INFRASTRUCTURE

OVERALL RISK LEVEL
HIGH

Thank you for completing the cybersecurity maturity assessment. The assessment is based off industry frameworks including the NIST Cybersecurity Framework and provides a temperature check on critical areas of your cybersecurity program. This executive report will help you identify your cybersecurity strengths & weaknesses, provide valuable insights to inform your strategy and deliver product recommendations to mitigate your specific cyber risks.

SUMMARY OF YOUR RESULTS

LOW RISK   HIGH RISK

Edge Devices and Remote Access

Network Security

Endpoint Protection / Endpoint Detection and Response (EPP/EDR)

Backups

Email Infrastructure

Vulnerability Scanning

Penetration Testing

Multi-factor Authentication (MFA)

Logs / SIEM

24/7 Monitoring

Risk Assessment

Security Policies

Incident Response Planning

Security Awareness Training

Information Security Program

Edge Devices and Remote Access
Device and remote software that provide an entry point into enterprise core networks.

HIGH

YOUR RESPONSES

LOW RISK

HIGH RISK

Are firewalls securely implemented and configured to protect the company's infrastructure?

Are all firewall logs sent to a SIEM/ Log Management Platform?

Does your company use a VPN and/or a Zero Trust (ZTNA) solution?

GENERAL RECOMMENDATIONS

- ⓘ Implement a pair of redundant firewalls to secure your network and tune your firewall rules to only allow business approved services.

- ⓘ Forward all firewall logs to a central log server/service or a Security Information and Event Management (SIEM) system/service for security investigations and/or troubleshooting.

- ⓘ Enable multi-factor authentication for all remote access logins.

SERVICE RECOMMENDATIONS

📄 **MDR for Log**

eSentire MDR for Log provides you with multi-signal visibility across your network assets, endpoints, applications and cloud services enabling data correlation and deep investigation regardless if your data is in the cloud, on premises or in between. We support you with a team of researchers who power MDR for Log with hundreds of proprietary runbooks, and cutting edge detections of threat actor tactics, techniques and procedures (TTPs). Our best-of-breed MDR approach means we partner with the leading technology platforms in data analytics, log management, and cloud SIEM.

LEARN MORE ➝

Network Security
Protects the enterprise network and data from breaches, intrusions and other threats.

HIGH

YOUR RESPONSES

LOW RISK

HIGH RISK

Is North/South network traffic monitored 24/7?

Is East/West network traffic monitored 24/7?

GENERAL RECOMMENDATIONS

- ⓘ Monitor north/south network traffic to detect/block unauthorized access/data loss.

- ⓘ Monitor east/west network traffic in order to detect/block lateral movement.

SERVICE RECOMMENDATIONS

MDR for Network

eSentire MDR for Network monitors your network traffic around-the-clock using proprietary deep packet inspection and advanced behavioral analytics. We automatically disrupt malicious traffic on your behalf and our 24/7 SOC Cyber Analysts work as an extension of your team to determine root cause and remediation support so threat actors cannot complete attacks to your network.
LEARN MORE →

MDR for Endpoint

eSentire MDR for Endpoint protects your assets 24/7 no matter where your users or data reside. We combine elite threat hunting with endpoint threat prevention and endpoint detection and response (EDR) capabilities. Our 24/7 SOC Cyber Analysts rapidly investigate and isolate compromised endpoints on your behalf, preventing lateral spread and business disruption. We work alongside you to determine root cause, remediate with corrective actions and ensure you are protected against business disruption.
LEARN MORE →

Endpoint Protection / Endpoint Detection and Response (EPP/EDR)

EPP is the standard for endpoint protection. EDR is included or added in an EPP to enable investigations & containment.

HIGH

YOUR RESPONSES   LOW RISK   HIGH RISK

Does your Endpoint Protection solution also provide Endpoint Detection and Response (EDR)?

Do you have a Detection and Response process that ensures someone investigates, assesses, and documents each alert?

GENERAL RECOMMENDATIONS

- ⓘ Implement an anti-malware solution that provides endpoint detection and response (EDR) to gather telemetry from endpoints and aid in security investigations & troubleshooting.

- ⓘ Create a detection and response process to ensure each alert is reviewed and investigated.

SERVICE RECOMMENDATIONS

🖥 **MDR for Endpoint**

eSentire MDR for Endpoint protects your assets 24/7 no matter where your users or data reside. We combine elite threat hunting with endpoint threat prevention and endpoint detection and response capabilities. Our 24/7 SOC Cyber Analysts rapidly investigate and isolate compromised endpoints on your behalf, preventing lateral spread and business disruption. We work alongside you to determine root cause, remediate with corrective actions and ensure you are protected against business disruption. Our best-of-breed MDR approach means we partner with leaders in endpoint protection (EPP) and endpoint detection and response (EDR) to deliver eSentire MDR for Endpoint.

LEARN MORE →

Backups
A copy of data taken and stored elsewhere so that it may be used to restore the original if the data is lost.

HIGH

YOUR RESPONSES	LOW RISK	HIGH RISK

Do you have offline backups?

Do you routinely check the viability of the backups you have?

Are your backups encrypted?

GENERAL RECOMMENDATIONS

- ⓘ Create offline backups that are immutable/air gapped to protect against ransomware attacks.

- ⓘ Create a data restoration process to validate that your backups are working as expected. This should be a full recovery test and not a sample from a user restore request.

- ⓘ Encrypt your data backup files to prevent authorized access.

SERVICE RECOMMENDATIONS

🔓 **CISO and Advisory Services**

eSentire works directly with you to assess your cybersecurity program maturity against your industry peers and measures your ability to address the latest cyber threats. We help you align your cybersecurity strategy and business objectives to build a cyber roadmap that reduces your cyber risk. We will help create and structure your security policies to adhere to important compliance requirements.

LEARN MORE ➝

Email Infrastructure
Architecture that works towards delivery of transactional emails to and from the enterprise.

HIGH

YOUR RESPONSES   LOW RISK   HIGH RISK

Do you use any form of phishing protection (enterprise email security, sandboxing, email tagging, etc.)?

GENERAL RECOMMENDATIONS

ⓘ Implement an email security solution to prevent phishing attacks that could lead to loss of credentials, data loss or unauthorized access to your environment.

SERVICE RECOMMENDATIONS

MDR for Microsoft

eSentire MDR for Microsoft includes Microsoft Defender XDR which provides robust email threat detection, investigation, and complete response on a 24/7 basis. Our dedicated security experts from eSentire's global Security Operations Centers (SOC) leverage Microsoft Defender XDR's highly integrated email security solution to detect and hunt both common and sophisticated email threats before they disrupt your business.

LEARN MORE ➞

Vulnerability Scanning
Ensures critical internal and external vulerabilites are identified and remediated.

HIGH

YOUR RESPONSES   LOW RISK   HIGH RISK

Do you perform internal vulnerability scans monthly?

Do you perform external vulnerability scans weekly?

GENERAL RECOMMENDATIONS

ⓘ   Conduct internal vulnerability scans at least monthly.

ⓘ   Conduct external vulnerability scans at least weekly.

SERVICE RECOMMENDATIONS

🔓 **Managed Vulnerability Services**

eSentire's Managed Vulnerability Service accurately identifies vulnerabilities across traditional and dynamic IT assets such as mobile devices, OT, IoT, virtual machines and cloud.

LEARN MORE →

Penetration Testing

Simulates external and/or internal attackers to test current defense measures & identify weaknesses in your security posture.

HIGH

YOUR RESPONSES   LOW RISK   HIGH RISK

Do you perfom an annual internal and external penetration test?

GENERAL RECOMMENDATIONS

ⓘ Conduct annual penetration testing to test your current defense measures and identify weaknesses in your external or internal security posture.

SERVICE RECOMMENDATIONS

💻 **Continuous Threat Exposure Management Services**

With eSentire Continuous Threat Exposure Management Services, our team helps you identify blind spots, build a strategy for mitigating risk and operationalizes capabilities to predict and prevent known threats. Our Continuous Threat Exposure Management Services include Penetration Testing and Virtual CISO services to support in building your security assessment and testing strategy.

LEARN MORE →

Multi-factor Authentication (MFA)
Authentication that requires the user to provide two or more verification factors to gain access.

HIGH

YOUR RESPONSES

LOW RISK　　　　**HIGH RISK**

Is multi-factor authentication (MFA) enabled for all critical busniess functions (i.e. remote access, admin access, email, etc.)?

GENERAL RECOMMENDATIONS

ⓘ　Enable multi-factor authentication for all remote access.

SERVICE RECOMMENDATIONS

🔓 **CISO and Advisory Services**

eSentire works directly with you to assess your cybersecurity program maturity against your industry peers and measures your ability to address the latest cyber threats. We help you align your cybersecurity strategy and business objectives to build a cyber roadmap that reduces your cyber risk. We will help create and structure your security policies to adhere to important compliance requirements.

LEARN MORE →

Logs / SIEM
Tracking and storing data to ensure system availability and alerting issues by analyzing metrics.

HIGH

YOUR RESPONSES

LOW RISK   HIGH RISK

Do you centrally collect and store logs via a SIEM or Log Management platform?

Do you leverage logs for threat detection (alerting, correlation, IoC sweeps, threat hunting, etc.)?

GENERAL RECOMMENDATIONS

ⓘ Forward all logs to a central log server/service or Security Information and Event Management (SIEM) system/service.

ⓘ Correlate logs to identify any patterns and sequences to identify unusual behavior.

SERVICE RECOMMENDATIONS

MDR for Log

eSentire MDR for Log provides you with multi-signal visibility across your network assets, endpoints, applications and cloud services enabling data correlation and deep investigation regardless if your data is in the cloud, on premises or in between. We support you with a team of researchers who power MDR for Log with hundreds of proprietary runbooks, and cutting edge detections of threat actor tactics, techniques and procedures (TTPs). Our best-of-breed MDR approach means we partner with the leading technology platforms in data analytics, log management, and cloud SIEM.

LEARN MORE →

24/7 Monitoring
Always on monitoring critical for a security program as attackers don't have business operating hours.

HIGH

YOUR RESPONSES   LOW RISK   HIGH RISK

Is 24/7 cybersecurity monitoring in place?

GENERAL RECOMMENDATIONS

Configure security alerts to be sent to an on-call person to be able to investigate and respond within a timely manner. Alternatively, consider using a managed security service provider to monitor your environment 24/7.

SERVICE RECOMMENDATIONS

Multi-Signal MDR
Our Managed Detection and Response service combines cutting-edge XDR technology, multi-signal threat intelligence and 24/7 SOC Cyber Analysts supported by Elite Threat Hunters to help you build a world-class security operation. Our threat protection is unparalleled - we see and stop attacks other providers and technologies miss, delivering the world's most complete response capability.
LEARN MORE ➟

Risk Assessment
Allows organizations with constrained resources to assess potential third-party and supply chain risks.

HIGH

YOUR RESPONSES   LOW RISK   HIGH RISK

Do you conduct annual third-party risk assessments?

GENERAL RECOMMENDATIONS

ⓘ Conduct a third-party risk assessment to get an unbiased report on the current security posture of your business.

SERVICE RECOMMENDATIONS

🔒 **CISO and Advisory Services**

eSentire works directly with you to assess your cybersecurity program maturity against your industry peers and measures your ability to address the latest cyber threats. We help you align your cybersecurity strategy and business objectives to build a cyber roadmap that reduces your cyber risk. We will help create and structure your security policies to adhere to important compliance requirements.

LEARN MORE ➝

Security Policies

Establishes rules and processes for workforce members, creating a standard around the acceptable use of the organization's IT.

HIGH

YOUR RESPONSES   LOW RISK   HIGH RISK

Do you have a formal Information Security Policy?

Do policies cover regulatory and legal requirements?

Are policies reviewed and updated annually?

GENERAL RECOMMENDATIONS

ⓘ Create an information security policy with supporting procedures and standards.

ⓘ Update your information security policy to cover your business, legal and regulatory requirements.

ⓘ Review and update all of your security policies at least annually.

SERVICE RECOMMENDATIONS

🔓 **CISO and Advisory Services**

eSentire works directly with you to assess your cybersecurity program maturity against your industry peers and measures your ability to address the latest cyber threats. We help you align your cybersecurity strategy and business objectives to build a cyber roadmap that reduces your cyber risk. We will help create and structure your security policies to adhere to important compliance requirements.

LEARN MORE →

Incident Response Planning
Proactive measure of researching potential cyber risks and understanding how to mitigate & remove them in a certain timeframe.

HIGH

YOUR RESPONSES   LOW RISK   HIGH RISK

Do you have a documented incident response plan?

Is your incident response plan tested annually?

GENERAL RECOMMENDATIONS

- Create and document a formal incident response policy and plan.

- Test your incident response plan at least annually using table top exercises.

SERVICE RECOMMENDATIONS

Digital Forensics and Incident Response

Our **unlimited** incident response ensures you can recover from the most advanced attacks. eSentire Digital Forensics and Incident Response services are available as IR Readiness, Incident Response Retainer or Emergency Incident Response Services.

LEARN MORE →

Security Awareness Training

Mitigate end user risk by training employees to be aware of threats like business email compromise (BEC) and phishing emails.

HIGH

YOUR RESPONSES   LOW RISK   HIGH RISK

Are all users subjected to annual security awareness training?

Do you conduct phishing testing of your users on a quarterly basis?

GENERAL RECOMMENDATIONS

- ℹ️ Ensure all users receive security awareness training at least annually.

- ℹ️ Conduct phishing tests on a regular schedule – at minimum on a quarterly basis.

SERVICE RECOMMENDATIONS

Managed Phishing and Security Awareness Training

eSentire's Managed Phishing and Security Awareness Training helps you identify risk, and test user resiliency, while you enable behavioral change and generate measurable results across the business.

LEARN MORE ➞

Information Security Program
Practices your business implements to protect processes, data, and IT assets.

HIGH

YOUR RESPONSES   LOW RISK   HIGH RISK

Do you have someone internally responsible for your information security program (i.e. CIO, CISO, etc.)?

Are the company's legal and regulatory requirements documented?

Do you have an existing cyber insurance policy?

GENERAL RECOMMENDATIONS

ⓘ   Assign an internal resource to be responsible for cybersecurity. Alternativity, you can hire a security consultant to assist if there are no internal resources.

ⓘ   Document your organization's legal and regulatory requirements as they pertain to cybersecurity and privacy.

ⓘ   Determine the amount of cybersecurity coverage you will require and secure a cyber insurance policy to protect your organization.

SERVICE RECOMMENDATIONS

🔓 **CISO and Advisory Services**
eSentire works directly with you to assess your cybersecurity program maturity against your industry peers and measures your ability to address the latest cyber threats. We help you align your cybersecurity strategy and business objectives to build a cyber roadmap that reduces your cyber risk. We will help create and structure your security policies to adhere to important compliance requirements.
LEARN MORE ⇀

The Importance of Mitigating Your Cyber Risk

In-house IT teams may not have the cybersecurity expertise or the time it takes to monitor cybersecurity threats 24/7. Day to day, the IT team is often focused on supporting the business and projects that drive revenue.

Cybersecurity is everyone's business—including C-level executives, managers, administrative assistants, and even part-time office staff. Unfortunately, any employee can be a potential cybersecurity attack vector and adversaries have more ways than ever before to bypass perimeter defenses. You can put all the right traditional cybersecurity measures in place, but all it takes is one employee clicking on a phishing email.

Understanding your organization's cybersecurity maturity, knowing where there may be gaps, and addressing those issues is imperative. Taking proactive steps to mitigate cybersecurity risk can mean the difference between a data breach or business as usual.

Ready to Review Your Cybersecurity Program?

We're here to help! As a complimentary follow up, consider booking a meeting with our expert solution architects to review your results of your cybersecurity assessment.

Book a Meeting

Product Recommendations

Based on the results of your cybersecurity assessment and areas of greatest risk, we recommend learning more about these eSentire services to reduce your cyber risk and put your business ahead of disruption.

MDR for Log   `HIGH PRIORITY`
LEARN MORE →

MDR for Network   `HIGH PRIORITY`
LEARN MORE →

MDR for Endpoint   `HIGH PRIORITY`
LEARN MORE →

CISO and Advisory Services   `HIGH PRIORITY`
LEARN MORE →

MDR for Microsoft   `HIGH PRIORITY`
LEARN MORE →

Managed Vulnerability Services   `HIGH PRIORITY`
LEARN MORE →

Continuous Threat Exposure Management Services   `HIGH PRIORITY`
LEARN MORE →

Multi-Signal MDR   `HIGH PRIORITY`
LEARN MORE →

Digital Forensics and Incident Response   `HIGH PRIORITY`
LEARN MORE →

Managed Phishing and Security Awareness Training   `HIGH PRIORITY`
LEARN MORE →