

Elevator Pitch

- Ostra's real-time, best-in-class, comprehensive solution provides layered protection to your thriving business.
- Don't waste time piecing your solution together.
- Ensure all your cybersecurity and compliance gaps are closed with Ostra.

Key Features/Benefits

24/7 Managed SOC & SIEM



- 24/7 monitoring via Security Operations Center (SOC)
- Activity insight via Security Information and Event Management (SIEM) technology
- Threat intelligence
- Security orchestration
- Customized dashboards for compliance reporting
- Event logging and analytics

Firewall & VPN



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

Cloud Security (CASB)

Elite Add-On



- Discover SaaS, IaaS and web use details and assess risk
- Secure sanctioned cloud services such as Office 365, Box and AWS
- Safe enablement of unsanctioned, business-led cloud services
- Govern cloud and web use for on-premises, mobile and remote users
- Data loss prevention across cloud platforms

Email Threat Prevention (ETP)



- Machine learning, AI and analytics identify attacks that evade signature and policy-based defenses
- Inspects URLs for links to credential-phishing sites and rewrites URLs
- Impersonation detection and in-house spam filtering
- Retroactive analysis and alerting

Endpoint Security (Antivirus & Malware Protection)



- Single agent with three detection engines to minimize configuration and maximize detection/blocking
- Integrated workflow to analyze/respond to threats within Endpoint Security
- Fully integrated malware protection with antivirus (AV) defenses, machine learning, behavior analysis, indicators of compromise (IOCs) and endpoint visibility
- Triage Summary and Audit Viewer for exhaustive inspection/analysis of threats

Mobile Device Management & Security (MDM)

Elite Add-On



- Secure data across all mobile devices (laptops/tablets, phones, IoT and more)
- Seamless integration with existing architecture and easy installation
- Robust policy configuration and enforcement including application, content and access management
- Threat detection and remediation, audits and reports

Why say "YES" to simplified cybersecurity?

- Ostra serves as an extension of your current IT/Security team
- Customizable pricing discounts that grow as your user needs expand
- Eliminate your client's security gaps and vulnerabilities with our Fortune-100 solution
- Solutions adhere to your Security Compliance needs (HIPPA, CMMC, etc.)

Opportunity & Qualification Talking Points

Protection/Solutions	Question(s)	Answer(s)
Cyberattacks	Has this happened to you? What happened? How long did it take?	Ostra provides a comprehensive, layered solution that typically costs small to medium size businesses 3x more to piece together on their own. Each layer of Ostra's solution provides protection against known and unknown threats.
Compliance gaps	Are you bound by regulations? What cost is involved if you fail to meet these?	We work with industry best-in-class technology providers that will aid in closing compliance and regulatory gaps that exist within your business.
Existing solution	How are you currently managing cybersecurity? SOC & SIEM? Cost & time involved?	Often, these solutions are pieced together—causing a fragmented, time-consuming monitoring process. With Ostra, you simply set it and forget it.
Assessment gaps	Has a security scan shown your vulnerabilities? Have you researched solutions and costs for out-of-the-box services?	Ostra's best-in-class comprehensive solution closes the gaps that were exposed in your initial external/internal scan at a much more affordable rate.

Overcoming Objections

1 This service is more than we have a budget for. Why should I buy it?

- Educate them about the vulnerability that the client is exposed to, and its potential impact. Can they protect themselves from unknown threats?
- Discuss what it would cost to staff and purchase these tools internally. Do they understand the cost of hiring the skill set needed to support and effectively deploy these tools on a 24/7 basis?
- Discuss how their organization is no longer helpless against these threats. Can they afford to buy these tools and layer them together themselves, or would they rather have Ostra do it for them on an affordable monthly subscription basis?
- Have a conversation to compare our service to the tools they are using, and the associated value. Offer to conduct our free assessment and then compare the findings to our service via the checklist.

2 Why pay a premium for this service?

- You are paying for the value that Ostra delivers, vs. the cost to be able to deliver internally within your organization.
- An elite level of service that typically only Fortune 500 companies can afford.

3 Why do we need that level of protection and support?

- How much do you value your data privacy, brand, and client relationships?
- What impact would a data breach have on your company?

4 What does one get for that premium?

- Avoidance of malware threats
- Ransomware incidents typically lasts 6 days, which is costly to your business.
- We help eliminate that risk and its financial impact.

5 Why should we buy from Ostra?

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

6 If they answer NO to any of these questions, then we believe our service should be seriously considered:

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

Battle Card



COMPANY

1. Who is Ostra?

- Our mission is to simplify cybersecurity for small to medium businesses.
- We provide a comprehensive, layered protection that our customers typically do not have the resources to provide for themselves.

2. Why Ostra?

- We protect customers from threats that others cannot prevent.
- We stop these threats before trouble occurs.
- Ransomware incidents can typically last 6 days and cost tens of thousands of dollars.
- We help eliminate that risk and financial impact.

3. Why Choose Now?

- No other service provider has the same value, customer focus, and tools as Ostra.
- World-class protection delivered at a flexible and affordable monthly subscription.

4. Why Not Ostra?

- Without Ostra, your organization remains vulnerable to known and unknown threats. Just compare your existing security tools to what Ostra offers.
- What are the risks based on the difference in capabilities?
- What are the ramifications of those risks?

PRICING

1. Who is the typical buyer for this service?

- Business decision-makers, typically with IT's buy-in.

2. Can we adjust users' totals monthly?

- Yes, Ostra's billing reflects monthly reported user totals

3. Does our contract renew automatically?

- Yes, unless clients opt out 30 days prior to renewal

SERVICE VALUE

1. Why Ostra vs. Typical Tools and Services?

- Best in class tools
- Layered protection
- Real-time updates

2. How does Ostra's service work?

- Easy set up and behind-the-scenes monitoring
- No ongoing user intervention
- Resources to manage your environment 24/7

3. Why don't I notice anything different?

- Our service has no impact on system performance.
- Updates are automatic so users do not need to manage this process.
- Our SOC/SIEM team manages and deals with threats, so users do not have to.

4. Can Ostra read my emails?

- Ostra personnel do not have access to read clients' email content without express consent.
- Ostra has safeguards to prevent this from happening.

5. What compliance requirements does Ostra meet?

- Ostra can help your organization comply with critical certification and regulatory requirements for data privacy/security. We specialize in securing data for clients in financial, technology, healthcare, federal, legal and other industries.

6. How long does it take to set up the service?

- 5 minutes per user or for groups of users

7. Can we manage updates and patches ourselves?

- This is a core part of the value of Ostra's service. As such, there is no need for clients to worry about related updates.
- Ostra tools can typically be updated multiple times daily. Users do not need to be distracted by this update frequency.

8. How does Ostra provide global surveillance?

- Ostra connects into our partner networks and sees threats in real-time.
- Ostra receives real-time updates at the same time as the largest global clients. These updates are immediately passed on to Ostra's clients, so they remain protected.