adaptiva

This report is based on the results of a comprehensive online survey of 345 cybersecurity professionals by Cybersecurity Insiders to gain more insight into the latest trends, key challenges, and solutions for endpoint security.

The 2022 Endpoint Security Report

By the Numbers

Sophisticated threats are on the rise, but IT isn't prepared to handle them.

The future of cybersecurity is stark — don't wait for the next critical threat.

The modern enterprise is facing increasing endpoint security risk from new and increasingly sophisticated threats, while IT teams are feeling insufficiently prepared to tackle new threats with platforms and solutions that aren't keeping up with reality.

While only **20%** of companies were compromised in the last year,

85%

expect to be in the year ahead.

What are the most reported operations challenges?

44% a perennial shortage of cybersecurity skills

38% the lack of continuous 24x7 security coverage

37% slow incident response

*Surveyees chose all that applied

Biggest Threats

38%
Malware (ransomware, trojans, exploit kits, etc.)

23%
Human error

18%
Zero-day exploits

Business Impact

*Surveyees chose all that applied

- **47%** say loss of end-user productivity
- **40%** say system downtime
- **39%** say loss of IT productivity
- **36%** say reputation and brand damage
- **32%** say theft of information assets
- **28%** say business or revenue impact

LEARN MORE IN THE FULL REPORT

What's wrong with last-gen endpoint management solutions?

46% of organizations say their legacy security products are **failing to stop** evolving threats.

41% of organizations that believe they have solid tools and processes in place are **still concerned that threats are slipping through** the defenses.

Slow incident response

High cost of operation

Negative impact on end-user or endpoint performance

High complexity of deployment and operation

High number of false positives and alerts

Biggest Endpoint Challenges

Patching

Organizations are slow to patch and aren't confident in the effectiveness of the patches that are pushed (43% of organizations take at least 1 week to roll out critical patches – 38% take longer than 1 week and 70% of organizations are either not confident at all or only moderately confident in the effectiveness of the patches that are pushed.)

Remediating

83% of organizations need more than a day to remediate endpoint issues.

Monitoring

Each month IT teams spend an average of 36 hours on endpoint security monitoring.

Don't wait for the next compromising threat.

Get ahead of the next critical threat with Adaptiva so you can harness the power of the devices already on your network.

Create custom health, security, and compliance checks with the Workflow Designer.

Automatically and continuously scan and remediate issues.

Prevent ransomware attacks, virus outbreaks, and data security breaches.

With a next-generation endpoint management solution like Adaptiva, you get lightning speed at massive scale with a peer-to-peer platform that harnesses the surplus capacity of devices already on your network to continuously deliver software, configurations, and patches to endpoints no matter where they are.

THE OLD WAY

NEXT-GEN SOLUTION: ADAPTIVA

Find out what Adaptiva can do to protect and secure your endpoints. We're one click away at Adaptiva.com.

CONNECT WITH US TODAY