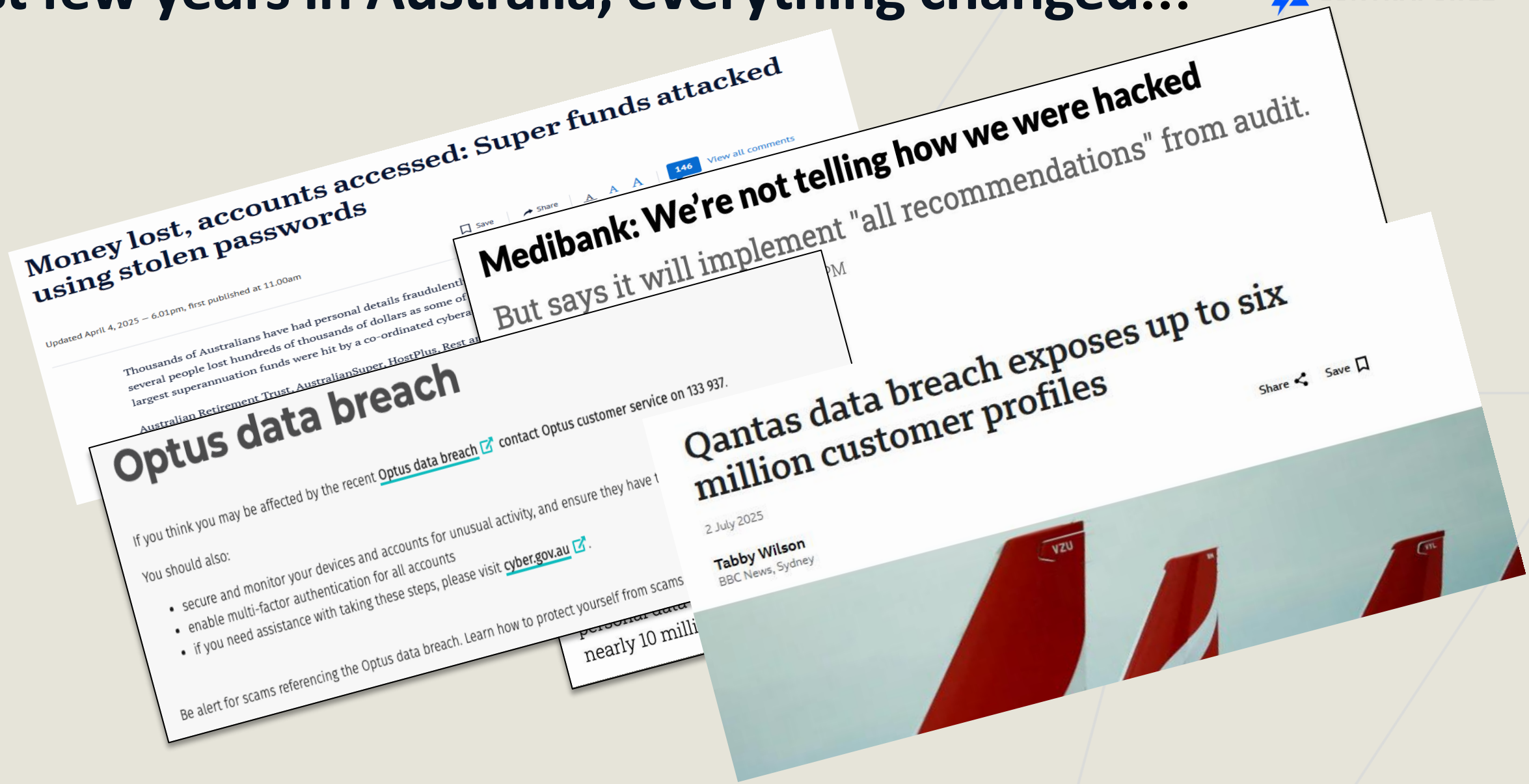
Automate Microsoft Threat Protection with Sentinel + ContraForce

Last few years in Australia, everything changed...

CONTRAFORCE



Your customers are now aware of security and the need to improve it…

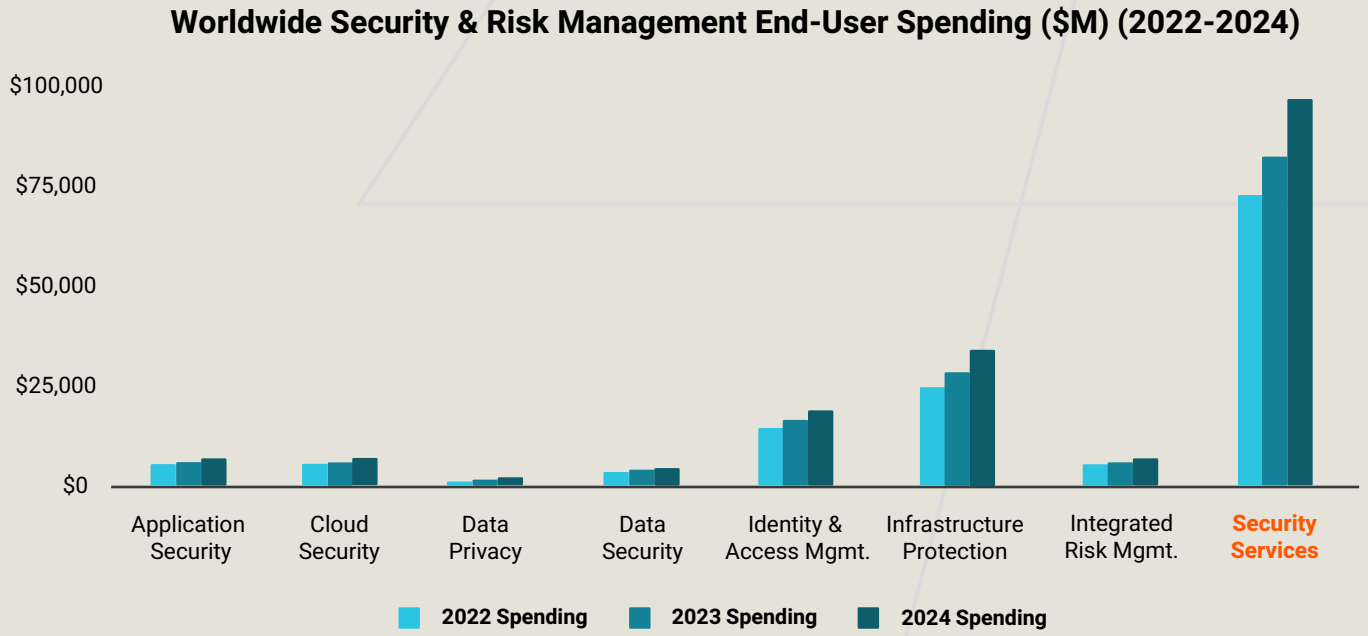
CONTRAFORCE

WHY NOW?

Growing Need for Security Services

Security Services Growth

In terms of total spend, **security services** continues to lead the way by a large margin, representing **42%** of total security and risk management end-user spending in 2024.

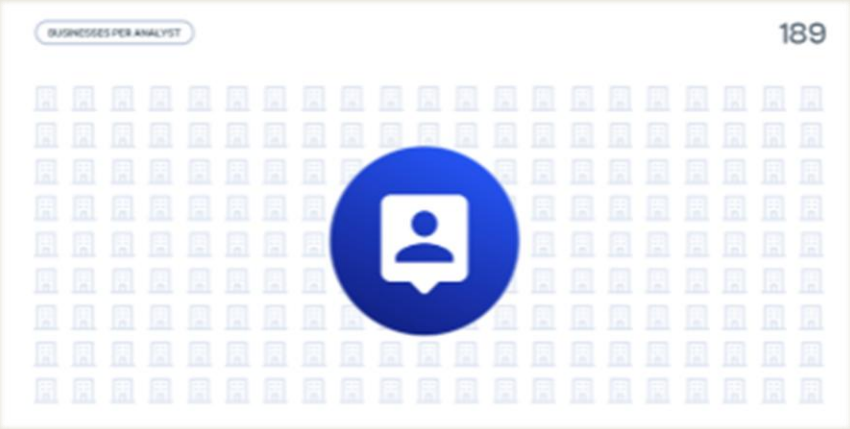


Source: Gartner

Two Challenges Managing Security

Expertise

- Finding and keeping security staff can be difficult
  - There is only 1 security analyst for every 189 US businesses[1]



Time

- Managing security can be time intensive, especially a SIEM:
  - Managing detection rules
  - Collecting context for incidents
  - Determining response actions

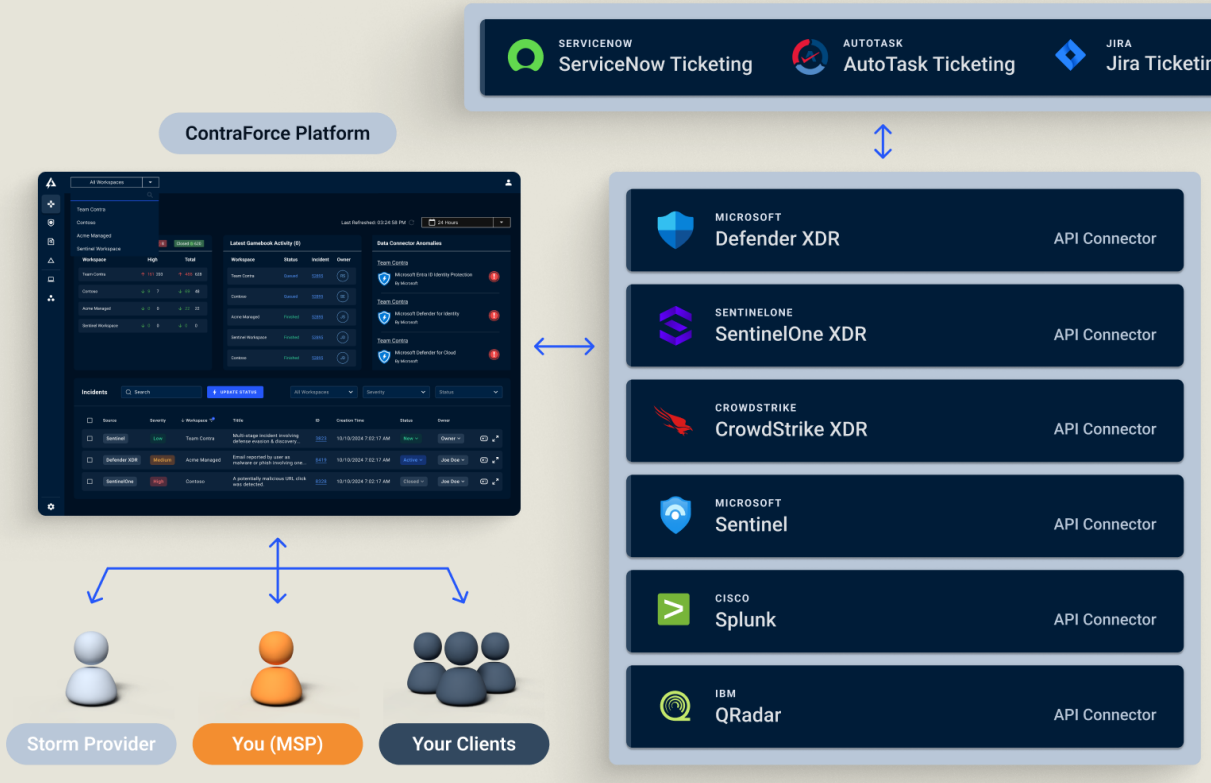
1. Growth Without Gains, ContraForce, 2025.

CONTRAFORCE

How do MSPs ensure customers are secure and protected from Cybersecurity incident ?

CONTRAFORCE

What is ContraForce ?



- Multitenant security platform that let you monitor all customer incidents.
- Deliver threat detection, investigation and response.
- API-Based Integration lets you onboard new clients within 30 minutes.
- Manage your clients' tools:
  - Endpoint including **Microsoft Defender**, **Crowdstrike**, & **SentinelOne.**
  - SIEM including **Microsoft Sentinel**, **QRadar**, & **Splunk.**
  - Integrate with your ticketing: like **ServiceNow**, **Autotask**, & **Jira.**
- Flexibility in service delivery, SLAs, month-to-month contracts.

CONTRAFORCE

Deliver XDR with Microsoft Defender and ContraForce

Defender XDR

Microsoft 365 E5 Security suite

- Defender for Endpoint P2 (Device Security)
- Defender for o365 P2 (Collaboration Security)
- Defender for Identity (Identity Monitoring)
- Defender for Cloud Apps (SaaS Security)
- Entra ID P2 (Identity & Access Controls)

Defender for Cloud

- Defender for Server
- Defender for Database
- Defender for Container
- Defender for Storage
- Defender for IoT

Microsoft Purview (Insider Risk Mgmt. & DLP)

Non-Microsoft log sources

Microsoft Sentinel

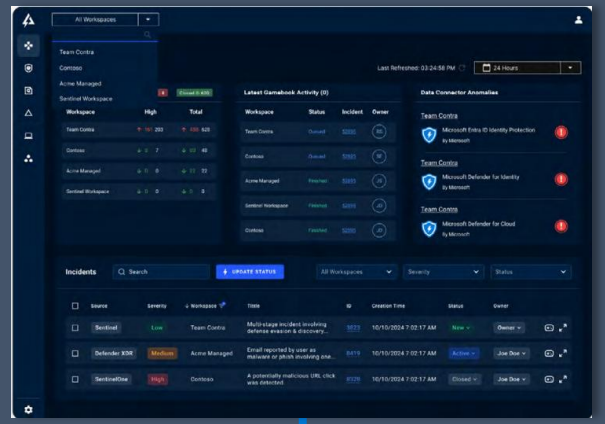
CROWDSTRIKE

SentinelOne

...

ContraForce

(Security Service Delivery Platform)



3rd Party SP

You (MSSP)

Managed Clients

Crayon

High Level overview On How ContraForce is Different

	ContraForce	Traditional MDR Providers
Contract Flexibility	• Month-to-Month • No long-term commitment	• Annual contracts • Not transferable between clients
Ease of Onboarding	• API-based • Onboarding in <30 minutes	• Agent-based • Ongoing maintenance as client endpoints added/removed
Improve ROI of existing tools	• No additional fees for EDR or SIEM	• Separate payment for proprietary EDR and SIEM tools
SLAs	• 1-hour detection and response SLAs for high severity incidents	• No contractual SLAs
24/7 visibility	• You and your clients	• Either you or your clients
Integration	• EDR: MDB, MDE, Crowdstrike • SEIM: Microsoft Sentinel, QRadar, & Splunk • ServiceNow, Autotask, & Jira	• Uses proprietary EDR & SEIM Tools
DIY SOC	• Migrate to your own SOC whenever you are ready (ContraForce Spark) • Increase your service margin	• Locked into their SOC

CONTRAFORCE

Meet Your Presenters

Automate Microsoft Threat Protection with Microsoft Sentinel

SPEAKERS

Nino Granzotti
Global Success Manager

Scott Goodman
Head of Sales

CONTRAFORCE

Agenda

August 14, 2025

- The Cybersecurity Crisis
- How to Automate your Microsoft Security Practice
- Microsoft Sentinel Update and Best Practices
- Q&A and Closing Remarks

ContraForce

Turning MSPs into MSSPs

Microsoft
Excellence Awards 2025
Microsoft Intelligent Security Association
FINALIST
ContraForce
Security ISV of the Year

Member of
Microsoft for Startups
Pegasus Program
Microsoft

Member of
Microsoft Intelligent
Security Association
Microsoft

Cyber Defense Magazine
Top Infosec Innovator
2024

SINET16
Innovator Award
2024

CRN 2024
Stellar Startups

SC Award 2024
Most Promising
Early Start Up

CONTRAFORCE

CONFIDENTIAL

The SECURITY SERVICE LANDSCAPE

The Cybersecurity Crisis

50% of businesses will out-source MDR to a MSSP in 2025

$10.5 Trillion
The Size of the Cybercrime Economy

$9.5 Billion
MDR Market Size by 2028

23.3%
MDR Market Annual Growth Rate

But MSSPs are struggling with:

- ✖ High onboarding costs
- ✖ Manual incident handling
- ✖ Scaling profitably
- ✖ Hiring security analysts

MDR (Managed Detection & Response): 24x7 outsourced security team that monitors your systems for threats, quickly finds attacks, and either fixes them or tells you exactly what to do

Democratizing Enterprise-Class SecOps

Making SOC Infrastructure Accessible to All

Before ContraForce

- ✖ Enterprise SOCs cost millions to build
- ✖ Require specialized security analysts
- ✖ Tooling only for enterprise budgets
- ✖ SMBs stuck with basic endpoint protection
- ✖ High barrier to entry for MSPs

After ContraForce

- ✓ MSPs can offer enterprise-class MDR
- ✓ Pay-as-you-scale economics
- ✓ Modern security stack accessible to all
- ✓ Grow ARR without hiring analysts
- ✓ Instant deploy of SOC capabilities

The Infrastructure Revolution

Just as cloud platforms democratized enterprise infrastructure, ContraForce democratizes enterprise security operations for the SMB and mid-market through channel partners.

The ContraForce Solution

Transform your IT team and service desk into a SOC

The Agentic Security Delivery Platform (Private Preview)

Core Capabilities:

- Autonomous Security Delivery Agents
- Intelligent workflow orchestration
- Multi-tenant isolation with shared intelligence
- Full explainability and audit compliance
- Zero analyst headcount scaling

60x

Faster incident response time
(30 min -> 30 sec)

95%

Cost reduction per incident
($15 -> <$1)

∞

24/7, multi-tenant, vendor agnostic, and free of human fatigue for infinite scale

CONTRAFORCE

Microsoft Sentinel Updates

Microsoft Sentinel is Changing

Sentinel’s migration to the Defender XDR portal

Microsoft Security consolidation continues

- From July 2026 forward, Sentinel will only be available in the Defender XDR portal.
- Does not require an underlying Defender license.
- All net-new deployments of Sentinel will be automatically onboarded to Defender XDR portal.
- If using Sentinel in the Defender XDR portal, Sentinel consumption pricing still applies.
- Access management and RBAC is changing – plan accordingly!

Sentinel Date Lake

Lowering long-term storage costs

Now in Public Preview

- Mainly effects retrospective investigations and long-term storage. There will be minimal impact on hot-storage and day-to-day investigations
- Start by using the data lake for low-frequency, long-term telemetry (i.e., DNS logs, firewall logs, or authentication records)
- Restrict or audit access to compute-heavy tools until your team gets more comfortable with forecasting cost
- Position it as an enhancement to existing Sentinel deployments, not a replacement

CONTRAFORCE

CONFIDENTIAL

PLATFORM DEMO

CONTRAFORCE

CONFIDENTIAL

Automate Your Microsoft Security Practice

Why Microsoft Sentinel + ContraForce

- Let Sentinel act as the security automation infrastructure for your customers
- Sentinel can be VERY cost effective AND provides granular detections and automation to identify and stop threats fast
- **Maximize existing Microsoft investment and relationship:**
  - BP, E3, E5 all have great security technologies that generate valuable telemetry, Send to Sentinel for low/no cost.
  - Unlock discounting and MDF incentives
- **ContraForce gives you a simple and clean interface providing:**
  - Unified visibility for a single source of truth
  - Out of the box automation to reduce labor overhead
  - Custom Detection Analytic Rules for reduced false positives and improved efficacy

Position Your MDR Offering

Target: SMB to mid-market customers (50–1,000 users), especially Microsoft Business Premium and E3/E5 license holders – **Bundles Only!**

Package MDR with Microsoft 365 Business Premium, Defender for Endpoint, Defender for Office 365, Entra ID, E3/E5 and Sentinel.

- Basic – Endpoint, Identity and Email – Business Hours Only
- Advanced – Include XDR Coverage and 24/7 Protection
- Elite – Custom Rule Detections, Logging and Monthly Reporting

Positioning:

- Emphasize business outcomes – Keep it simple and focus on outcomes
  - Ransomware and malware protection
  - Business Email Compromise (BEC) and phishing
  - Regulatory compliance

Microsoft Sentinel Cost Examples

Variables

- Sentinel Data Connectors (Entra ID, EDR, XDR, Network)
- Number of Users
- Data Retention
- Sentinel Ingestion Cost: $0.37-$3.39 per user/mo

	Data Connectors Enabled	Users	Ingestion Cost per user/mo	ContraForce WS Cost	Total Cost per month
Customer 1	0365 + Defender (2)	25	$0.37	$57	$66.25
Customer 2	+XDR (8)	75	$0.75	$57	$113.25
Customer 3	+ Network (13)	75	$3.39	$57	$311.25

Cost Comparison against Huntress

Variables

- **Fixed vs. variable cost:** ContraForce's flat $57/tenant/month means effective per-user cost drops dramatically as the number of seats increases. $5 - $6 per user/month gap across all seat counts.
- **Savings at scale:** At 250 seats, you're saving **$1,286/month** vs Huntress Managed EDR+ITDR in this example.
- **Margin impact:** For MSPs, the predictable fixed pricing makes it easier to model margins and scale without proportional cost growth.

User Count	Business Premium	CF WS	Total BP + CF	Huntress MDR	Huntress Managed ITDR	Total BP + Huntress
50	$1,974	$57	$2,031	$241	$138	$2,353
100	$3,948	$57	$4,005	$413	$207	$4,568
250	$9,870	$57	$9,927	$860	$483	$11,213

Crayon

Presentation

Questions

If you’re ready to put what you’ve learned into action — let’s talk.

Book a follow-up meeting to:

- Learn how to deploy Microsoft Sentinel and ContraForce in minutes
- See how to automate incident response
- Discover how to package, price, and sell MDR services
- If you have more questions about anything discussed today

Get Started

We’re committed to your success.

- Partner with us to build a business case
- Explore Contraforce Resources
- Why ContraForce Stands Out Blog & Demo
- Get Our Recent Research
- Cybersecurity Resource Round-Up

CRAYON APAC

Thank you!

Alaa Rahal
Pre-Sales technical MW & Security

alaa.rahal@crayon.com

Scott Goodman
Head of Sales

scott@contraforce.com

Nino Granzotti
GlobalManager

nino@contraforce.com