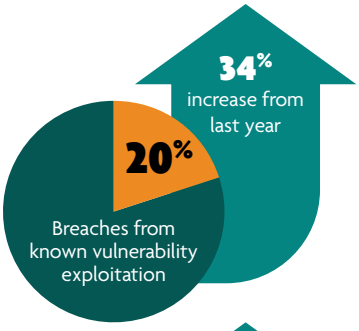

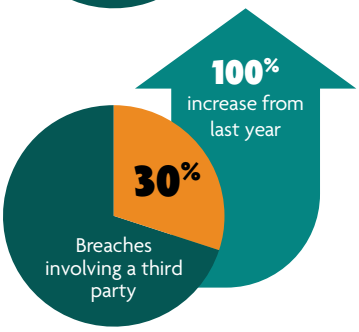

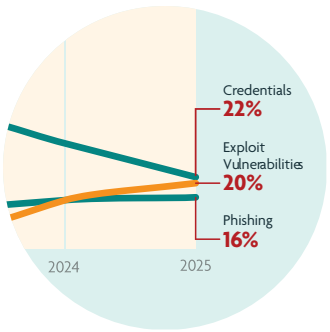

The 2025 cybersecurity crisis: How MSPs can protect their clients

Critical security alert: 2025 Verizon Data Breach Report findings

The latest Verizon Data Breach Investigations Report reveals an alarming trend: most organizations cannot keep pace with the evolving cybersecurity threats. As an MSP, your clients are counting on you to protect them from increasingly sophisticated attacks.

Key threat statistics

34% increase in breaches from known vulnerability exploitation compared to last year

100% increase in attacks involving third-party vulnerabilities

30% of breaches now involve third-party compromises, creating access points to client network

Only **54% of vulnerabilities** were patched before exploitation

20% of initial access breaches now begin with vulnerability exploitation, nearly matching credential theft (**22%**) as the top attack vector

Two critical security challenges putting your clients at risk

1. The vulnerability exploitation crisis

The reality: 20% of breaches stem from known vulnerability exploitation—a 34% increase from last year. Attackers are finding and exploiting new security weaknesses faster than most organizations' patching cycles.

What this means for your clients: While you manage their day-to-day IT operations, sophisticated attackers run automated scans, identifying and exploiting vulnerabilities within days—sometimes hours. This exposes your clients' data, operations, and reputation to significant risk that traditional MSP services often lack the specialized security bandwidth to address effectively.

2. The third-party security problem

The reality: 30% of breaches now involve a third party—double the figure from last year. Every vendor connection, integrated system, and supplier relationship can serve as an entry point for attackers targeting your clients' businesses.

What this means for your clients: Attackers are increasingly using third parties as gateways to breach their actual targets. Even with your strong internal controls, third-party vulnerabilities create backdoors into client networks, potentially exposing sensitive data and critical systems.

How MSPs can strengthen client protection

A proactive cybersecurity approach

Occasional patching and reactive incident response no longer provide adequate protection. Effective security now requires a proactive, comprehensive strategy focused on:

Continuous vulnerability management

- Automated scanning of all systems for known weaknesses
- Prioritization of patches based on actual exploit risk
- Public-facing systems patched first, regardless of operational convenience

Rapid remediation timeline

- Reducing client vulnerability exposure from months to days
- Implementing automated patching where possible
- Creating clear remediation processes for critical vulnerabilities

Visibility into security exposure

- Knowing which client systems are vulnerable, exposed, and critical
- Understanding your actual security posture, not just compliance checkboxes
- Identifying blind spots in client security programs

Third-party risk management

- Vetting vendor security practices before client integration
- Implementing strong access controls for third-party connections
- Segmenting networks to limit potential damage from partner breaches

Why MSPs need automated vulnerability management

Many MSPs lack the specialized expertise and resources to stay ahead of the vulnerability exploitation crisis. Your clients need proactive vulnerability management that:

Automatically identifies and prioritizes vulnerabilities before attackers exploit them.

Streamlines patch management with intelligent remediation workflows

Provides comprehensive compliance coverage across multiple frameworks

Delivers actionable risk assessments that drive profitable client conversations

Scales efficiently across your entire client base

Don't let your clients wait for a breach

ConnectSecure's automated **vulnerability management and compliance platform** integrates seamlessly with your MSP operations, whether you're just starting to offer security services or looking to enhance your current offerings.

Ready to turn vulnerabilities into revenue opportunities?

Start your **14-day free trial** or schedule a **private demo** to see how ConnectSecure can help you identify client risks and build stronger security service offerings.

Based on data from the 2025 Verizon Data Breach Investigations Report

Get started

See ConnectSecure in action with a Free 14-Day Trial.

No credit card required.

START YOUR FREE TRIAL

CONNECTSECURE

About ConnectSecure

ConnectSecure is a global cybersecurity company that amplifies managed service providers' (MSPs) ability to assess client risk, build recurring revenue, and overcome the challenges of the ever-evolving cyber threat landscape. Focused on partnering with and meeting the specific needs of MSPs, ConnectSecure delivers tools to identify and address vulnerabilities, manage compliance requirements, and grow service provider practices.