

How to Stop Advanced Threats Targeting Your Endpoints

Endpoints are often the first targets attackers go after, whether it's through ransomware campaigns or insider threats. As the most frequently targeted element of your IT environment, they need constant protection. To stay ahead, you need to understand who's behind the attacks, how they work and how to stop them.

KEY PLAYERS



RANSOMWARE GROUPS

DragonForce, Ransomware Hub, LockBit

These threat groups run ransomware like a business. They are targeted, fast and ruthless.



INSIDER THREATS

Disgruntled or ex-employees and hackers posing as insiders

Some employees misuse access to steal data or cause damage, while hackers phish their way in, act like trusted users and quietly steal sensitive information or money.

HOW THEY WORK



DOUBLE AND TRIPLE EXTORTION

Hacker groups don't just encrypt data, they threaten to steal it, leak it and demand multiple payouts along the way.



SUPPLY CHAIN TARGETING

Threat actors compromise one weak vendor and gain access to every business connected to them.



ADVANCED PERSISTENT ATTACKS (APT)

Attackers quietly infiltrate a network and lurk silently, waiting for the perfect moment to strike.



STOLEN CREDENTIALS

They use legitimate logins to quietly access sensitive data.



MOUSE JIGGLER SOFTWARE

Keeps sessions alive to avoid timeouts and stay under the radar.



PRIVILEGE ESCALATION

Once inside, they work their way up to take full control.

HOW TO DEFEND



CONTINUOUS MONITORING

Stay alert to changes in system behavior and catch threats before they spread.



EDR TOOLS

Detect and stop threats at the endpoint - where the battle begins.



OFFLINE BACKUPS

If cybercriminals encrypt everything, you'll still have a clean restore point.



BEHAVIORAL MONITORING WITH EDR

Spot unusual activity even from a valid user account.



VPN AND GEOLOCATION

Flag suspicious logins based on location or device.



RESTRICT ADMIN ACCESS

Fewer users with full control mean fewer chances of disaster.

Stopping advanced threats is easier with a layered approach. The award-winning solutions Datto EDR and Datto AV catch threats early while Datto Managed Detection and Response (MDR) provides 24/7 monitoring. Together, they strengthen your entire defense strategy. But don't just take our word for it. See what the third-party tests say in our latest report!

[READ THE MIERCOM REPORT](#)