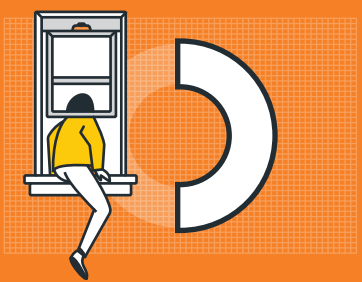
CATO NETWORKS | WINDSTREAM ENTERPRISE

Keeping your IT staff happy

How CIOs can turn the burnout tide in 6 steps

IT professionals are feeling burnt out.

According to a study of 36200 IT professionals across 33 countries by Yerbo, 2 in 5 workers are at high risk of burnout.



42% of IT workers who are facing high levels of burnout are considering quitting their company in the next few months, Yerbo found.

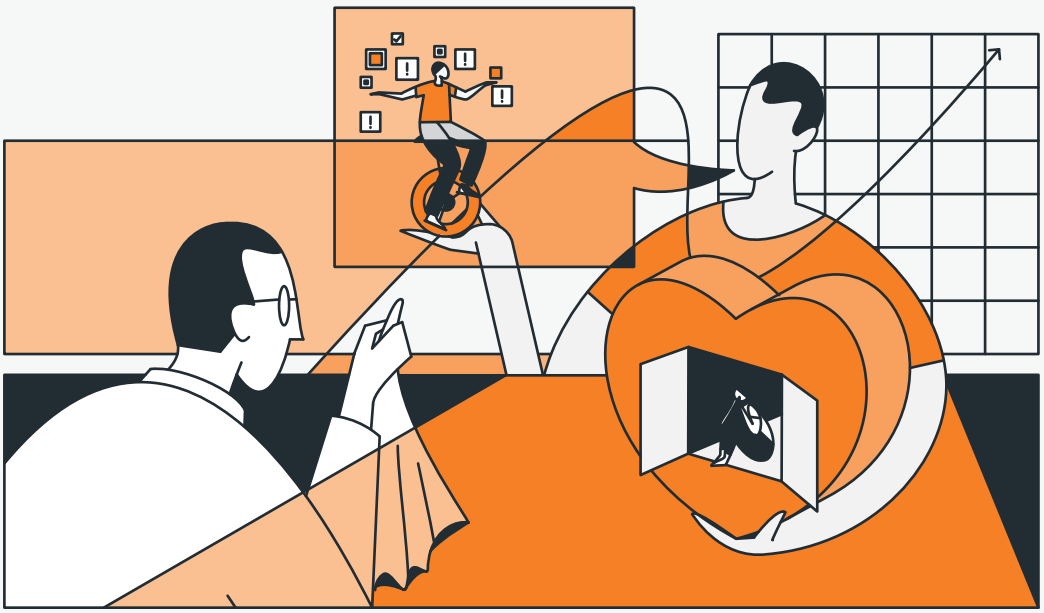
Deloitte found that 70% of professionals feel their employers are not doing enough to prevent or alleviate burnout.

CIOs should take these statistics seriously.

It’s time to get strategic

Stop worrying about what could go wrong and start putting a plan into action.

This eBook is a 6-step action plan to understand the main challenges your IT team is facing, which erodes their loyalty and happiness. After identifying the main challenges, this guide will give you a clear plan of action to meet each challenge head-on, win your team's loyalty, and encourage their career growth. Doing so will directly benefit you, allowing you to use the year to move fast, optimize process, eliminate the fires your IT team is facing, while tackling business critical projects head-on.



Result

Happy IT team, end users, management and yearly KPIs achieved.

6 Reasons why good IT managers quit their jobs

Your action-plan to turn the tide

IT pain point #1

Your IT team is stressed out by angry, frustrated users

It's hard for IT to feel valued when they're constantly on the receiving end of negative employee feedback. Users routinely complain about poor network performance, slow internet, dropped Zoom calls with prospects, and internet outages. Add in late-night "emergency" phone calls, security false positives and breaches which stop users dead in their tracks, and IT is understandably running on fumes.

Did you know?

IT manager
#5 most stressful job in America

IT security analyst
#24 most stressful job in America

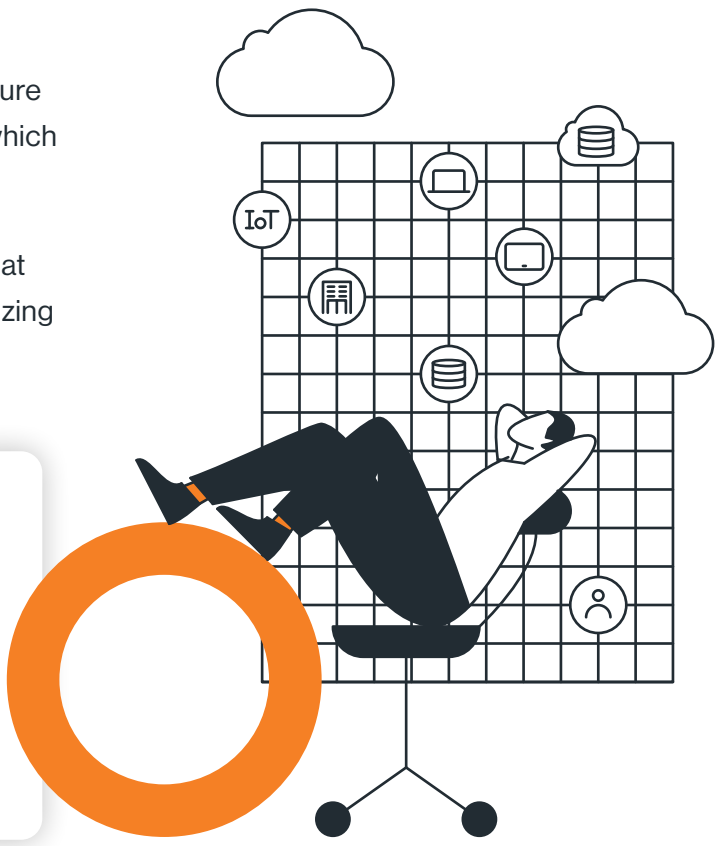
CIO action plan #1

Reliable global connectivity is the lifeline of a successful enterprise.

A true SASE service with a private global backbone delivers high availability performance, backed by a 99.999% uptime SLA.

SASE also reduces single points of failure in legacy networking point solutions, which ultimately optimizes performance.

Its self-healing architecture ensures that traffic is automatically rerouted, minimizing the chance of outages.



Result

IT managers can now breathe a sigh of relief and guarantee business continuity while providing a flawless user experience. IT is now free to enjoy a silent helpdesk, thanks to no more user complaints about performance.

> I&O executives are deploying highly disruptive emerging technologies to ensure continued, uninterrupted access to enterprise networks and effective delivery of network services within organizations. Investments in network technologies have seen continued growth, as 53% of respondents note that they have increased or plan to increase investments in network technologies in 2021, compared with 32% in 2020."

Gartner

Gartner 2021-2023 Emerging Technology Roadmap for Large Enterprises

IT pain point #2

They're unmotivated by endless, repetitive admin work

It's difficult for IT to feel like they're making a difference when they're caught in a cycle of never-ending admin work that's best left to automation. This can include network and security monitoring and maintenance, updating firewall rules, applying patches, and deploying fixes. All of which adds labor and downtime and keeps your networking and security posture "status-quo" (instead of optimized and future-proofed.) Other common "best left to automation" scenarios include detailed root-cause analysis to isolate and identify network problems thanks to siloed point solutions. Your highly trained IT staff should leverage their expertise to meet your strategic business objectives, instead of focusing on repetitive, manual work.

"With our previous system, every time they released a firmware update, we had to go one by one to all the routers around the company and push the update to it. Afterwards, [we'd] make sure it's back up and running.

IT Team Manager, Consulting and Engineering, Forrester Research, The Total Economic Impact™ of Cato Networks

CIO action plan #2

Leverage automation to maximize business impact

As CIO, it's up to you to determine your team's North Star. This means making strategic choices about what your team should and should not focus on. With a true SASE solution, IT can automate routine, manual monitoring and configuration from a single management application.

This includes easily automating system optimization, managed updates, patching, security updates, rollbacks and more.

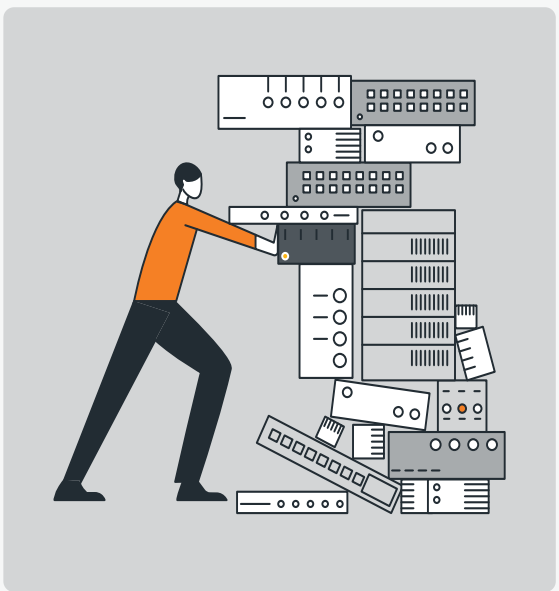
Result

When IT shifts from reactive to proactive, they're free to focus on business-critical targets, like opening new global sites and digital transformation.

IT pain point #3

They’re aggravated by unnecessarily complicated point solutions

For every business problem, your IT team has implemented a corresponding point solution. At best, it's a loosely integrated hodgepodge of legacy virtual machines, hardware and software comprising your networking and security stack. Each solution has its own separate management console, maintenance and update schedule, billing cycle, and customer service representative, and it’s difficult for your IT team to see the big picture let alone manage, maintain, isolate and fix any network or security issues.



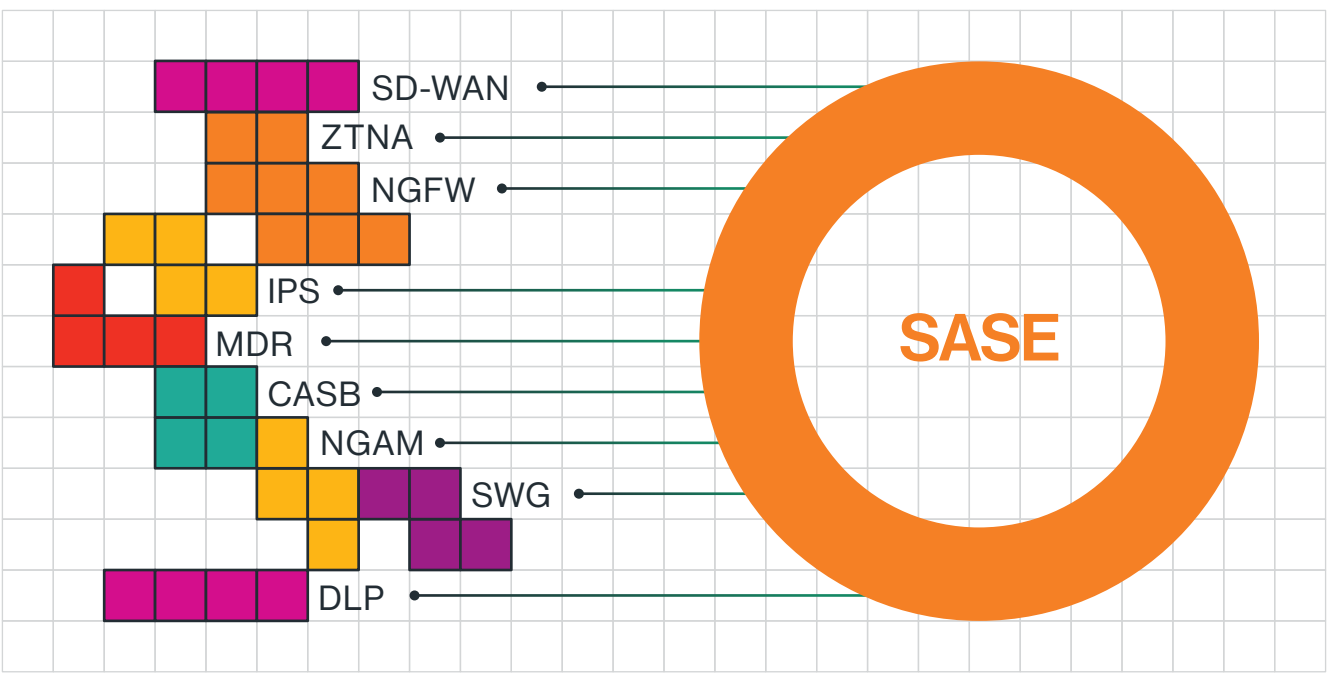
> The requirement to address changing needs and new attacks prompts SRM (security and risk management) leaders to introduce new tools, leaving enterprises with a complex, fragmented environment with many stand-alone products and high operational costs”.
>
> Gartner, Predicts 2022: Consolidated Security Platforms are the Future

CIO action plan #3

Eliminate networking and security solution sprawl with converged SASE

In a fragmented infrastructure, finding, remediating, and preventing a problem becomes extremely challenging and significantly less effective.

SASE transforms your network from disjointed point solutions to one platform with a single and central management application, achieving consistent policies throughout your enterprise, eliminating routine deployment of updates and patches.



> SRM leaders tell Gartner that they want to increase their efficiency by consolidating point products into broader, integrated security platforms that operate as a service.
>
> Forrester Research, The Total Economic Impact™ of Cato Networks

IT pain point #4

They're exhausted from supporting branch work and WFA

Enter COVID-19 and WFA is no longer the exception, but the “new normal.” IT must now ensure high network availability and an optimal security posture for thousands of users from any location. With a larger infrastructure, a growing attack surface and increasing end-user frustration about application performance, IT’s workload has successfully doubled overnight. And with 1000s of users backhauling to the VPN server, IT is back in reactive mode, answering frustrated users about performance degradation, and patching VPN vulnerabilities, instead of fulfilling your strategic business objectives.

McKinsey found that 52% of employees would prefer a flexible working model even after COVID.

CIO action plan #4

Ensure business continuity and best-in-breed security with ZTNA

IT and IS teams are adopting SASE so users can work seamlessly and securely, regardless of location. SASE optimizes traffic to and from all edges, while continuously inspecting traffic for threats, and enforcing access control. This is because SASE treats remote users no differently than office users. All security and optimization services available to office workers can now be secured, which improves the remote user experience. Access is now provided based on user authentication and includes additional security layers like zero trust and device posture checks.

Result

IT is now able to provide a uniform security posture, reduce the attack surfaces, and easily ensure user productivity.

IT pain point #5

They're fighting a security battle on 1000s of simultaneous fronts

The corporate network is more vulnerable than ever to security threats. With the expansion to global branches, the blurred lines between BYOD and corporation issued devices, secure remote work, the complexity of integrating networking and security point solutions, and the attack surface has infinitely expanded. For every new security product and management application, the opportunity for misconfiguration increases as does the number of policies. Misconfigurations can easily lead to high-profile security incidents, while multiple sets of separate policies can lead to gaps that are difficult to identify. IT is waging an uphill battle in a losing war.

> It's crucial that a firewall update be applied immediately. Otherwise, you risk being breached. But it could take our management provider 14 days to update our firewalls".
>
> Kenneth Middelboe Carlson, IT Senior Administrator, Hoyer Motors

CIO action plan #5

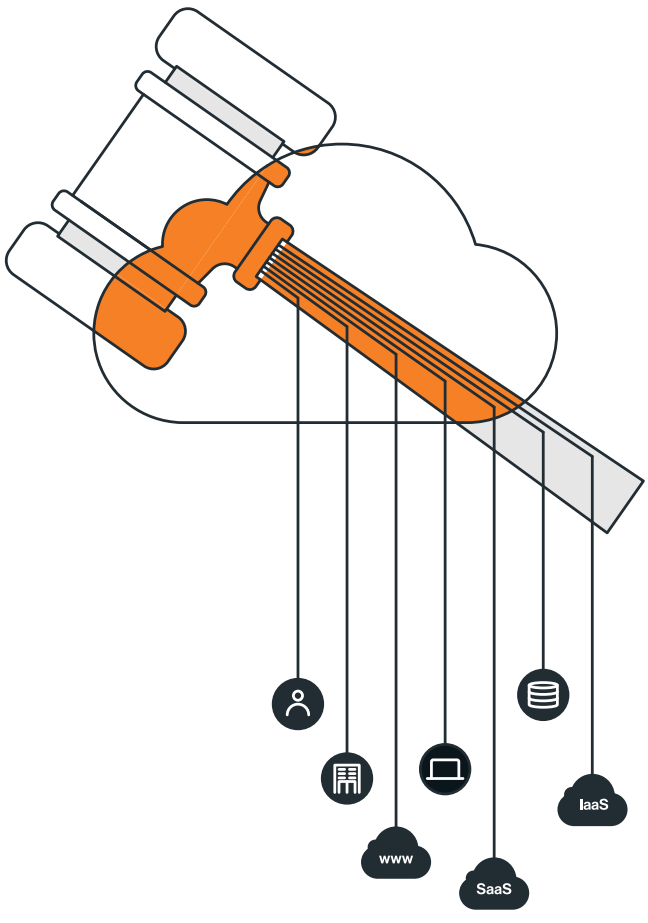
Minimize security vulnerabilities through cloudification and consolidation

A fully converged security stack delivered as a cloud service (SASE or SSE) applies a single, consistent set of access and security policies across all users, branches, datacenters and clouds.

With a holistic view into your organization's policies, IT is easily able to troubleshoot and conduct compliance audits. A consolidated security stack that is fully maintained and up to date allows IT to identify and address basic and advanced cyber threats with real-time prevention, while minimizing the risk of security false positives.

Result

IT is now able to return to its role of technology business partner, instead of playing security defensive.

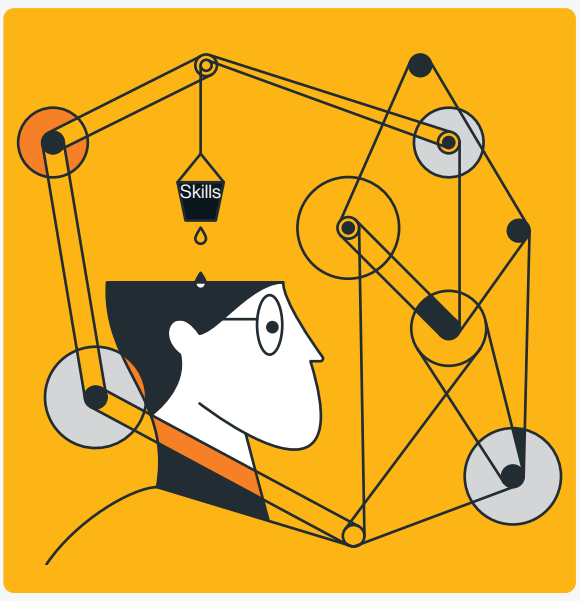


> Cato Networks gave us strong visibility into how inconsistent our rule sets were and what traffic we were allowing to move across the WAN. We realize how inconsistent our rule set was, and that was a huge benefit from a risk and compliance perspective because now they're all the same".
>
> Kenneth Middelboe Carlson, IT Senior Administrator, Hoyer Motors

IT pain point #6

They're overwhelmed by skillset gaps and professionally unfulfilled

Your IT staff remember their recruitment interviews better than you do. Perhaps you made suggestions of vertical promotions or lateral opportunities to expand on their skills and training. And even if you didn't, a former manager, colleague, or HR administrator may have implied that it was possible, leading to unfulfilled expectations. In addition to feeling professionally "stuck," IT professionals often feel overwhelmed and unprepared due to crucial skills gaps needed to drive business growth. Maybe your IT professional or network engineer is out of their comfort zone managing cybersecurity, or another function they inherited due to team member attrition, lack of available resources, or inability to find a subject matter expert. Which means, your plans for business growth will inch forward, hampering your ability to drive innovation and progress.



"The talent shortage as the primary adoption barrier to emerging tech is concerning, because it demonstrates the critical skills gap that exists in most industries today. Not enough people within an organization have the skills that are necessary for business growth in the modern age".

Kenneth Middelboe Carlson, IT Senior Administrator, Hoyer Motors

Did you know?

According to a 2021 LinkedIn study, IT positions are the second most difficult to fill

CIO action plan #6

Bridge your team's skillset gap and invest in their higher education

Gaps in your IT teams' expertise and career overwhelm are a call to action, not cause for defeat. According to a 2019 LinkedIn Workforce Survey, 94% of employees would stay at a company longer if it invested in helping them learn. And, with rising compensation requirements and lack of IT staff with the necessary skills requirements, your best course of action is to uptrain your current staff to fill business gaps, rather than searching externally.

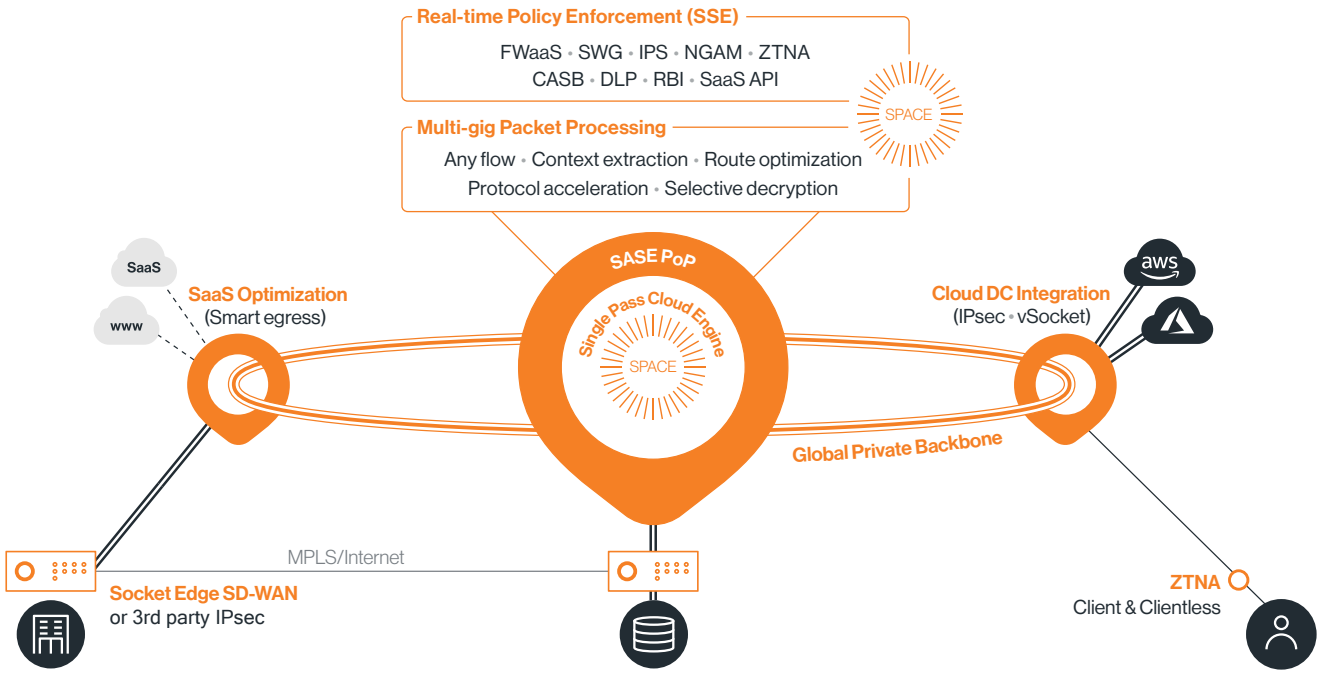
Did you know?

Cato Networks offers free SASE certification courses that your entire team can use to supplement their knowledge of networking and cybersecurity strategies. The course allows CIOs, IT, IS, and networking professionals to learn the architectural requirements of true SASE, learn to separate fact from marketecture, and effectively plan a SASE implementation.

Why SSE from Windstream Enterprise

The Security Service Edge (SSE) enables enterprises to move away from a rigid and disjointed IT architecture to a converged security platform delivered as a cloud service. With SSE, enterprise IT can rapidly address new business and security requirements such as cloud migration, adoption of public cloud applications, and work from anywhere. SSE's converged architecture reduces cost and complexity with simple management through single pane of glass, self-healing infrastructure, and automatically evolving defenses that seamlessly mitigates emerging threats. Customers can opt to manage their infrastructure themselves or co-manage it with their preferred partners.

SASE cloud with SSE



SSE, SD-WAN, SASE: Your journey, your way.