corsica technologies

SECURITY SOLUTION DISCOVERY GUIDE

Datto EDR vs. Microsoft Defender + Sentinel

Two managed detection & response stacks that map directly to one another. Both are **EDR + MDR**, both run 24/7 by a SOC — so the real decision comes down to two things: **how customizable** you need it, and **how the costs are structured**.

01 Two stacks that map to each other

Add Microsoft Defender to Sentinel and you have a genuine apples-to-apples comparison. Each stack is the same three parts — **a tool (EDR), a managed service (MDR), and a SOC** — just from a different vendor.

Datto EDR

A KASEYA PRODUCT

EDR · MDR · SOC

- EDR **The tool** — Datto EDR endpoint agent
- MDR **The service** — managed detection & response
- SOC **The people** — Corsica SOC, 24/7 response

Defender + Sentinel

A MICROSOFT PRODUCT

EDR · MDR · SOC

- EDR **The tool** — Defender endpoint agent + Sentinel SIEM
- MDR **The service** — managed detection & response
- SOC **The people** — Corsica SOC, 24/7 response

THE KEY DISTINCTION

EDR is a **tool** — software that runs on endpoints

MDR is a **service** — "managed" means people run it for you

02 Side-by-side at a glance

	Datto EDR KASEYA · EDR + MDR + SOC	Defender + Sentinel MICROSOFT · EDR + MDR + SOC
VENDOR	Kaseya product	Microsoft product
THE STACK	Datto EDR — tool + managed service	Defender (EDR) + Sentinel (SIEM)
MANAGED BY	Corsica SOC — 24/7 detect & respond	Corsica SOC — 24/7 detect & respond
CUSTOMIZATION	Baseline policies you can tweak	Build from the ground up — granular rules
COMPLIANCE FIT	May lack a rule for niche frameworks	Build any rule to match your framework
COST MODEL	Bundled, predictable subscription	Per-user licensing + Azure ingestion
LICENSING	Included in the service	May need E3 / E5 — up to +$20 / user / mo
WHERE COSTS SIT	Bundled within Corsica Secure	Separate line from Corsica Secure — still via Corsica as CSP
BEST FIT	SMB / standardized requirements	Regulated / complex / highly custom

03 Strengths & considerations

Datto EDR

STRENGTHS

- \+ 24/7 managed detection & response via Corsica SOC
- \+ Fast deployment, low operational overhead
- \+ Predictable, fully bundled cost
- \+ Strong endpoint protection out of the box

CONSIDERATIONS

- − Baseline policy set — less granular customization
- − May lack out-of-the-box rules for niche compliance frameworks
- − Less suited to highly bespoke security requirements

Defender + Sentinel

STRENGTHS

- \+ Build from the ground up — granular, custom detection rules
- \+ Map controls to any compliance framework (HIPAA, CMMC, SOC 2)
- \+ Enterprise-scale visibility, analytics & forensics
- \+ Same 24/7 managed response from Corsica SOC

CONSIDERATIONS

- − Higher, variable cost — per-user licensing + Azure ingestion
- − May require an E3 / E5 upgrade (~+$20 / user / mo)
- − Licensing & Azure billed separately from Corsica Secure

04 The cost conversation

This is where the two models genuinely diverge. Datto EDR is one bundled, predictable fee. Defender + Sentinel introduces Microsoft licensing and Azure costs that are billed directly to you — and stay with you no matter who manages the service.

Datto EDR

BUNDLED & PREDICTABLE

One managed fee

Tooling, managed service and SOC labor are bundled into a single subscription — Corsica's cost of goods is built in.

- ✓ No new Microsoft end-user licensing required
- ✓ No separate Azure ingestion bill
- ✓ Easy to budget, month over month

Defender + Sentinel

THREE MOVING PARTS TO BUDGET

1. **Per-user licensing**
   Users often must move from Business Premium up to **E3 or E5** — an increase of up to **$20 / user / month**. Billed directly by Microsoft.
2. **Azure ingestion**
   Sentinel logs to Azure — a separate, usage-based bill from Microsoft on its own pricing structure. We can **estimate your ingestion before you commit**.
3. **Separate from Corsica Secure**
   Licensing and Azure sit on a **separate line from your Corsica Secure managed service**. Corsica remains your CSP, so billing still runs through us.

⚠ **Business Premium alone isn't enough.** Without the right end-user licensing, Defender + Sentinel can't fully monitor email, SharePoint Online and user activity — so the tools can't deliver the visibility you're paying for. The license tier is what gives them that reach.

05 When to choose each

CHOOSE DATTO EDR IF

- → You want one predictable, bundled cost
- → Baseline security policies meet your needs
- → You're an SMB or have standardized requirements
- → You want fast time-to-value, low overhead
- → You don't need to build custom compliance rules

Excels at standardized protection, predictable cost.

CHOOSE DEFENDER + SENTINEL IF

- → You're in a highly regulated industry (HIPAA, CMMC, SOC 2)
- → You need custom rules mapped to your own framework
- → You want granular control over detection & data protection
- → You have — or are growing into — a complex environment
- → You can absorb per-user licensing + Azure costs

Excels at tailored controls for your exact compliance needs.

06 It's not either / or — it's where you are in the journey

Many organizations start with Datto EDR for fast, predictable, standardized protection — then move to Defender + Sentinel as they grow more complex or more regulated and need to build controls to their own framework.

START HERE
Datto EDR
Fast protection, managed response, predictable bundled cost.

→

MATURE INTO
Defender + Sentinel
Custom rules, compliance-grade visibility & forensics at scale.

THE CORSICA DIFFERENCE

We deliver both — and help you pick the right starting point.

Fully managed or co-managed, with a 24/7 SOC, deep Microsoft Defender + Sentinel expertise, and our Cybersecurity Guarantee. Let's map your environment, compliance needs and budget to the right model — and estimate your Azure costs before you commit.

GUARANTEE

Book a discovery consultation

855-411-3387 · corsicatech.com