




Source: IDG

A senior principal architect interviewed by IDG said he thinks alert detection and response are, "probably the harder parts of the job. A lot of time is spent chasing things that aren't necessarily real. There's never a let up, and if there is, we start worrying that something is wrong: 'Why aren't things going off? Something's not working'."

# Creative Staffing:

IT leaders should work closely with their HR counterparts to ease the challenge of finding qualified security skill sets.

**IDG respondents offered the following ideas:**

**"We send our people to training. Then we augment them with some people who are just coming into the workforce."**

– Senior principal architect, financial services

**"We support different non-profit organisations that offer technology training to different individuals around the United States. We support internships, and then we hire from that pipeline, and we train them ourselves."**

– Executive vice president of IT, financial services

**"We hire a lot of co-ops from universities and then convert them into full-time SOC analysts."**

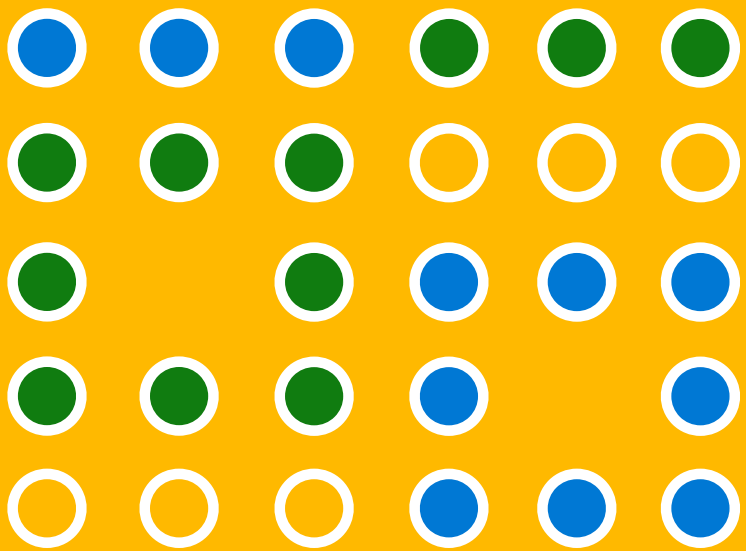
– Vice president and CISO, software provider

Shifting to cloud SIEM can help alleviate chasing down false positives and thus create efficiencies like reducing the mean time to respond. For example, the telecom solutions architect said his cloud-based SIEM sends alerts to an automated solution, also in the cloud, that spins out a workflow to manage events.

This sort of efficiency can increase over time with a cloud-based SIEM, as organisations tie automation solutions to critical business applications.

# Staffing Concerns

Another issue that shows no signs of abatement is finding, training and retaining qualified staff. Despite 81% saying their security operations centres (SOCs) are adequately staffed, respondents admit their security personnel are spending far more time (60%) on routine IT operations tasks versus security-related functions (27%).



**On-prem or in the cloud, organisations are averaging 27 full-time employees to carry out SIEM-related infrastructure, maintenance and training tasks**. And yet for companies hosting these solutions in their data centers, security staffing issues are acute. Half of their SOC employees are devoted solely to supporting SIEM, according to the research.

> "Internal skills are definitely a challenge," said the vice president and CISO of a software company. "We hire them and get them trained on [SIEM]. Then, once they have this skill set they become more attractive to other employers who may want to short-circuit the process and hire your trained employees."

To circumvent the ongoing global security skillset challenge, on-prem SIEM users are going to greater lengths to procure personnel (see Creative Staffing box).

By comparison, however, practitioners whose companies had deployed a cloud SIEM solution specifically called out the benefit of freeing their security teams to focus on other tasks. And for some, the staffing challenge has become the basis for moving to a cloud-based SIEM.

> "If you think about something that's on-prem, you need significant server administration skills, you need app management-specific skills, you need networking skills," said the CIO of a technology services company, which migrated from on-prem to cloud. "It's a whole host of skills to provide the care and feeding for it that you don't need for cloud."

Cloud-based SIEM creates staffing efficiencies by shifting that pressure to a provider whose core competency is SIEM management – at scale. For example, SIEM solutions on average collect data from 31 different sources, according to the research. Cloud SIEM can automate analysis of all this data. In addition to eliminating manual work, this frees up IT and security staff for more strategic work.

> **If you think about something that's on-prem, you need significant server administration skills, you need app management-specific skills, you need networking skills."**

– CIO, technology services company

# The Migration to Cloud SIEM

Based on the IDG research, all these challenges – costs, performance, alert fatigue and staffing – are key pieces of the SIEM-to-cloud migration story (see Figure 4). “Running on-prem, we just didn’t have the capital or the hardware to keep up,” said the telecom company’s senior security solutions architect. “It was decided to move to the cloud, where we pretty much had unlimited scalability and redundancy.”

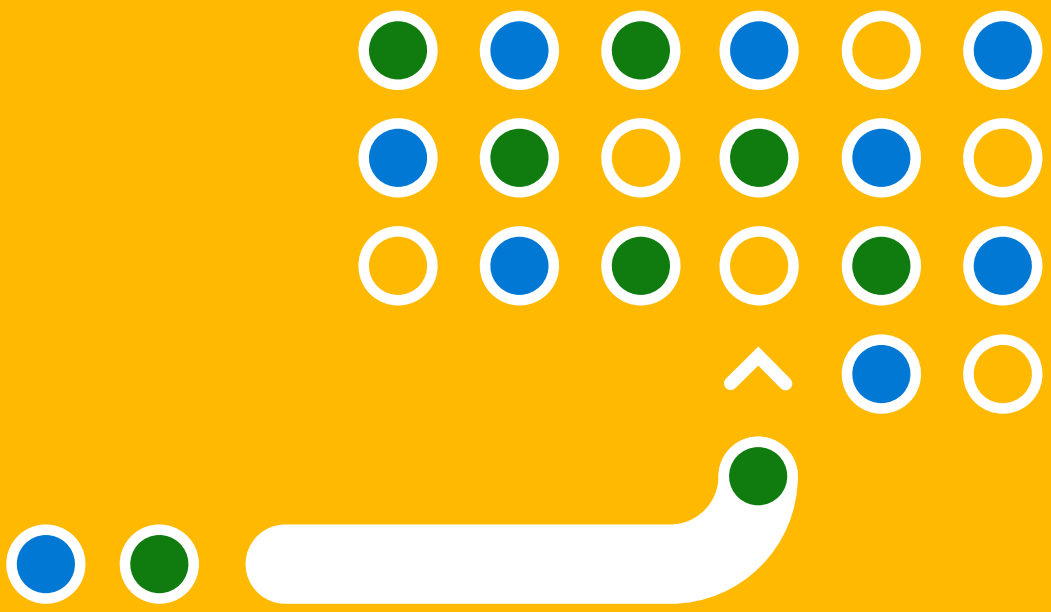
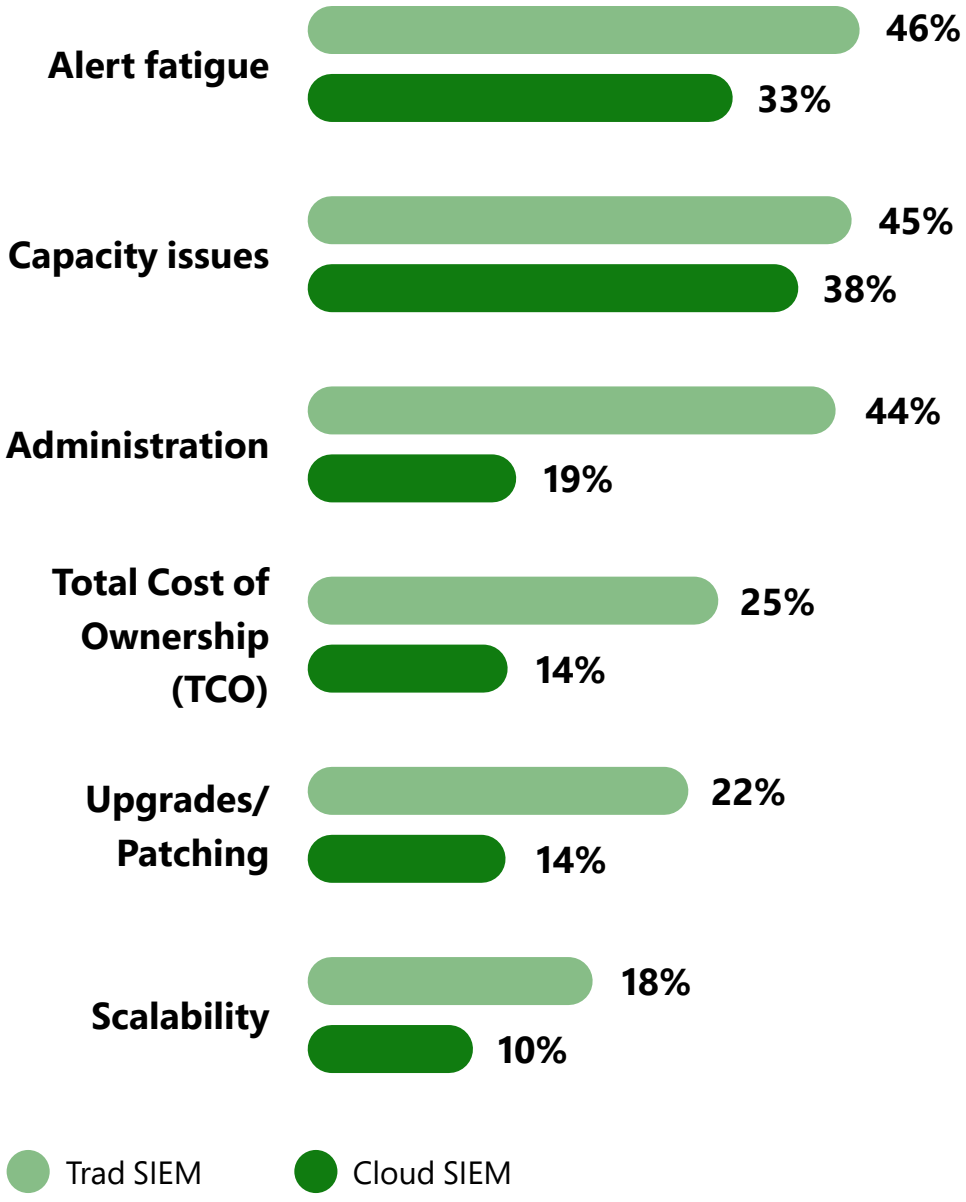


Figure 4.

## Shift to Cloud SIEM reduces occurrence of key challenges




Source: IDG

Cloud adopters – who report using solutions such as Microsoft Azure Sentinel, QRadar and Splunk – also report greater speed in retrieving and analysing data, as well as the ability to handle multiple data sources.

This could be because they're leveraging automation at a higher rate (50%) than traditional SIEM users (26%).

"We could handle a huge volume of logs, and we could process them really quickly," explained the CISO of an electronics company that uses cloud-based SIEM.

**Over time, additional benefits come to light, according to organisations that have been using cloud-based SIEM for two plus years:**

**Insight acceleration.** "The ability to get data from [SIEM] and bring that into the business... It's something we couldn't do before. It was not stable enough or secure enough, and sometimes it was lagging behind in upgrades and features, but that's not the case anymore. Now we can capitalise on the data that we gather."

**Greater visibility.** "When we migrate data from one cloud instance to another, or from cloud to on-prem, or on-prem to cloud, we have end-to-end visibility of the data itself, such as: 'Where was it encrypted? Was there any kind of exfiltration?' That is extremely helpful."

**Improved customer experience.** "If you have fewer people getting locked out of their accounts and fewer breaches, that improves trust metrics. As a result, there's more usage of your actual product, resulting in more revenue."

**Stability.** "We have 99.9% stability; we haven't had any outages except for the regular maintenance windows. We can add additional data without being concerned about the performance of the system, and we can do so as our company grows nationwide."

**IT operations.** "We solved the problem of scalability and maintenance. We no longer have to maintain updates."

Looking ahead, the telecom senior security solutions architect sees deeper cloud integration, such as tying SIEM with cloud-based business intelligence and DevOps. He anticipates, for example, that this will improve workflows by automatically spinning out notifications when certain milestones are hit – ultimately enabling new ways to capitalise on data.

> **Running on-prem, we just didn't have the capital or the hardware to keep up. It was decided to move to the cloud, where we pretty much had unlimited scalability and redundancy."**

– Senior security solutions architect, telecom company

# Barriers to Cloud-Based SIEM adoption

When IDG probed for reasons why on-prem users are opting to stay there, security concerns topped their list. “I would never say never, but I trust the security of the cloud less than my on-prem private cloud,” said one respondent.

On the flip slide, companies with cloud-based SIEM perceive better security than what they could achieve on premises. For example, the telecom solutions architect cites security as the number one benefit of his cloud SIEM solution, "primarily because you can further lock down the environment."

Other cloud SIEM users agreed, saying they had more easily achieved multifactor authentication implementation; improved compliance, a higher level of SOC intelligence and threat correlation; and gained greater visibility into overall security posture.

Aside from security concerns, some respondents said a lack of control with the cloud model was keeping their SIEMs on-prem.

"**The big one is maintaining custody, control and possession of very sensitive data," said the VP of technology for a financial services firm. "If the information [in our SIEM] were to fall into the wrong hands, it could act as a roadmap as to how to compromise and exploit our organisation.**"

Along similar lines, the VP and CISO of a software company cited controlling data gravity as the main reason he's staying on-prem. Having to transmit 90% of log sources up to the cloud would add too much latency and expense to make it worthwhile, he said.

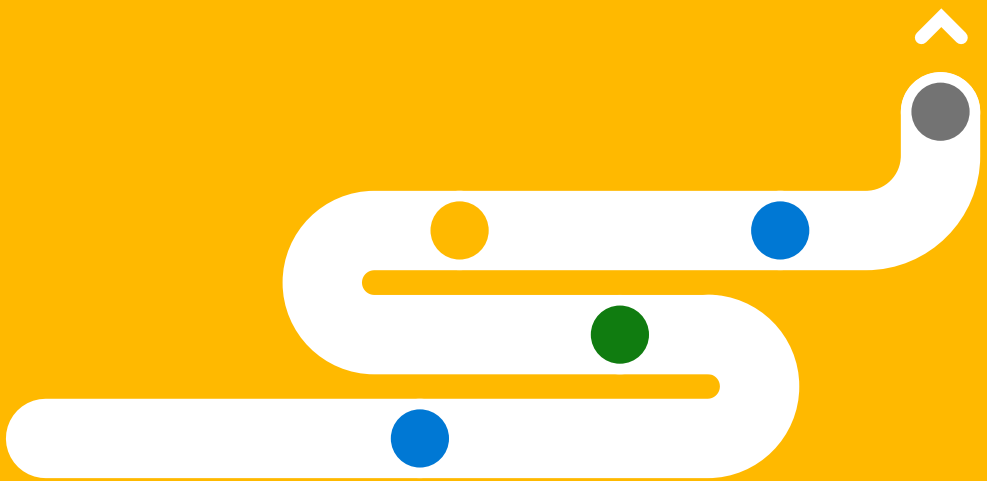
Other issues: Risk management and a lack of internal familiarity with cloud. "There's a lot of data that's being published," said a senior principal architect, financial services. "In the wrong hands, it possibly could be mined to figure out where the weak points are. It's about risk mitigation. Also, our unfamiliarity … of cloud keeps us a little bit at bay", he adds.

## As we get to be more cloud-savvy as an organisation, which we are definitely doing, that becomes less of a barrier."

– Senior principal architect, financial services company

# Five Best Practices and Words of Advice

Any cloud migration requires consideration and a business case. With that in mind, IT leaders whose companies have migrated SIEM to the cloud shared their best practices and advice, based on their own lessons learned.



## 1 Understand business and security drivers.

The tech services CIO suggested asking: "What are you expecting it to do? What that really drives down to is: What am I looking at and why? I would argue, why are you on-prem? Why do you want to manage it yourself? The one big advantage of driving to a cloud-based implementation is now I don't have to worry about upgrades or enhancements or security fixes or anything else. That was stuff that I used to have to worry about myself."

## 2 Understand data flow.

"Really think about what a data flow in your environment looks like," suggested the electronics company CISO. "How do I want to see that flow in a SIEM? Figure out if you're really going to get the value you think you're going to get. You have to know what your requirements are, and then figure out if that is achievable across your environment. The old traditional SIEM doesn't really meet the majority of the needs anymore. That's why you're seeing companies … with these big logging systems in the cloud because the traditional SIEM is not getting it done."

> **You have to know what your requirements are, and then figure out if that is achievable across your environment.**
>
> – CISO, electronics company

## 3 Articulate use cases.

"Don't jump straight into cloud just because everybody is on the cloud," advised the head of architecture, security and privacy for a digital services provider. "I would define your own use cases first. The deployment of a tool is only going to be as successful as your understanding of the threat you're under.

"Too many people try to apply their most aggressive use cases," he said. "They don't really see the benefit and they end up using it for only one or two specific needs. That takes too long, costs too much and you don't see the value for it. Find your most urgent use cases and do an on-prem deployment. At the same time, build your more strategic use cases and understand what a corresponding cloud deployment looks like. Then roll out cloud at a two-to-three month lag behind the on-prem implementation."

## 4 Seek flexibility.

"I think you have to consider migration," said the telecom senior solutions architect. "There's always a concern that you don't want to be locked into a vendor. When you consider any type of solution, you have to see if there's any flexibility in making sure that when the time comes, if you find a better solution, you are able to easily migrate. In other words, be able to export the data you already aggregated and migrate it."

## 5 Look for an active support community.

The digital services executive reflects that having adopted a popular solution was a benefit. "If we need help, our ability to extend the platform is enhanced significantly because of the wide adoption of the tool. If you are a company that doesn't have a whole lot of in-house resources or institutional cloud knowledge, it may help to adopt a tool that already has a significant market presence."

# The Bottom Line

As companies seek faster threat detection and response, as well as other benefits like capacity and cost-effectiveness, they're making the shift to cloud-based SIEM.

"**We used on-prem at first because frankly, the need was more urgent**," said the head of architecture, security, and privacy for the digital media provider. "**The benefit there was that we found out what worked well on-prem and what didn't. We used this to drive our cloud implementation**."

"Remember back in the day when you had to have a software install and you had to restart your computer repeatedly? Think about doing that across your enterprise," he noted. "That's what you have to do for on-prem. So, the business use case better be very positive for you to stay there.

## About the Research

In March 2020, IDG conducted an online quantitative survey among 300 U.S.-based IT and security leaders across all industries. Respondents work at companies with 5,000+ employees, and either have or plan to adopt a SIEM solution. Concurrently, researchers conducted eight one-on-one interviews with senior IT executives: four who have adopted on-premises SIEM, and four who have migrated SIEM to the cloud. The research was sponsored by Microsoft.

# Ease of Migration with Microsoft

**Whether your company is new to SIEM or has an existing on-premises solution, Microsoft can help you modernise your Security Operations Centre.**

Azure Sentinel is a cloud-native SIEM that allows you to collect data at cloud scale – providing unlimited compute and storage capability. With built-in AI and machine learning, you can automate and orchestrate up to 80% of common tasks, allowing your team to detect real threats quickly and accelerate response to priority incidents.

And because you're in the cloud, you don't have to worry about servers or infrastructure; you only pay for the resources you need and can put security first.

With the number and complexity of threats growing, you need visibility across your enterprise and the ability to connect to and collect data from all your sources. Make it possible with a SIEM reinvented for the modern world.

**Get more information at: [https://azure.microsoft.com/services/azure-sentinel](https://azure.microsoft.com/services/azure-sentinel) >**

Microsoft