AT&T Business

Trust issues

Why businesses should adopt Zero Trust security

Introduction

AT&T conducted three surveys over 12 months. The surveys targeted IT professionals and IT security professionals on LinkedIn and explored common IT pain points for enterprises, including:

- How to identify, block, and mitigate targeted threats to prevent ransomware attacks and data loss.
- How to manage and secure an increasingly diverse network that may connect cloud applications, remote users, Internet of Things (IoT) devices, and Bring Your Own Device (BYOD).
- How to transform from a traditional firewall-based network security approach to one that better addresses a changing threat landscape.

We surveyed organizations with between 1,001 and 10,000 employees across various industries. The surveys were conducted by AT&T with Akamai.

Read our results to learn about the state of IT security and why businesses should consider adopting a Zero Trust approach to security.

IT security teams need help

Our survey identified troubling gaps in security strategies. As cyberattacks become more frequent and sophisticated, organizations need to work harder to stay ahead of risk. But many organizations do not have the staff or resources to manage and update their security tools effectively. Additionally, IT security teams are struggling to keep employees educated on cyber-risks and security best-practices.

Only 54% are educating users on safe Internet and email practices

Only 38% are keeping all their security tools up to date

Only 31% are protecting their networks from internal threats and vulnerabilities

67% of organizations participating in our survey lack the staff and resources to manage security tools

Security must extend beyond the perimeter

As organizations change the way they do business, they alter the risk landscape. This can create new vulnerabilities.

The idea of having a secure corporate perimeter is becoming increasingly difficult. Users, devices, applications, and data have moved outside organizations' traditional zones of control, providing new potential entry points for cybercriminals.

51%
see use of third-party applications as a risk

67%
have not developed a corporate standard to manage IoT devices

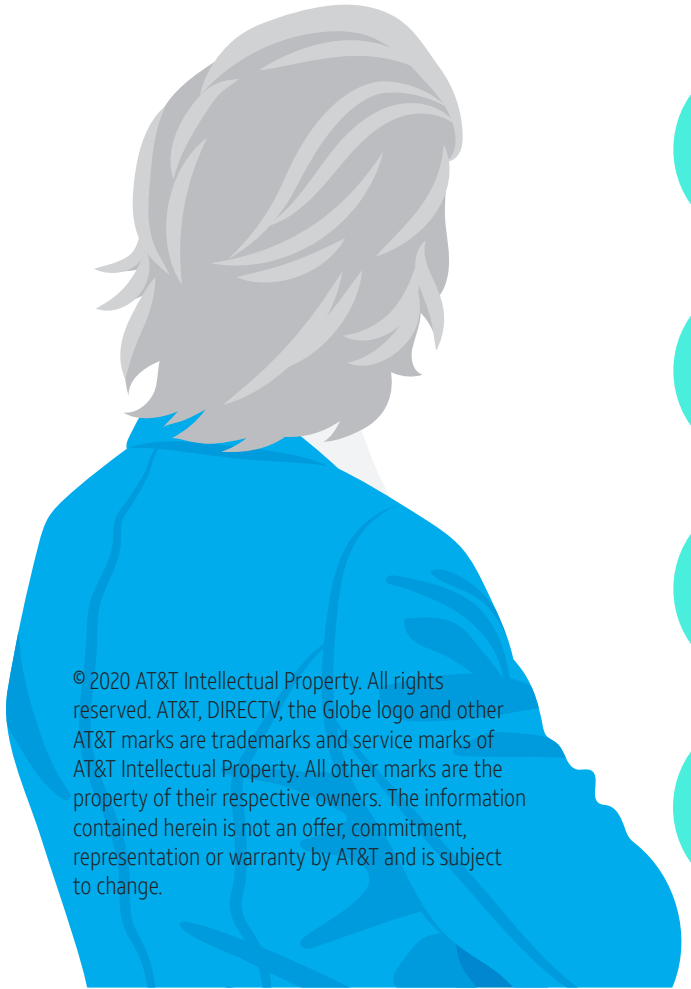
43%
find remote workers create a security risk

36%
list BYOD as a risk

Equip your business with the right tools

As business endpoints extend to the cloud and beyond, traditional security tools in and of themselves don't offer complete protection. Organizations need security tools that help defend against evolving attacks. A more robust security policy can help stay ahead of threats more effectively.

Here's what survey respondents are using today.



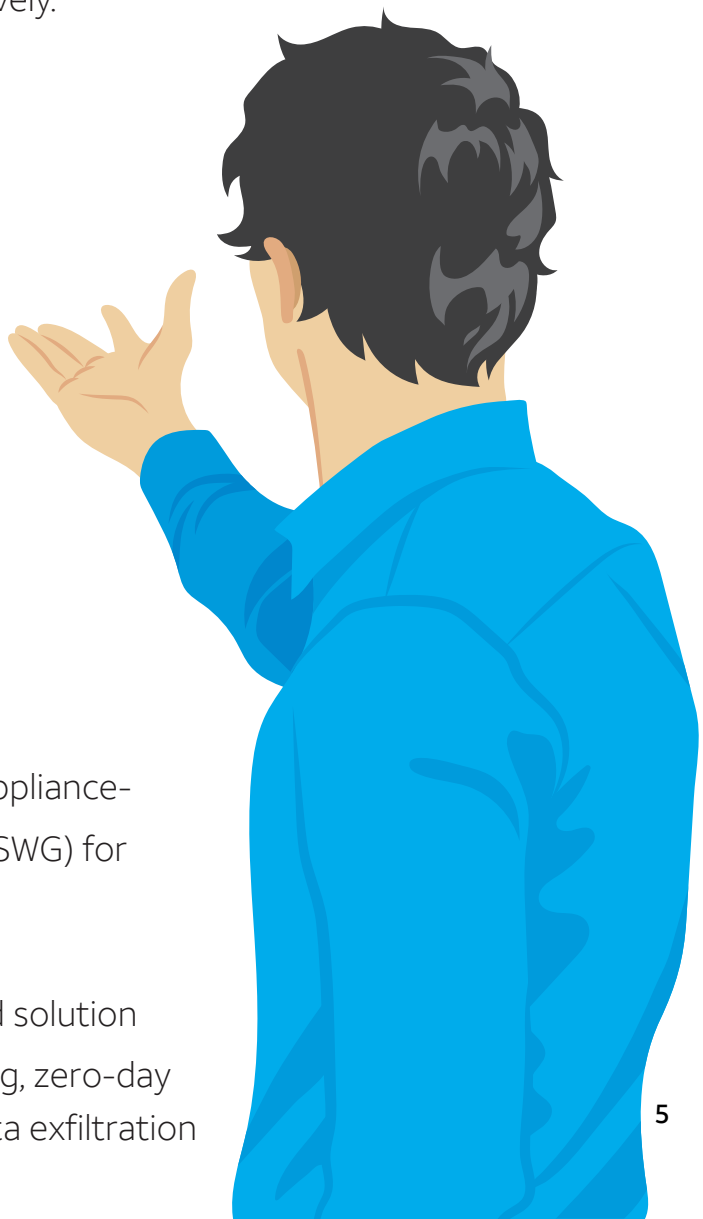
89% use a firewall

87% have anti-virus solutions

72% have implemented multi-factor athentication

56% use a centralized appliance-based secure web gateway (SWG) for URL filtering

50% have a cloud-based solution that protects against phishing, zero-day malware, and DNS-based data exfiltration



Build stronger security strategies

Based on our research, there are gaps in current security strategies. Resources are limited and awareness needs improvement. And as data and endpoints extend beyond traditional zones of control, security initiatives must be enhanced to address these new threat vectors.

The solution is to adopt a Zero Trust security policy to replace the principle of “trust but verify” with “always verify, never trust.” This will ensure that only authorized users and devices can access your data - whether on-premises, remotely, or in the cloud.

Take a Zero Trust approach with AT&T

AT&T can help your organization put a Zero Trust security strategy in place. Our solutions are designed to help you ensure that users and devices can safely connect to the Internet, regardless of where they are connecting from. Plus, you can restrict users and devices so that they only have access to the applications they need – not to the entire network.

Approach data security proactively with

Enterprise Traffic Protector

Identifies, blocks, and mitigates targeted threats

Enterprise Application Access

Zero Trust connectivity to corporate apps for internal and external users

To learn more about our Zero Trust security solutions, contact your AT&T Account Team or visit www.att.com/cdn and have us contact you