NETWORK RISING

How network teams can thrive in an increasingly complex IT landscape

BLUECAT™

You are officially overwhelmed.

There's an inbox full of urgent help desk tickets.
Those critical patches still need to be scheduled.
A cloud migration is looming on the horizon.
The SD-WAN controllers need to be updated.
The security team needs a bunch of logs for an investigation.

Who's going to make all of this happen?

Today's network teams are always playing catch-up.

The compounding complexity and scale they have to contend with on a daily basis is staggering. Maybe there's always been a certain baseline of chaos in the background of IT departments. But now it is getting definitively, measurably worse.

The more network you try to grasp, the more slips through your fingers. As data and compute move from the network core to the edge, those predictable, centralized systems of the past are fading away. In their place, we're seeing a spaghetti of overlapping technologies which operate at unprecedented speed. All of those systems have to be maintained, configured, and optimized, even as they drift away from the control of network admins and into the hands of stakeholders.

All of this was done for a reason, of course. The amazing new functionality of the cloud, SD-WAN, automation, virtualization, and agile software development is a dream come true for end users. They finally have the flexible, "smart", on-demand network they always wanted. They can develop applications right in the cloud. They can process, analyze, and use data right at the network edge, without having to route that compute through the core. Let the good times roll!

The network team, on the other hand, is stuck holding the bag for all this innovation. Where did their happy hour go? When do they get to join the conga line of functionality and ease of use?

We went looking for answers. BlueCat and IDG recently surveyed hundreds of network administrators about this trend of compounding complexity, and found some surprising conclusions by looking at the beating heart of every network – the Domain Name System (DNS).

In this eBook, we'll talk about the serious consequences of increasing workloads on legacy network systems and the people who run them. Then we'll look at the role DNS can play in making those systems more efficient and effective, allowing you to net more and work less.

The most valuable resource in IT: time

Today's software and networks can be scaled to meet almost any challenge. The amount of storage and compute is unprecedented, and still expanding rapidly. It's tempting to say that modern technology is unlimited in what it can accomplish.

But there's a catch – humans. The limitation on any IT team is the number of administrator hours available to plan, orchestrate, and manage all of these technological resources.

The most valuable asset in any IT department is time – the one part of the network that doesn't scale.

It's important, then, to look at how the time of network administrators is used. You would think that this one precious resource would be optimized for maximum efficiency. You would imagine that humans would be reserved for the tasks that only they can accomplish, leaving the mundane, predictable work to automated systems.

Of course, we found the exact opposite.

30% of administrator time is spent on DNS-related tickets.

"The development organization doesn't consider what they're doing with DNS. It's always an afterthought. We have situations right now where, due to design decisions, they query DNS eight times before the right one hits."

That's right – nearly one-third of your network administrators' valuable time is spent doing the back-end grunt work of DNS management. Adding host records. Assigning IP addresses. Maintaining conditional forwarding rules. Managing DHCP leases.

All of these are essential network tasks to be sure, but they don't require a lot of creative thinking. Imagine what your network team could do with 30% more time to get the job done.

Unfortunately only 26% of administrator time is spent on strategic initiatives.

This number should be much higher. This is what we pay humans to do, right? We want them to be the puppet masters, integrating and orchestrating all of these complex systems. We want them looking into the future, innovating and paving the way for the next generation of functionality.

Nobody can get there with only one quarter of their time. It's just not possible – not with all of the considerations and planning involved. This is where the opportunity cost of all of those DNS service tickets starts to really hurt. It's no wonder the network team feels like it can never get ahead of the game – they're too buried in the tactical to gain sight of anything strategic.

"We have the data. Getting access to it and using it in the best possible way is part of our current challenge."

Is DNS Worth Your Time?

CIOs & CISOs depend on their network teams to transform the IT landscape and enable the digital transformation they seek. Easier said than done. This is what's actually taking up the network team's time and why strategic initiatives are taking the biggest hit.

30%
of the network team's day is spent on DNS-related workflows

38%
of the network team's day is spent on network-related management/maintenance workflows excluding DNS

26%
26% of the network team's day is spent on strategic initiatives excluding networking DNS tasks

6%
is spent on other tasks

The cost of ignoring DNS

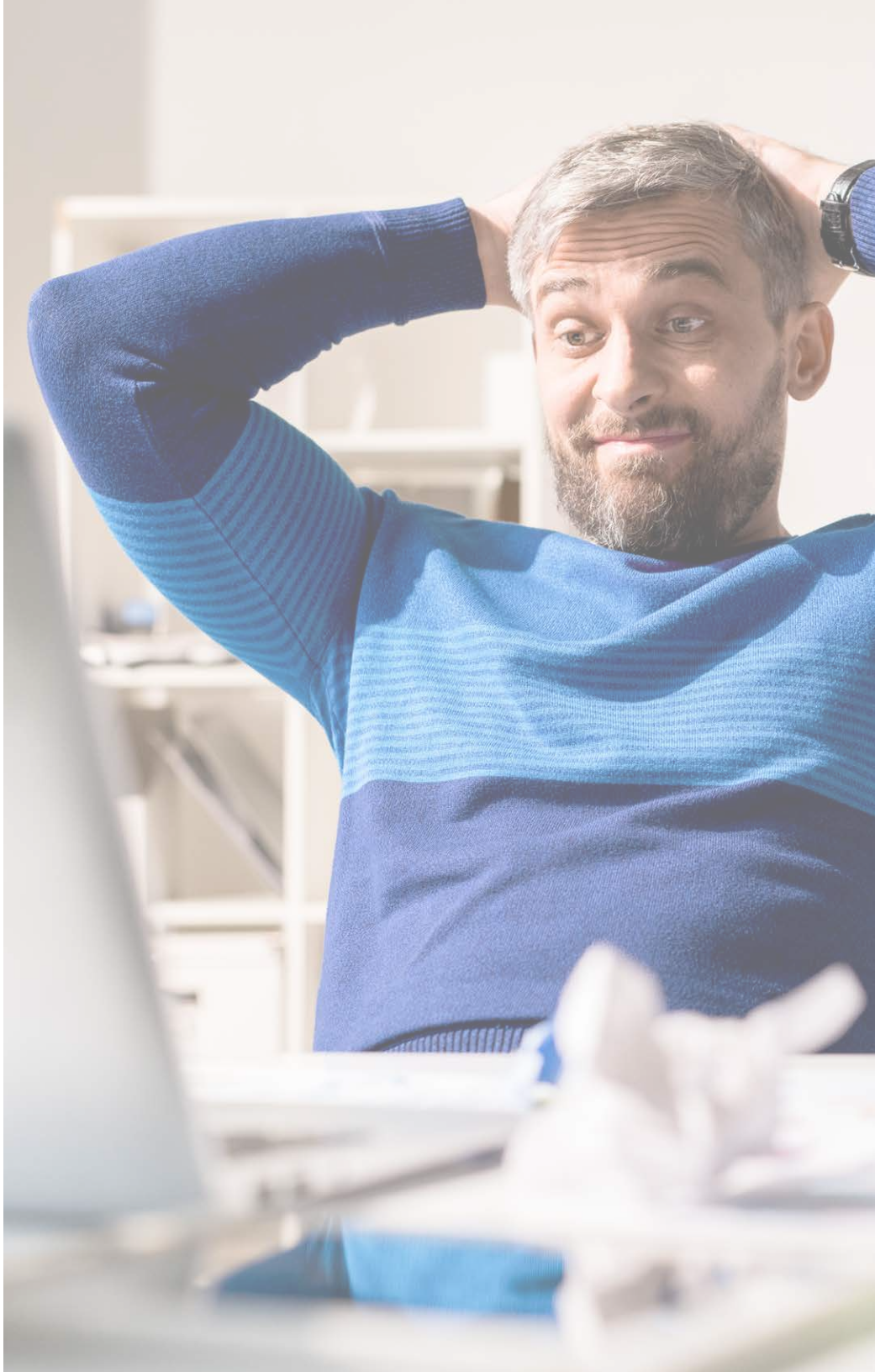
How did DNS sneak up on us? How did this old school, background protocol suddenly eat up this much time and effort?

You'd think that all that time and effort would be spent on something amazing and impactful. If one third of your network administrator time is going into DNS, it had better be the best DNS in the whole world. Only a gold-plated, maximum-functionality, Lamborghini-level DNS deserves that much time and effort, right?

Again, our survey found that the opposite is true.

Despite spending one third of their time on DNS-related issues, three quarters of the network admins we surveyed reported some sort of major DNS functionality gap.

For all that time rummaging through service tickets, most administrators still feel like their DNS doesn't deliver what they actually need. Here are some of the major functionality gaps our survey identified:



66% struggle to support strategic business initiatives using decentralized, legacy DNS infrastructures.

"Once you have DNS data, the general question becomes What do you do with it? Where does it go? Who's consuming it? That's where different groups are involved - slicing and dicing the data, collecting it, running it through different tools."

Cloud deployments create a host of issues on the DNS back-end. A tangle of conditional forwarding rules must be maintained. Duplicate data records and DNSes are created to keep information available across hybrid environments. Integrating custom business applications with DNS resources is a constant battle. DNS admins simply can't keep up with the pace and the scale of demands produced by the cloud and other strategic business initiatives.

How are you going to play it?

When your network team is overwhelmed, it's important to have the right balance of humans and automation to deal with the workload. Assemble a line-up that strikes a balance between both. Unlock and amplify their strengths, neutralize their weaknesses, and go into battle with confidence.

63% lack visibility or control over their DNS data.

All network communications flow through DNS, which makes it a powerful tool for understanding and securing the enterprise. Yet decentralized DNS systems like Microsoft and BIND don't have any way to consistently capture, monitor, and act on the massive amounts of data which flow through networks every day. Many network admins struggle to even compile basic DNS logs, let alone identify malicious activity such as DNS tunneling, domain generation algorithms, and other DNS exploits which operate freely across the enterprise.

"Security is very important and we need to do it, but it's just one use case for analytics. If I'm gathering the same data fourteen different times, I want to leverage it for performance, application behavior, and architectures."

33% can't deliver real time access to DNS resources.

The agile, DevOps cycle of most development teams can be brutal on the workload of back-end network support personnel. The constant creation and demolition of just-in-time network capabilities simply doesn't scale when humans have to manage supporting configurations in the background. Even though they spend one-third of their time on DNS-related issues, network admins still can't deliver these basic services fast enough.

For all the time and resources that are being invested in DNS, the gap between what the network team can deliver and what end-users need continues to widen. Network administrators are going to keep falling further and further behind as the demands of cloud, SD-WAN, DevOps, and other strategic business initiative pile up.

Confessions of a Network Administrator

With all the pressures and demands unloaded on the network teams, how do they really feel about it all? Protecting their identities, these are the unfiltered realities they face.

"The business doesn't understand project timeframes. They overcommit us regularly."

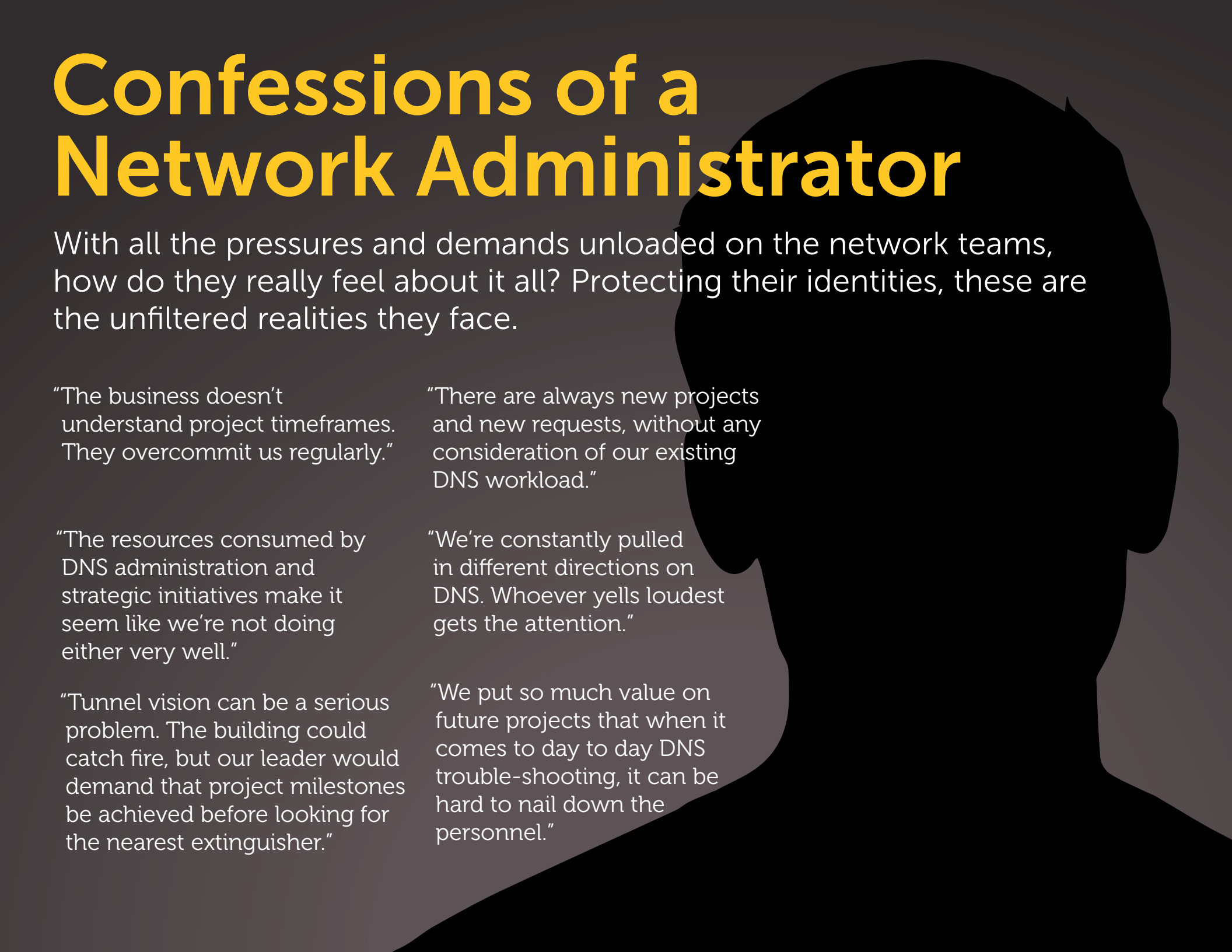
"There are always new projects and new requests, without any consideration of our existing DNS workload."

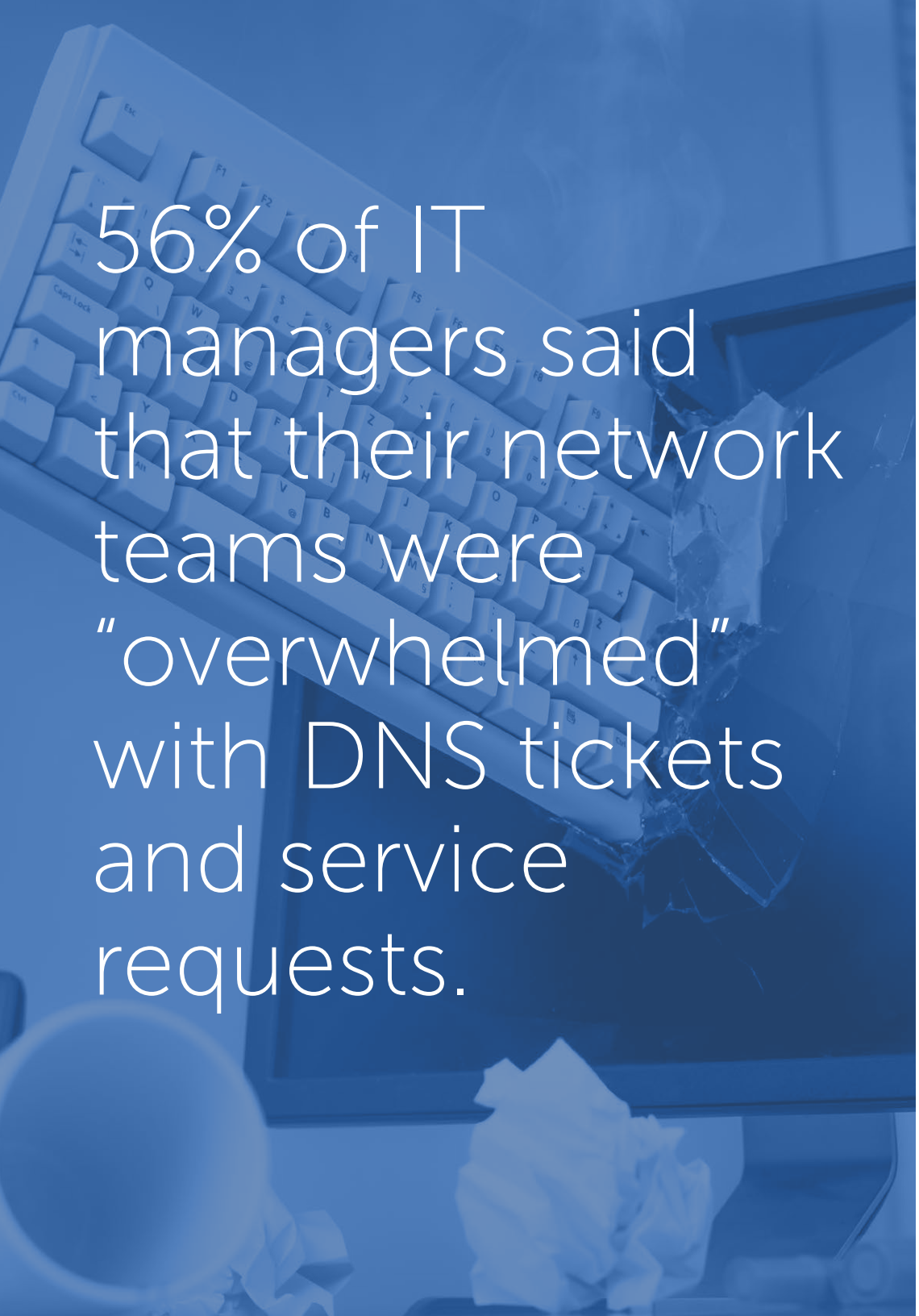
"The resources consumed by DNS administration and strategic initiatives make it seem like we're not doing either very well."

"We're constantly pulled in different directions on DNS. Whoever yells loudest gets the attention."

"Tunnel vision can be a serious problem. The building could catch fire, but our leader would demand that project milestones be achieved before looking for the nearest extinguisher."

"We put so much value on future projects that when it comes to day to day DNS trouble-shooting, it can be hard to nail down the personnel."





56% of IT managers said that their network teams were "overwhelmed" with DNS tickets and service requests.

The first step in recovery is recognizing you have a problem. Our survey showed that when it comes to identifying DNS as a barrier to network team effectiveness, the groundswell is growing.

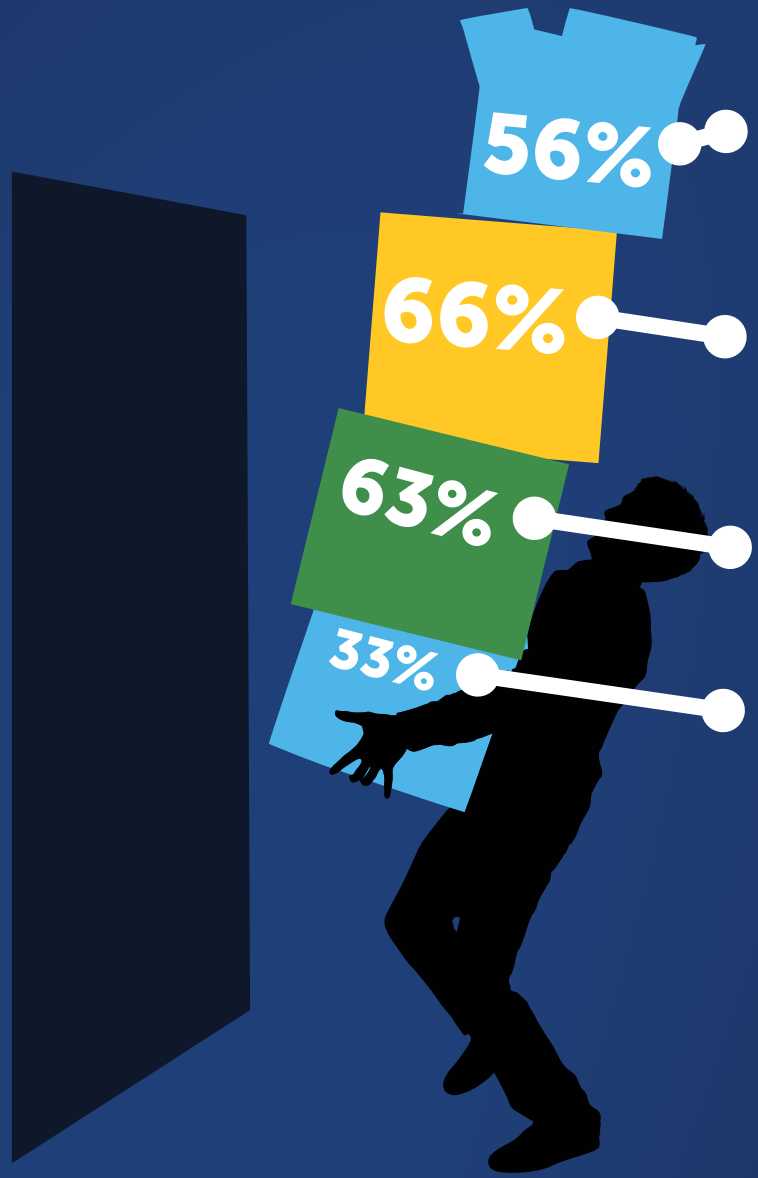
CIOs generally don't pay attention to DNS. They consider it a basic network service – something that's just supposed to work. Yet our survey results show the rising visibility of DNS as an issue among top-level IT executives, precisely because of the resource toll it exacts and diminishing functionality it delivers.

For a piece of the network which usually sits so far in the background that it goes completely unnoticed, that is a significant number. CIOs are starting to realize that the long-term impact of business initiatives on the performance of their networks and the teams that support them is growing worse by the day.

If so much of the network team's time is currently consumed by DNS-related issues, the compounding complexity of most enterprises means that the number of "overwhelmed" teams will only continue to grow. CIOs are coming around to the fact that DNS is distracting from the strategic initiatives they truly care about. Delivering innovating services on the network edge in real time will always be the priority – IT managers are only now realizing that a centralized, automated DNS back-end is necessary to make it all happen.

Is He Going to Make It?

Bogged down and overloaded? Network teams can tell you all about it. DNS is making the day-to-day network maintenance a difficult task. It's become the barriers and obstacles no one wanted and making those important projects even harder to complete. The delicate balancing act can't last forever.

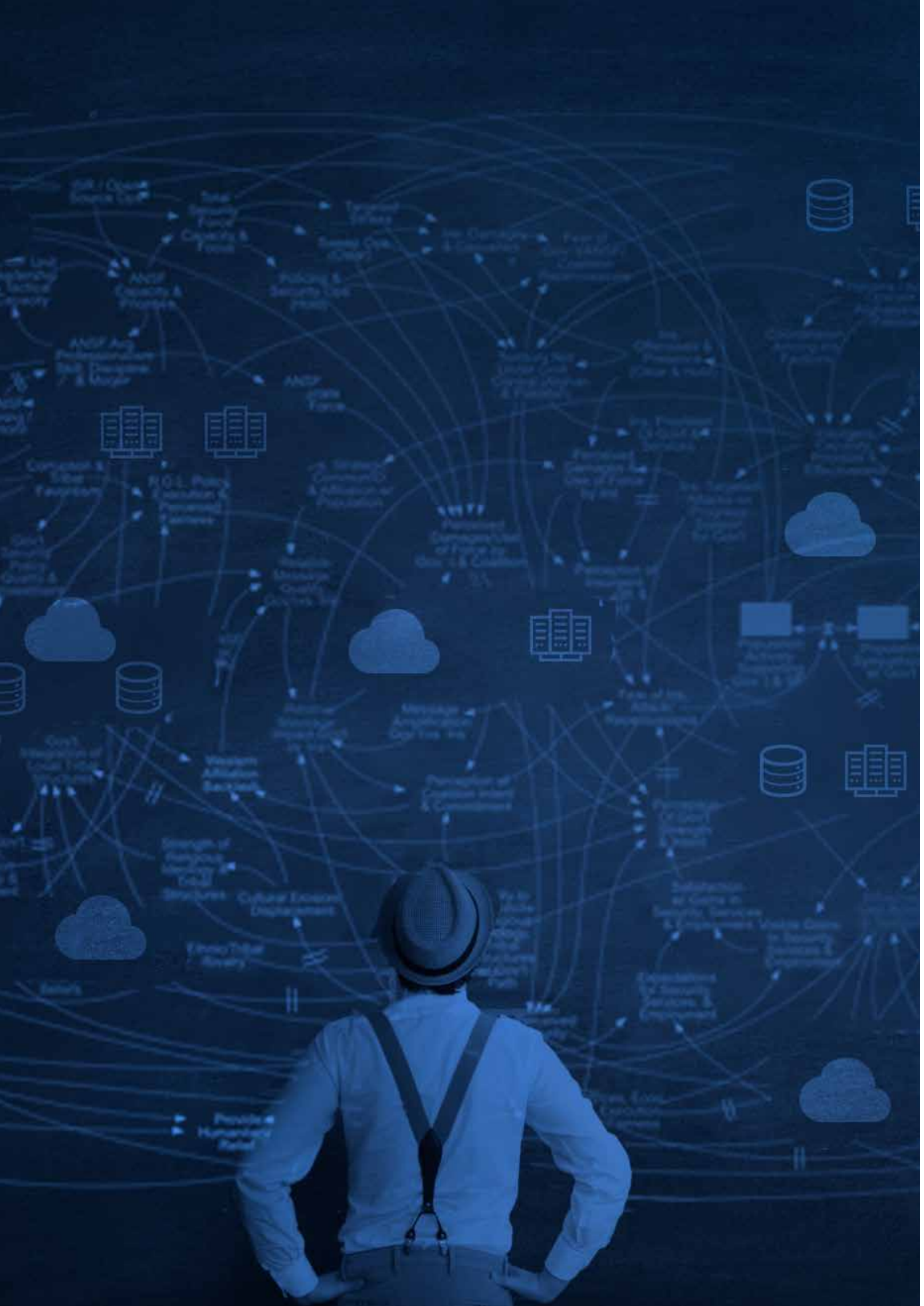


56% of IT managers said that their network teams were "overwhelmed" with DNS tickets and service requests

66% struggle to support strategic business initiatives using decentralized, legacy DNS infrastructures

63% lack visibility or control over their DNS data.

33% can't deliver on real-time access to DNS resources



What is to be done?

It's clear that the decentralized DNS solutions at use in many large enterprises are only making a bad problem worse. The compounding complexity of the cloud, SD-WAN, DevOps, and other strategic initiatives is putting a real strain on the time and resources of network teams. As a result, IT administrators are spending far more time on DNS than they would in an ideal world.

Here's what the survey results tell us about restoring DNS to its rightful place as an enabler - rather than a roadblock - for change across the network.

Step One: Centralize

Your network demands automation, visibility, and control. Can your DNS infrastructure deliver?

If you use Microsoft DNS or BIND, the answer is a definitive "no". Without a single, centralized repository for DNS, DHCP, and IPAM (DDI) data, there is no foundation for automation. Visibility into network activity is extremely complicated. Controlling that activity is nearly impossible. These decentralized solutions rely too much on human management to scale effectively.

Only a "single point of truth" can provide reliable, real-time information to the network systems and end users that need it. Without a centralized system to gather and disseminate DDI information, network administrators are stuck consulting spreadsheets or sorting through a pile of sticky notes. (Yes, we've seen this.)

Scalable DDI starts by putting all your infrastructure under one roof.

In order to do this right, some up-front investment is required. Migrating those disparate DNS resources into a single system is a delicate process. Translating the patchwork of fixes and scripts into a new platform will take some time. But the good news is that you really only have to do it once. Then you're ready to reap the rewards of automation, gain visibility and control over your network, and start managing DDI at a strategic level.

Step Two: Automate

All of those menial yet important DNS tasks which consume one-third of your network team's time are ripe for automation.

Assigning host records, managing IP addresses, configuring conditional forwarding rules, assigning DHCP leases – all of these things should be done without human involvement.

With a centralized repository of DDI data in place, the world is your oyster. You can use automation tools to push data into the system and synchronize existing data with outside applications.

Here's the best part: end-users can do most of the work themselves. When all of the grunt work of assigning back-end DDI resources and managing configurations happens automatically, network administrators can confidently push functionality out to the people who need it most – application developers, project teams, and power users in the field.

This is how network teams get their happy hours back. Automation of back-end DNS tasks makes it possible to focus on the strategic initiatives that really matter. Automation saves that most precious resource – administrator time – for complex problems which require abstract thought and long-term thinking. Automation is how administrators can net more and work less.

Step Three: Leverage

The visibility and control most administrators crave is extremely difficult to achieve without centralized DNS infrastructure.

Pulling logs from multiple network sources, cleansing data provided in multiple formats, and then analyzing information in an actionable way is a full time job in and of itself. Anyone who's ever had to provide DNS logs to a security team will tell you that it can take days, if not weeks.

Centralized DNS dramatically simplifies the process of gathering and rationalizing data. When all the information is flowing through a single system and passing through the same monitoring points, collecting that data becomes far easier.

Once you have all the data sitting in a searchable log, automation can help spot anomalies, performance problems, and potential security vulnerabilities. You can comb through DNS information and look for things that shouldn't be happening. Maybe a security camera is querying the finance server. Maybe an administrator in Hong Kong is lurking in the New York files. Maybe all your printers are sending updates to Vladivostok. DNS data can tell you what's going on across the enterprise.

With all of this visibility into what's happening in the world of DNS, you can start to actively control and manage the enterprise in new ways. Administrators can implement role-based privileges by granting (or denying) access to DNS resources. Suspect activity such as DNS tunneling and the use of domain generation algorithms can be blocked at the source. Insider threats can be quickly identified by the paths they use to search for sensitive information outside of their proper purview.

Get your happy hour back

The toll of compounding network complexity is real. As the tide of strategic initiatives continues consume the time, energy, and resources of network teams, CIOs and IT managers are looking for ways to refocus their efforts on the work that really matters. Network admins are just looking for a break. They want one-third of their working lives back.

It's tempting to try and patch your way out of the problem, but that just makes things worse. Adding configurations and work-arounds only increases the complexity that most administrators are trying to get rid of. Adding to the pile of patches will only make the transition to an agile, adaptive DNS harder.

Large enterprises now see that centralizing, automating, and leveraging DNS infrastructure is the natural complement to most strategic network initiatives. Without a back-end DNS to support them, projects such as cloud, SD-WAN, and agile software development will continue to exact an unacceptable toll.

With over twenty years of experience in the field, BlueCat offers the DNS solutions that enterprises need to be successful at scale.

Want your happy hour back? BlueCat can help you get there. It's time for a strategic discussion about your DNS.

About BlueCat

Today's networks are drowning in complexity. If your DNS infrastructure isn't adaptable by design, your network - and your entire business - is fragile. Think outages. Downtime. Data loss.

BlueCat helps your business thrive on complexity with Adaptive DNS. Move beyond static, manually-controlled, off-the-shelf DNS that breaks under network complexity, and move to a DNS that embraces it. Adaptive DNS is powered from the edge of your network, scaling to meet escalating demands by users, applications and services. It's open and automated, giving you the power to enforce business policies, manage security, analyze data, and remediate threats.

Thrive on complexity from edge to core with BlueCat Adaptive DNS™. Talk to us.