OSTRA
Your Trusted Cybersecurity Team™

NEW PARTNER ACADEMY

Sales Training

Agenda

- Ostra Origin & Mission
- Ostra Solution Components
- Sales Journey
- Starting the Conversation
- Getting to Yes
- Resources

OSTRA

OSTRA ORIGIN & MISSION

Why We Do What We Do

About Ostra

Origin Story

- Founded by Michael Kennedy

- A defining ransomware event changed his focus

- Founded Ostra to better protect SMBs

OSTRA

Beat the statistics

Ostra simplifies cybersecurity while providing Fortune 100-level, proactive, layered data protection to businesses of all sizes

Average time for a company to discover a data breach:

277 Days

(Source: IBM 2024)

How frequently a cyberattack occurs:

39 seconds

(Source: Cobalt 2024)

Average cost of a data breach:

$4.88 Million

(Source: IBM 2024)

OSTRA

OSTRA SOLUTION COMPONENTS

How We Do What We Do

Ostra Solution Components

24/7 Managed Security Operations Center (SOC)
- ✓ 24/7 monitoring
- ✓ Round-the-clock support
- ✓ Advice from our knowledgeable team of experts

24/7 Security Information and Event Management (SIEM)
- ✓ Threat intelligence
- ✓ Security orchestration
- ✓ Event logging and analytics
- ✓ Customized dashboards for compliance reporting

Email Security
- ✓ Machine learning, AI and analytics identify attacks
- ✓ Inspects URLs to credential-phishing sites and rewrites URLs
- ✓ Impersonation detection and in-house spam filtering
- ✓ Retroactive analysis and alerting

Security Awareness Training
- ✓ Access to ongoing psychological security training
- ✓ Phishing testing and reporting

Firewall & VPN
- ✓ Automated Detection & Prevention of Zero-Day exploits & malware
- ✓ Advanced analysis, machine learning & shared threat intelligence
- ✓ Credential Phishing Prevention & blocking new malicious URLs
- ✓ Selective Web Traffic Decryption and Safe Search Enforcement

Collector & Sensor
- ✓ Seamlessly combines several monitoring and detection systems
- ✓ Captures real-time threat detection and analysis
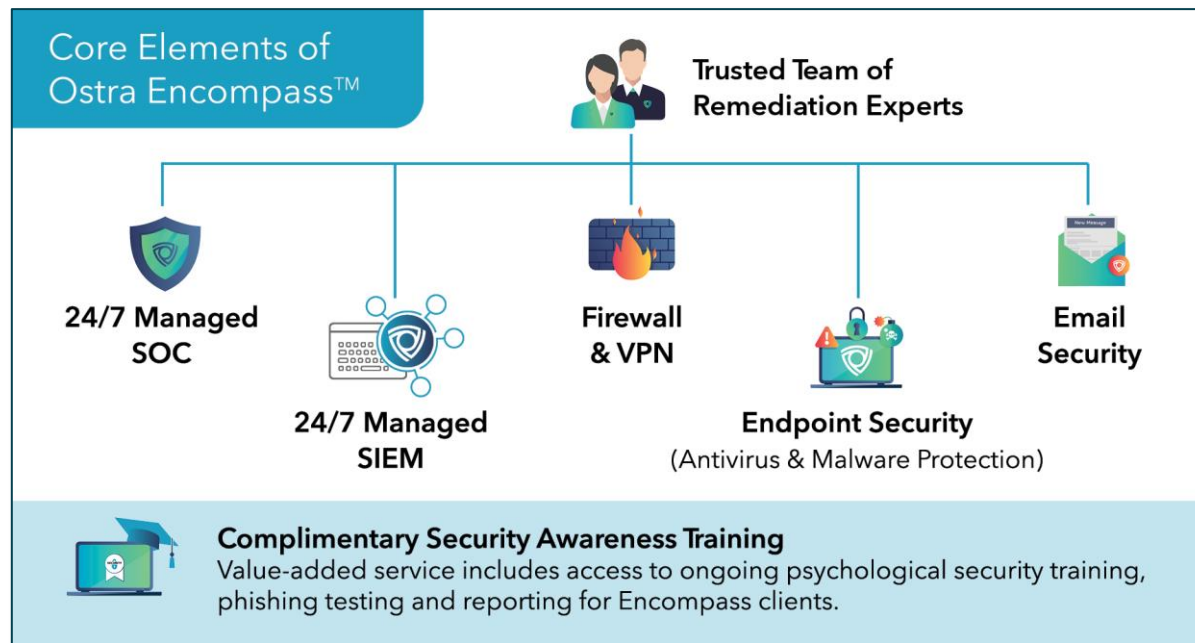- ✓ Creates a system for faster event reconstruction

Endpoint Security (Antivirus & Malware Protection)
- ✓ Single agent with 3 detection engines minimizes configuration
- ✓ Integrated workflow to analyze/respond to threats
- ✓ Fully integrated malware protection with antivirus defenses, machine learning, behavior analysis, indicators of compromise and endpoint visibility
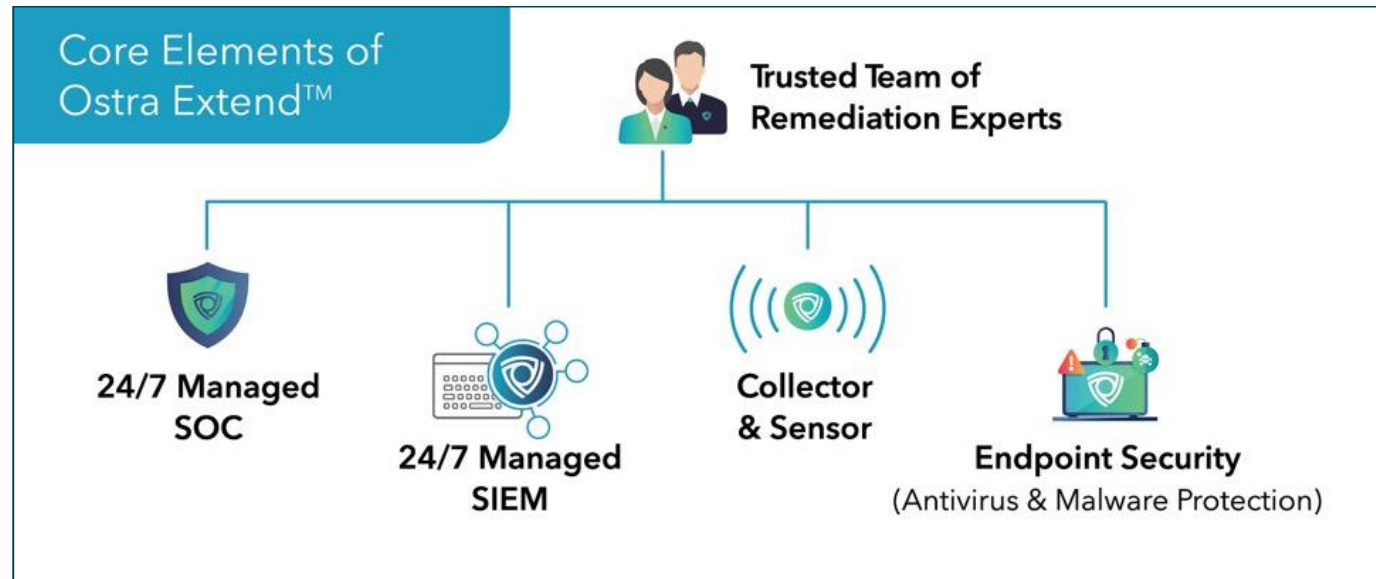
OSTRA

Ostra **Encompass**™

- We **Encompass** your company's needs as Your Trusted Cybersecurity Team with one holistic, easy to install, fully managed security operations solution across critical categories of cybersecurity

- **Ideal fit:** Clients looking for a holistic solution with no existing, retained components

Core Elements of Ostra Encompass™

Trusted Team of Remediation Experts

24/7 Managed SOC

24/7 Managed SIEM

Firewall & VPN

Endpoint Security
(Antivirus & Malware Protection)

Email Security

Complimentary Security Awareness Training
Value-added service includes access to ongoing psychological security training, phishing testing and reporting for Encompass clients.
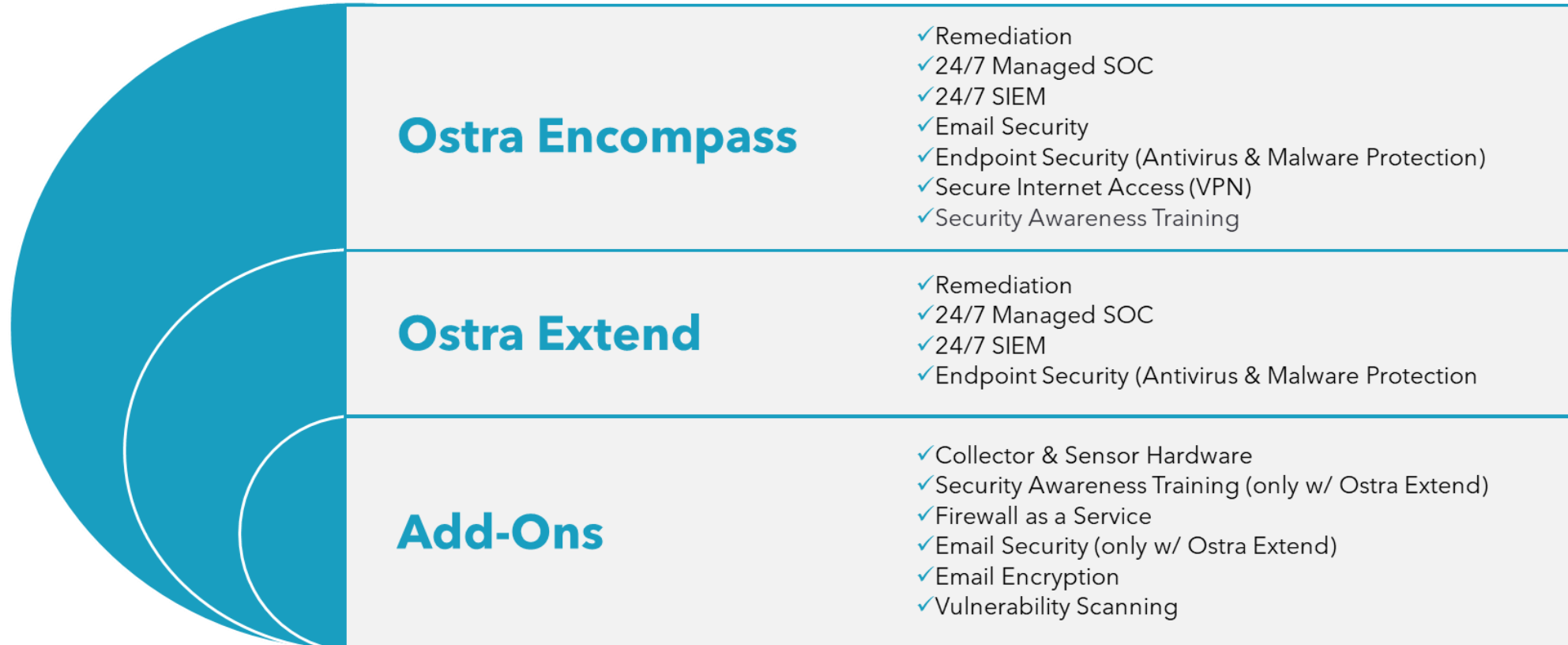
OSTRA

Ostra **Extend**™

- **Extend** your existing security capabilities with proactive 24/7 enterprise-wide monitoring and hands-on remediation of your clients' endpoints

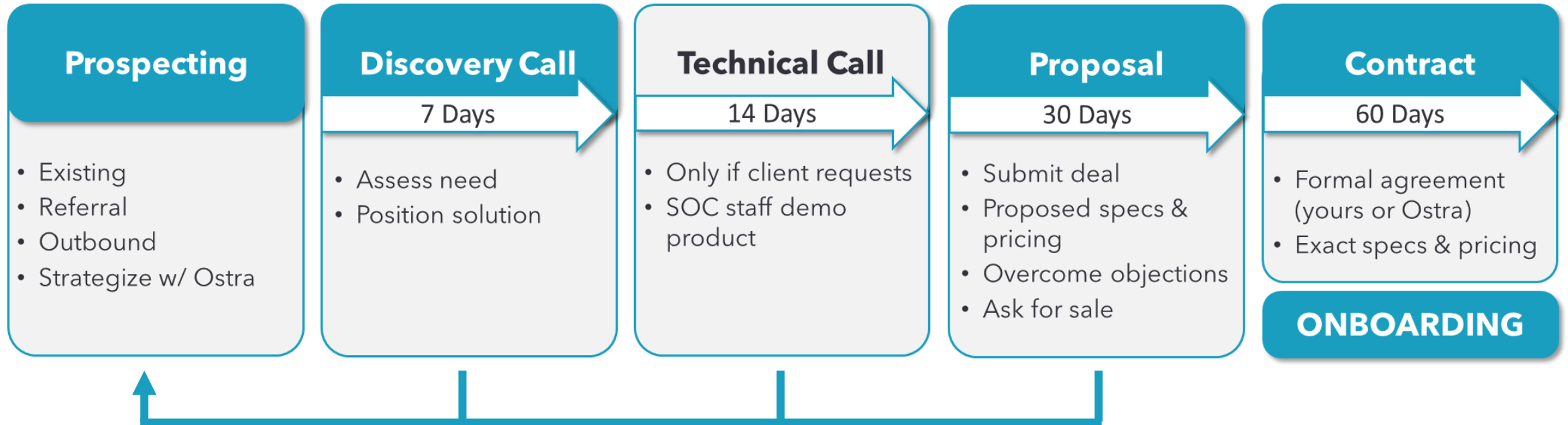- **Ideal fit:** Clients with existing infrastructure or security solution subscriptions

Core Elements of Ostra Extend™

Trusted Team of Remediation Experts

24/7 Managed SOC

24/7 Managed SIEM

Collector & Sensor

Endpoint Security (Antivirus & Malware Protection)

OSTRA

Ostra Pricing Model

Ostra Encompass

- ✓ Remediation
- ✓ 24/7 Managed SOC
- ✓ 24/7 SIEM
- ✓ Email Security
- ✓ Endpoint Security (Antivirus & Malware Protection)
- ✓ Secure Internet Access (VPN)
- ✓ Security Awareness Training

Ostra Extend

- ✓ Remediation
- ✓ 24/7 Managed SOC
- ✓ 24/7 SIEM
- ✓ Endpoint Security (Antivirus & Malware Protection

Add-Ons

- ✓ Collector & Sensor Hardware
- ✓ Security Awareness Training (only w/ Ostra Extend)
- ✓ Firewall as a Service
- ✓ Email Security (only w/ Ostra Extend)
- ✓ Email Encryption
- ✓ Vulnerability Scanning

Contact sales for detailed pricing

OSTRA

SALES CYCLE

Selling What We Do

The Sales Cycle

Prospecting	**Discovery Call**	**Technical Call**	**Proposal**	**Contract**
	7 Days →	14 Days →	30 Days →	60 Days →
• Existing • Referral • Outbound • Strategize w/ Ostra	• Assess need • Position solution	• Only if client requests • SOC staff demo product	• Submit deal • Proposed specs & pricing • Overcome objections • Ask for sale	• Formal agreement (yours or Ostra) • Exact specs & pricing

ONBOARDING

All "No" responses mean "Not Now" and return to cycle

OSTRA

Registering a Deal

1. Register the deal via Partner Portal
   - Who are you pitching?
   - How big is the deal?
   - What can we do to help?
   - When you expect to close?

2. Help us book a meeting with the client. Meetings must be attended by at least one stakeholder (CEO/CFO/COO/CTO, Director of IT/Ops, President, etc.)
   - Make a warm email intro; or
   - Book a meeting

Register a Deal

Client Contact First Name*

Client Contact Last Name*

Client Email*

Client Contact Job Title*

Client Company Name*

Client Company Website*

Partner Name*
Your company name

Estimated Close Date*

Deal Notes*

Submit

OSTRA

Referral Partner

Accounting Readiness

- **AP process** – Ostra owes the channel partner:

- For **Referral Partners**, where Ostra is paying "commission" to that partner: Partner will be set up as a vendor in Bill.com.

- Payment requires the following details:

    1. **A current W-9** form for the Partner as a payee which includes the correct payee's name, address and Tax ID number (EIN or SSN depending on entity type)

    2. **Current email address** for the payee

- Ostra will also require the following to make the actual payment:

    3. **Terms of the payment and amount** according to the contract between the channel partner and Ostra, along with approval to pay – with either the contract itself or portion of that, or an invoice from the channel partner if applicable.

- Partner will be paid the month after payment is received from the client

OSTRA

Reseller & Service Provider Partner: Billing

Invoicing Procedures

1.Monthly Invoicing:
- ➢ Services will be billed the 1st of each month for that month's services.

2.New Customers and Upselling Billing Start Timing:
- ➢ Billing will commence 21 days after reporting the deal to Ostra Cybersecurity Services.
- ➢ If day 21 falls before the 20th of the month, the first invoice will be prorated and issued on the 1st of the following month.
- ➢ If day 21 falls after the 20th of the month, the first invoice will be prorated and issued on the 1st of the second month

Scenario 1: Billing starts before the 20th
- ➢ Deal reported June 25th
- ➢ Billing starts July 16th (21 days)
- ➢ First invoice on August 1st (prorated for July 16-July 31 and August)

Scenario 2: Billing starts after the 20th
- ➢ Deal reported July 1st
- ➢ Billing starts July 22nd (21 days)
- ➢ First invoice on September 1st (prorated July 22-July 21 and August and September)

3.Invoice Calculation:
- ➢ The first invoice will be based on the initial quote provided
- ➢ Licenses exceeding order will true-up monthly

OSTRA

Reseller & Service Provider Partner: Billing

Cancelation Procedures

1.Full Company Offboarding
- ➢ To **cancel all company services**, contact your salesperson
- ➢ Billing will cease 60 days after Ostra Cybersecurity receives notification. Any Ostra Cybersecurity hardware must be returned within this period. Billing will continue until the hardware is returned.

2.Partial Services Offboarding:
- ➢ Contact your salesperson

OSTRA

STARTING THE CONVERSATION

How to Uncover Your Client's Needs

Who are we looking for?

Small and Mid-Sized Business (SMB) – Direct

- 50-500 employees
- Companies with compliance or cyber insurance needs ideal
  - Ex: Insurance agents, CPAs, Law Firms, Auto Dealerships, Financial Institutions, Education
- Companies with no existing Cybersecurity tools or services (Encompass)
- Companies with a few existing Cybersecurity tools or services (Extend)
- Companies that recently experienced a Cybersecurity incident

OSTRA

Qualifying Clients

Questions to ask your client:

- What is your company's current cybersecurity strategy?

- Has your business ever been affected by a cyber attack?

- Do you feel confident in your current cybersecurity strategy?

- Are you the person who makes decisions regarding your cybersecurity solutions?

- What is your recovery process in the event that a cyber attack occurs?

Keywords/phrases to listen for:

- No cybersecurity tools in place or they aren't sure what they have

- Just have antivirus/malware protection

- Not enough time/resources to manage

- Compliance concerns

- Anything that is or relates to MDR, XDR, EDR, SOCaaS, etc.

- Cybersecurity solutions are too expensive

OSTRA

Qualifying Clients

For Clients that may be a good fit...

Bring up Ostra Cybersecurity in that moment

- "It sounds like there's some opportunity to review cybersecurity solutions"

- "If you're open to it, I'd like to introduce you to our partners at Ostra Cybersecurity"

- "We partner with Ostra because they provide an all-encompassing cyber solution that businesses of all sizes typically afford"

GETTING TO YES

Simplifying Selling

Common Objections

This service is more than we have a budget for.

Why should I buy it?

- Educate client on vulnerability and potential threat impact
- Discuss cost to staff and purchase tools internally
- Discuss how their organization is no longer helpless against threats
- Compare our service to their current tools
- Offer to conduct our assessment and compare findings via checklist

Why should I pay a premium for this service?

- Communicate paying for the value that Ostra delivers, vs. the cost to deliver internally within their organization
- Ostra provides an elite level of service that typically only Fortune 500 companies can afford

OSTRA

Common Objections

Why do we need that level of protection and support?

- How much do they value their data privacy, brand, & client relationship?
- What impact would a data breach have on their company?

Why pay a premium for this service?

- Avoidance of malware threats
- Ransomware incidents typically last 6 days, which is costly
- We help eliminate that risk and its financial impact

OSTRA

Common Objections

Why should we buy from Ostra?

- No other service provided offers this level of protection for SMBs
- What data security risks are they most concerned about?
- We provide the peace of mind to focus on their business
- We protect clients from threats others cannot
- Do they have any compliance requirements?

We believe our services should be seriously considered if they answer "no" to the following

- Is your cybersecurity robust enough?
- Is your business protected from new and emerging threats?
- Are you prepared to handle all these risks and issues on your own?

OSTRA

RESOURCES

Partner Resources

- **Ostra Partner Portal**: **partners.ostra.net**

  - Register deals

  - Sales & Marketing resources

  - Need a login? Email **partnersuccess@ostra.net**

- Browse resources and news on **ostra.net/blog**

- Follow **Ostra on LinkedIn** for latest tips and content

OSTRA

Questions

THANK YOU!

www.ostra.net