

## Competitive Battlecard

SECURUS  360 VS  CROWDSTRIKE

### SECURUS 360 Core Capabilities

**Sapphire AI Insights Sapphire**

Delivers 98%+ accurate autonomous investigations – closing 70% of benign cases without analyst involvement.

**Sapphire SOC Analyst**

Automates 90% of Level 1 and 2 analyst tasks. Faster triage, less burnout, more consistent outcomes 24/7.

**XDR Agent**

Deep endpoint telemetry feeding realtime detection. Every signal captured, in context, the moment it happens.

**Cloud Security**

Integrated CDR and CSPM – cloud attacks stopped and misconfigurations caught before they become exposures.

**SIEM**

AI-powered and built into the platform, not bolted on, not outsourced. Detection, investigation, and response in one place.

**Threat Exposure Management**

Visibility across vulnerabilities, dark web activity, external exposures, and Shadow AI, before attackers find them.

**Vulnerability Scanning**

Widespread cyber infrastructure scanning with detailed reports and remediation steps.

**M365 Security**

Catches Microsoft 365 misconfigurations with prioritized remediation so nothing slips through.

**Strategic Advisory**

Direct access to experienced security leaders to build your roadmap, meet compliance, and reduce long-term risk.

### CROWDSTRIKE Core Capabilities

Source: <https://www.crowdstrike.com/en-us/>

**Falcon Endpoint Protection (Next-Gen AV)**

Protects against malware, ransomware, and sophisticated attacks across endpoints. Deploys in minutes via a single lightweight sensor.

**Cloud Security (CNAPP)**

Unified cloud-native application protection across workloads, containers, and cloud configurations.

**Charlotte AI**

AI assistant that accelerates investigations and surfaces insights across analyst workflows.

**Endpoint Detection & Response (EDR)**

Continuous endpoint visibility with automated detection and intelligent prioritization of malicious activity.

**Next-Gen SIEM**

Log ingestion, correlation, and detection across the environment, delivered through the Falcon platform.

**Managed Detection & Response (Falcon Complete)**

Fully managed endpoint protection and response available as a separate add-on service tier.

**Identity Protection**

Detects and stops identity-based attacks, credential abuse, and lateral movement in real time.

**Threat Intelligence & Huntig**


Adversary intelligence and proactive threat hunting delivered through the Falcon platform.

**Exposure Management**

External attack surface management and vulnerability prioritization across assets.

Category	Securus360	CrowdStrike	The Difference
<b>Core Model</b>	Unified AI-native SecOps platform. Detection, investigation, and response complete out of the box <b>ADV</b>	Modular platform – full coverage assembled across bundles, tiers, and add-ons	<b>Complete vs. assembled.</b> Securus360 is comprehensive from day one. CrowdStrike's coverage depends on which modules you've purchased.
<b>SOC Model</b>	AI automation with human oversight and built-in SOC support – included in the platform <b>ADV</b>	Self-operated platform with Falcon Complete managed service available as a separate paid tier	<b>Included SOC support vs. paid add-on.</b> Securus360's SOC backing is part of the platform. With CrowdStrike, full managed coverage is an additional cost.
<b>SIS Visibility</b>	Native PowerSchool and SIS activity monitoring and correlation <b>ADV</b>	Endpoint and identity visibility across connected systems	<b>Visibility beyond the device.</b> Securus360 connects endpoint, identity, and PowerSchool activity to detect threats impacting student and staff accounts.
<b>AI / Analytics</b>	Agentic AI autonomously investigates, decides, and responds – 99% reduction in false positives <b>ADV</b>	Charlotte AI assists analysts with investigations and surfaces insights to accelerate workflows	<b>Autonomous AI vs. AI-assisted analysts.</b> Sapphire acts without waiting for human input. Charlotte AI makes humans faster, but humans still drive the workflow.
<b>Detection, Investigation &amp; Response</b>	48% faster response to malicious attacks – executed autonomously inside the platform <b>ADV</b>	EDR with automated response capabilities – analyst-driven or via Falcon Complete add-on	<b>Autonomous execution vs. analyst-executed.</b> Securus360 closes threats without human intervention. CrowdStrike's full managed response requires either internal resources or Falcon Complete.
<b>Platform Architecture</b>	Single unified platform – all capabilities operate within one workflow, no assembly needed <b>ADV</b>	Modular Falcon platform – capabilities added via tiers, bundles, and integrations	<b>Unified by design vs. unified by assembly.</b> Securus360 is one product. CrowdStrike is many products on one platform.
<b>Automation / SOAR</b>	Automation embedded natively across all workflows – works without additional configuration <b>ADV</b>	Fusion SOAR available for automated response – effectiveness depends on playbook setup and configuration	<b>Out-of-the-box vs. configured.</b> Securus360 automates by default. CrowdStrike's automation delivers more value the more you invest in configuring it.
<b>Risk &amp; Vulnerability Management</b>	Continuous exposure visibility across vulnerabilities, dark web activity, external risk, <b>ADV</b>	Exposure management and vulnerability prioritization via Falcon Surface module	<b>Broader native scope.</b> Securus360 includes dark web monitoring and Shadow AI visibility as part of the core platform – coverage areas that require additional CrowdStrike modules.
<b>SIEM &amp; Log Management</b>	Built-in AI-powered SIEM – included in the core platform, no separate license	Next-Gen SIEM available within the Falcon platform – inclusion varies by bundle tier	<b>Verify with your rep.</b> Securus360's SIEM is always included. CrowdStrike's SIEM availability depends on which tier you're on, confirm what's covered before comparing.
<b>Endpoint Visibility</b>	Deep endpoint telemetry via XDR agent across all connected devices	Endpoint telemetry via single lightweight Falcon sensor across devices	<b>Comparable.</b> Both platforms deliver strong endpoint visibility – Securus360 within a broader unified workflow, CrowdStrike through a dedicated sensor with deep
<b>Cloud Security</b>	Integrated CDR and CSPM – cloud attacks stopped and misconfigurations caught	Comprehensive CNAPP covering workloads, containers, and cloud configurations	<b>Comparable.</b> Both deliver strong cloud security coverage through different architectural approaches.

## WHY ORGANIZATIONS CHOOSE SECURUS360

 **CROWDSTRIKE** built the best endpoint tool.

 **SECURUS360** built the complete platform.

CrowdStrike is one of the most recognized names in cybersecurity and for good reason. Their endpoint detection is strong and their platform runs deep. But **recognition doesn't always mean the right fit**.

The challenge with CrowdStrike is that full coverage comes with full complexity. Comprehensive protection means assembling the right combination of modules, bundles, and tiers. **SOC support is a separate purchase**. Automation delivers more value the more you configure it. For many organizations, the result is a powerful but expensive stack that still demands significant internal resources to operate.

Securus360 gives you a **complete, unified AI-native platform – SOC support, SIEM, XDR, vulnerability management, cloud security, and exposure visibility, without the assembly**. One platform, one workflow, one cost structure built for organizations that need comprehensive coverage without enterprise-level complexity.

### 99%

**Reduction in False Positives**  
Sapphire AI and your SOC team eliminate noise at the source.

### 48%

**Faster Threat Response**  
From detection to decision to action – inside one platform.

### 70%

**Less Time on Benign Cases**  
Sapphire auto-closes what doesn't need human attention.



### Complete Coverage, Day One

CrowdStrike's full protection requires selecting the right tiers, bundles, and modules. Securus360 ships complete – SIEM, XDR, cloud security, vulnerability management, and SOC support all included from the start. No assembly. No surprises



### SOC Support That's Already Included

With CrowdStrike, fully managed coverage means purchasing Falcon Complete on top of your existing licenses. Securus360's SOC support is built into the platform. Expert backup without a separate contract or line item.



### AI That Acts, Not Just Assists

CrowdStrike's Charlotte AI makes your analysts faster. Sapphire AI removes the analyst from the equation for 70% of cases; investigating, deciding, and responding autonomously so your team spends time only on what genuinely requires human judgment.



### One Platform = Lower Complexity

CrowdStrike's model means more licenses, more integrations, and more internal overhead to operate effectively. Securus360 consolidates your security stack into one platform for fewer tools, contracts, and a total cost of ownership built for organizations that want comprehensive protection without enterprise-level resources.

## See Securus360 in Action

Launch a self-guided tour to explore how Securus360's unified platform supports detection, investigation, and response.

[Launch Tour](#)