Top Cybersecurity Threats to Watch in 2026

The most dangerous threats aren't always the loudest — they're the ones that blend in and exploit trust across operations. As attackers adapt to stronger controls and increased AI adoption, several threat patterns are accelerating faster than organizations can keep up.

Social engineering at scale

Generative AI is enabling hyper-personalized phishing, vishing, and impersonation campaigns that are harder for users (and filters) to detect.

- Deepfake executives and vendors
- Context-aware lures trained on public data
- Automated campaign testing and optimization

Why it matters: Trust (not technology) becomes the primary attack surface.

Identity-first intrusions

Attackers are increasingly bypassing exploits by logging in as an employee or known entity, versus breaking down the front door to the organization.

- MFA fatigue and token theft
- SaaS account takeovers
- Abuse of over-privileged identities

Why it matters: Traditional perimeter and endpoint defenses never trigger.

Lateral movement across cloud / SaaS

Compromised credentials are being used to pivot silently between cloud apps, escalating access and exfiltrating data without malware.

- OAuth token abuse
- Shadow SaaS expansion
- Data exfiltration via legitimate APIs

Why it matters: Breaches look like normal user activity.

Multi-extortion ransomware campaigns

Ransomware operations are evolving beyond encryption into data theft, harassment, and regulatory pressure.

- Double and triple extortion
- Targeting backups and recovery systems
- Data leaks timed for maximum impact

Why it matters: Recovery alone no longer resolves the incident.

splunk>
a CISCO company

Software and supply chain attacks

Attackers are exploiting trusted software, updates, and vendors to gain initial access.

- Compromised dependencies
- Malicious updates
- Third-party access abuse

Why it matters: Trusted relationships become attack paths.

API-centric attacks

As APIs power modern applications and integrations, attackers are targeting weak authentication and excessive permissions.

- Broken object-level authorization
- Token leakage
- Abuse of undocumented endpoints

Why it matters: APIs expose data and functionality at scale.

Living-off-the-land (LotL) attacks

Threat actors continue to blend in by abusing native tools and administrative utilities.

- PowerShell, WMI, and CLI abuse
- Minimal malware footprint
- Difficult forensic visibility

Why it matters: "Nothing looks malicious" until it's too late.

Exploitation of newly disclosed vulnerabilities

Time-to-exploit is shrinking dramatically.

- Weaponization within hours
- Automated scanning and exploitation
- Patch gaps exploited at scale

Why it matters: Detection and response time matters as much as prevention.

Turn threat awareness into action

Download our latest edition of Top 50 Cybersecurity Threats to discover the most common threat types; how and why they're evolving; and where to aim your defenses next. And when you're ready to turn that intelligence into action, Splunk can help bring clarity and speed to your security operations.