arksoft | White Paper 2026

2026 Cybersecurity Outlook

Trends, threats & readiness — what every MSP needs to know now. Cyberattacks are inevitable, and clients are looking to their MSPs for answers as they brace for phishing, ransomware and costly downtime.

KEY FINDINGS AT A GLANCE

70% Of Businesses Expect A Successful Phishing Attack Within The Next 12 Months

40% Lost At Least A Full Day To Downtime After A Security Incident

74% Of MSPs Plan To Expand Security Services To Meet Rising Client Requirements

— Executive Summary

2026 marks a turning point for managed service providers. As cyber threats grow in both frequency and sophistication, SMB clients no longer expect simple "IT support" from their MSP, they expect an end-to-end security partnership. This report brings together field observations from our managed-services engagements alongside broader industry trends. Our goal is to help MSP partners plan the year ahead with the right priorities, guide their clients with convincing data, and grow their portfolio by investing in the areas that matter most.

3×
Upward trend in phishing and ransomware-driven incidents across the SBM segments

70%+
of SMBs are willing to outsource security to a trusted MSP

#1
Upward trend in phishing and ransomware-driven incidents across the SBM segments

Figures Above Are Illustrative, Reflecting Broad Industry Trends And Arksoft Field Observations Rather Than A Single Proprietary Survey. Headline Statistics On The Cover Are Sourced From The 2026 Kaseya Cybersecurity Outlook Report.

Source: 2026 Kaseya Cybersecurity Outlook Report.

1. The 2026 Threat Landscape

Attackers now move faster and more precisely with AI-assisted tooling. Automated phishing campaigns, session hijacking with stolen credentials, and opportunistic attacks against unpatched systems hit SMBs disproportionately hard.

Leading Threat Vectors

- **Credential-Based Attacks:** Weak Or Reused Passwords Remain The Easiest Way In.
- **Unpatched Vulnerabilities:** Delays In Closing Known CVEs Sit Behind A Large Share Of Breaches.
- **Ransomware 2.0:** Double Extortion — Encryption Plus The Threat Of Data Exfiltration.
- **Supply-Chain Risk:** MSPs Themselves Have Become A Primary Target.

> ”Most of our clients treated patch management as a background task — until a breach. Now we put it at the center of the contract.”

2. The Challenges MSPs & SMBs Face

MSPs must grow their client portfolio while managing an expanding attack surface with a limited pool of specialists. SMB clients, meanwhile, wrestle with shortages of budget, expertise and visibility.

Challenge	MSP Perspective	SMB Perspective
Talent gap	Finding and retaining skilled security staf	Cannot build an in-house security team
Visibility	Need for centralized monitoring across many clients	Unaware which assets are exposed
Patch management	Manual processes don't scale	Critical patches delayed for months
Compliance	Different regulatory load per client	Struggle to keep up with KVKK / sector rules

3. Where Budgets Are Shifting

Security spend has moved from the "optional" column to "operational necessity." SMBs are turning away from one-off hardware purchases toward predictable monthly subscription models and managed services.

Top Investment Areas For 2026

- **Identity And Access Management (IAM) With Self-Service Password Reset**
- **Automated Patch Management Platforms**
- **Endpoint Detection And Response (EDR/XDR)**
- **24/7 Monitoring And Managed Detection & Response (MDR)**
- **User Awareness Training**

OPEX

Subscription models are replacing CAPEX investments

Prevent

Budget weight is shifting from reactive to preventive solutions

Consolidate

Preference grows for a single, integrated managed platform

4. Rising Client Expectations

SMBs now position their MSP as a strategic security advisor. The "call us when something breaks" model is giving way to a proactive, reportable and measurable service relationship.

- **Transparency:** Regular Security Posture Reports And Clear Metrics.
- **Proactivity:** Risks Closed Before They Become Incidents.
- **Speed:** Response Measured In Minutes, Not Days.
- **Advisory:** Guidance On Investment Priorities.

5.New Opportunities For MSPs

Every challenge is a revenue opportunity for the well-positioned MSP. For partners looking to expand their portfolio in 2026, these stand out:

Challenge	MSP Perspective
Managed patching service	The #1 root cause of breaches; high margin through automation.
Self-service password reset	Cuts help-desk load, raises security, fast payback.
Security awareness subscriptions	Low-cost recurring revenue; targets the human factor.
Compliance packages	KVKK and sector rules create ongoing advisory work.

6.Your 2026 Readiness Checklist

A practical checklist to review together with your clients:

- ✓ Is automated patch management active across all clients?
- ✓ Has authentication been made multi-factor (MFA)?
- ✓ Is a self-service password reset portal in place?
- ✓ Is there an up-to-date inventory of critical assets?
- ✓ Is an incident response plan defined and tested?
- ✓ Are backups verified on a regular basis?
- ✓ Are clients given a regular security posture report?
- ✓ Do users receive regular awareness training?

How Arksoft Helps

Arksoft delivers managed security services for MSP partners and SMBs from a single source: automated patch management (Easy2Patch), self-service password reset (ArkSSPR), centralized endpoint management and compliance consulting. To be ready for 2026 and guide your clients with confidence, let's talk

Request A Free Consultation →