CHECKLIST

Tips for Simplifying Endpoint Security with a Unified Agent

Securing today's distributed workforce has led to increasingly fragmented and complex endpoint security. Security teams often rely on multiple agents to handle protection, detection, vulnerability management, and secure access, which can create performance issues, integration gaps, and management overhead. A unified agent strategy addresses these challenges by consolidating multiple functions into a single endpoint solution. These tips can help you successfully evaluate and implement a unified agent approach.

☑ Secure Connectivity

To support modern workforces, endpoint protection must go beyond prevention and threat detection and include secure, zero-trust access. A unified agent should establish encrypted tunnels, enforce policy-based access control, and continuously assess device trust. Integrating continuous zero-trust device posture checks with zero-trust network access (ZTNA) and virtual private network (VPN) solutions ensures that access to applications is granted only to functional, authenticated devices, minimizing the attack surface without degrading the user experience.

☑ Protection Efficacy

Effective endpoint defense requires behavior-based detection that operates independently of cloud lookups or signature databases. Security teams should prioritize endpoint detection and response (EDR) platforms that monitor kernel-level activity in real time, offering protection against unknown threats, fileless attacks, and lateral movement. This approach requires a unified agent capable of enforcing local runtime decisions with high fidelity and low false positives. Look for proven efficacy, such as 100% protection ratings in independent evaluations by third-party organizations like SE Labs, to ensure the platform delivers reliable, real-world security.

☑ Vulnerability Ratings

Modern endpoint protection must include integrated vulnerability assessment. A unified agent should continuously scan for known exploits, outdated software, and misconfigurations, delivering contextual risk scores and patch guidance. Support for virtual patching is essential for maintaining protection when permanent fixes are not yet available, as it reduces exposure without operational disruption.

☑ Ransomware Defense and Recovery

Endpoint platforms must defend against ransomware before, during, and after execution. Offline behavioral analysis should detect and contain threats without relying on internet connectivity. Online, the system should enforce dynamic policies based on user, device, and application context to prevent privilege escalation or data exfiltration. Integration with sandboxing and threat intelligence platforms is critical for timely response and recovery.

☑ Anti-Tampering Capabilities

Endpoint agents must be resilient by design. Tamper resistance is non-negotiable. Agents must prevent unauthorized modification or shutdown, especially during attacks. Kernel-level integration helps enforce this capability, along with cryptographic validation of processes and configuration.

Ensuring agent integrity is a prerequisite for any meaningful detection and response capability. Third-party testing frameworks, such as those used in antivirus anti-tampering evaluations, can provide valuable validation of an agent's resilience and help benchmark effectiveness across vendors.

☑ **Operating System Support**

Endpoint protection must operate uniformly across diverse environments. Security teams should demand unified agent support for Windows, macOS, and key Linux distributions without sacrificing functionality. Feature parity across operating systems ensures that detection, prevention, and response workflows remain consistent, regardless of platform.

☑ **Agent Weight and Interoperability**

Lightweight, efficient agents are essential for enterprises. Endpoint protection should not require scheduled scans or heavy system resources. The unified agent must operate silently, consuming less than 1% of system performance, while maintaining full compatibility across OS versions, virtual environments, and security tools, minimizing support overhead and software conflicts.

☑ **EDR Automation**

EDR should reduce the workload of the security operations center, not add to it. Organizations need platforms that automate triage, containment, and ticketing through prebuilt playbooks and adaptive policies. A unified agent must support multi-tenant and multi-user environments, integrate with third-party tools such as security information and event management (SIEM) and identity and access management (IAM) systems, and deliver actionable outcomes without requiring manual intervention.

☑ **Extended Detection and Response Capabilities**

To scale, EDR must evolve into extended detection and response (XDR), which requires an endpoint agent that serves as a telemetry anchor, capturing rich data across devices, users, and applications. Organizations should prioritize solutions that enable the endpoint agent to correlate data natively with network, identity, and cloud sources, driving fast and coordinated responses across domains.

☑ **Managed Service Options**

Not all organizations can staff a 24×7 SOC. Endpoint protection must provide access to managed detection and response services that extend coverage, augment internal teams, and expedite response times. A unified agent should enable these services through integrated telemetry, remote response capabilities, and clear alerting protocols without requiring additional tooling.

☑ **Total Cost of Ownership**

Reducing costs starts with consolidation. A unified endpoint agent should combine secure connectivity, threat prevention, detection, and response. This consolidation streamlines operations, reduces the support burden, and simplifies licensing. Additionally, seamless integration with existing security infrastructure further lowers total cost of ownership by eliminating the need for redundant tools, enabling faster deployments, and maximizing the value of current investments. Together, these efficiencies contribute to stronger protection with significantly reduced complexity and cost.

FortiEndpoint Meets Modern Requirements

FortiEndpoint meets modern endpoint security requirements through a single, unified agent based on FortiClient. It integrates secure connectivity, real-time prevention, behavioral detection, and response automation. FortiEndpoint supports all major operating systems, operates with minimal impact, and connects natively into the broader Fortinet Security Fabric. FortiEndpoint enables organizations to converge endpoint protection and access control, delivering better security outcomes with lower complexity. Learn more about Fortinet Endpoint Security solutions and our approach to unified endpoint protection.

July 10, 2025 4:08 PM / MKTG-1635-0-0-EN