CITY OF MADISON HEIGHTS

CITY HALL - EXECUTIVE CONFERENCE ROOM, 300 W. 13 MILE RD.

INFORMATION TECHNOLOGY ADVISORY COMMITTEE MEETING AGENDA

APRIL 22, 2024 AT 5:30 PM

CALL TO ORDER

ROLL CALL

ADDITIONS/DELETIONS

APPROVAL OF MINUTES

1. ITAC Meeting Minutes of October 23, 2023

MEETING OPEN TO THE PUBLIC

REPORTS

2. Ty Dolan - Skynet Innovations Quarterly Business Review
3. Discussion on Disaster Recovery Plan
4. Discussion on Cyber Security Platform

UNFINISHED BUSINESS

NEW BUSINESS

ADJOURNMENT

NOTICE: Persons with disabilities needing accommodations for effective participation through electronic means in this meeting should contact the City Clerk at (248) 583-0826 or by email: clerks@madison-heights.org at least two working days in advance of the meeting. An attempt will be made to make reasonable accommodations.

Information Technology Advisory Committee Meeting
Madison Heights, Michigan
October 23, 2023

A Information Technology Advisory Committee Meeting was held on Monday, October 23, 2023 at 6:00 PM at City Hall - Executive Conference Room, 300 W. 13 Mile Rd.

PRESENT
Council Representative Mark Bliss
Brian Davis
Dale Gardner
Curtis J. Kogelman
City Manager Melissa Marsh
Zach Palmer
Deputy City Manager/City Clerk Cheryl Rottmann
Paul Timmins
Scott Tuller

ABSENT
Alternate Robert Didur
Council Alternate Sean Fleming

OTHERS PRESENT
Skynet Project Engineer Tim Bank
Skynet On-site Lead Engineer Colin Wynn

1. ITAC Meeting Minutes of May 8, 2023

Motion to approve the ITAC meeting minutes of May 8, 2023, as printed.

Motion made by Marsh, Seconded by Timmins.

Voting Yea: Council Representative Bliss, Davis, Gardner, Kogelman, Marsh, Palmer, Rottmann, Timmins, Tuller

Motion carried.

MEETING OPEN TO THE PUBLIC:

There were no members of the public wishing to speak.

2. Zach Palmer - Skynet Innovations Quarterly Business Review

Zach Palmer presented the Quarterly Business Report from Skynet Innovations. Items that were discussed based on the report:

Fire Station 2 Renovations

Colin Wynn noted that there was unforeseen damage to the fiber causing a change order to be made on the project.

Disaster Recovery Plan

It was the consensus to prepare a draft Disaster Recovery Plan, following the FBI template, prior to the next ITAC meeting.

Cybersecurity Platform

It was the consensus to review and document recommendations on antivirus products as well as from SIEM/SOC.

Motion to provide an update on the city's cybersecurity platform by the next ITAC meeting.

Motion made by Council Representative Bliss, Seconded by Timmins.

Voting Yea: Council Representative Bliss, Davis, Gardner, Kogelman, Marsh, Palmer, Rottmann, Timmins, Tuller

Motion carried.

Service Level Agreement

Councilman Bliss requested an update report from Skynet for the previous six-month period.

3. Discussion on Telephone Outages

Colin Wynn updated ITAC on phone outage issues that the City has experienced. He stated that the issues have been attributed to an old VoIP router and a new one has been included in the CIP for this upcoming budget cycle. They are also looking at switching from WOW and moving to ATT which is what the library uses and using ATT as a backup. We currently don't pay for bursting with WOW.

Discussion was held on the possibility of also looking into a cloud-based replacement program for the telephones.

Motion to study firewall traffic rate limit changes for VoIP traffic prioritization and report back in ninety (90) days.

Motion made by Timmins, Seconded by Council Representative Bliss.

Voting Yea: Council Representative Bliss, Davis, Gardner, Kogelman, Marsh, Palmer, Rottmann, Timmins, Tuller

4. City Council Computer Policy

City Manager Marsh stated that since the city has transitioned from the network to cloud/internet-based programs for Council members to access agendas and information, there really is no need to provide access to the city's network and provide a city owned device. Ms. Marsh asked ITAC for a recommendation on how to proceed based on these changes with a computer device policy.

Motion to support development of a policy to provide a stipend to newly elected members of Council for purchase of their own computer device to access Council agendas and information.

Motion made by Tuller, Seconded by Davis.

Voting Yea: Council Representative Bliss, Davis, Gardner, Kogelman, Marsh, Palmer, Rottmann, Timmins, Tuller

Motion carried.

ADJOURNMENT

Having no further business, Chair Kogelman adjourned the meeting at 6:51 p.m.

Technology Business Review

Date: April 16th, 2024

Client Name:	Melissa Marsh City Manager City of Madison Heights 300 West 13 Mile Road, Madison Heights, MI, 48071	Account Manager:	Ty Dolin Skynet Innovations

Risk and Exposure Review

Hardware

Item	Summary	Score
Asset Inventory	All equipment is documented in asset management database	100
Internet Firewalls	Replaced firewalls in 2022/2023, watchguard firewalls. Support renewal date: 1/1/2026	100
Power Management	Project needed for visibility internal battery replacement, pending discovery. Power audit in 2022 didn't reveal any issues for backup power currently. UPS list that needs to be replaced. Budgeting 2024/2025 for replacement	80
Local Host Servers	Equipment is in good working order. Servers are monitored and patched on a regular schedule. SAN and host servers budgeted for in 2023/2024, will likely need rollover to 2024/2025 for completion.	80
Network Switching	Budgeted for 2023/2024, 13 switches to be replaced. Approved and In Progress	75
Phone - VoIP	The current phone system is viable for a few more years. Scheduled for FY 2024/2025 (Budgeted $250,000) covers the phone system replacement. Likely will need to go out to bid.	80
Workstations	Yearly computer replacement based on budget. Workstation budget for 2023/2024 being utilized. ~20 devices have been replaced so far 2023/2024.	100

Business Applications / Software

Item	Summary	Score
Email Cloud Host	Microsoft hosts city email and is a viable service for the foreseeable future. License renewal date: 7/1/2024	100
Operating Systems	Server operating systems are up to date and patched on a regular schedule. All PC's either have windows 11 or are able to upgrade. Windows 10 supported to end of 2025	100
Monitoring and Alerting	Datto & Blumira sends automated alerts for hardware downtime and severity status. No action needed, provided by Skynet	100

Document Imaging	Laserfiche being utilized by clerk	100

Security

Item	Summary	Score
Anti-Malware	Webroot is installed and updated daily. License renewal date: Monthly subscription budgeted for	100
Spam Filter	Barracuda filter and encryption installed and updated daily. License renewal date: Monthly subscription budgeted for	100
Directory Services	Microsoft Active Directory with leveraging organizational units and group policies.	100
Intrusion Detection and Prevention	Firewalls are up to date and monitored for basic uptime. Support license renewal date: 9/7/2027	100
VPN – Remote Access	Watchguard Firebox installed and utilized. Support license renewal date: 1/1/2025	100

Slick Sheets: Blackpoint Cyber

Continuity

Item	Summary	Score
Backup to Cloud	Wasabi implemented and utilized; Wasabi is monthly subscription.	100
Backup and Recovery Software	VEEAM installed and updated. License renewal on 5/23/2024 is budgeted for.	100
Disaster Recovery Plan	Work in progress, Initial draft being provided to ITAC 4/22	75
Redundant Internet	2 separate circuits don't currently interact, part of next network redesign project. Scheduling downtown to ensure function of circuit (Cutover)	80
Backup Power – City Hall	Server room is on generator power	100

2024 Technology Plan

The following lists technology maintenance items that are scheduled on an annual basis. Additional monthly maintenance can be found in the AutoTask management portal.

First Quarter

Renew Madison-heights.org email SSL – Budgeted for $200 (completed)
DUO MFA Renewal – Budgeted for $1,728 (completed)
Computer Replacements – Utilizing remaining budgeted for 2023/2024 (Continued)
Wireless Network Upgrade – Budgeted for $61,000, funds requested $26,640.00 (Approved, In Progress)
Network Equipment Updates – Budgeted for $122,872 (Approved, In Progress)

Second Quarter

Network Equipment Updates - *Continued*
Storage Area Network and Host Servers – *Continued*
Wireless Network Upgrade – *Continued*

Computer Replacements – Utilizing remaining budgeted for 2023/2024 – *Continued*
DUO FOB's 113x $29.70 = $3,356.10 (Approved and In procurement process)
Storage Area Network and Host Servers – Budgeted for $96,000 (requoting due to VMWARE licensing model changing)
Mobile Device Management – Budgeted for $10,000 (TBD, different routes to choose from)
VEEAM Backup Support License Renewal – Budgeted for $4,631 (Budgeted)

Third Quarter – Start of Fy 24/25 (Projected)
MS 365 Licenses Renewal – Budgeted for $43,879 (Budgeted)
Computer Replacements – Budgeted for $47,000 (in progress, ongoing yearly project)
Azure / ENTRA P1 Licenses add-on to MS365 G3 GCC and G1 GCC Licenses – Budgeted for $16,800 (CIP)

Fourth Quarter (Projected)
Network Equipment Update Phase II – Budgeted for $130,000 (CIP will have updated quotes)
Budget process for 2025, 2026, 2027
Planning calendar year 2026

Completed Projects – 2023/2024

Knowbe4 Setup and Implementation
Meraki License Renewals (good through 25/26)
Library Firewall Project
Verkada door system management
City Hall migration with construction
Office equipment & Hardware moving
Windows server 2012R2 EOL updates to windows server 2019 and 2020
VEEAM/Wasabi cloud backup setup

Upcoming Projects –24/25, 25/26

PC Replacements **2024/2025** – Budgeted at *$46,000*
Mobile Device Management and Policy **2024/2025** – Budgeted at *$10,000 (CIP to be updated)*
Networking Equipment Updates Phase II **2024/2025** – Budgeted at *$130,000 (CIP to be updated)*
Phone System Upgrade **2025/2026** – Budgeted at *$250,000 (CIP)*
DPS Fiber Project **2025/2026** – Budgeted at *$125,000 (CIP)*

Information Technology Memorandum

TO: City of Madison Heights
Information Technology Advisory Committee
Cheryl E. Rottmann, Deputy City Manager

FROM: Ty Dolin, Skynet Innovations

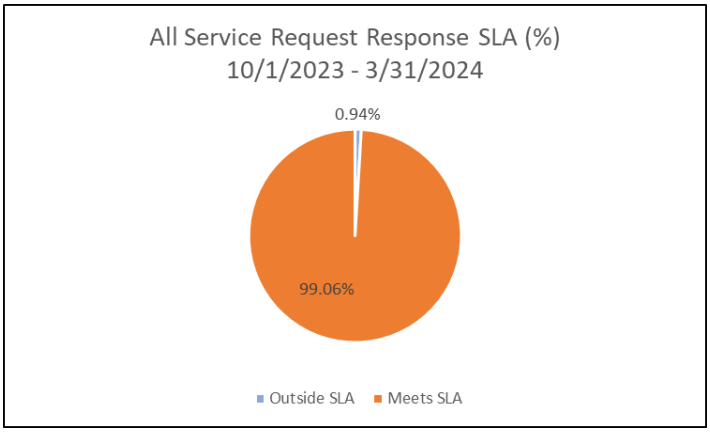
DATE: April 16th 2024

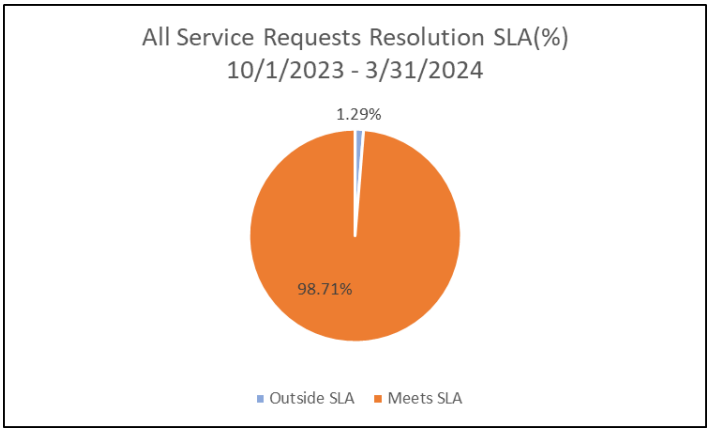
SUBJECT: Service Level Adherence Report – October 1st, 2023 to March 31st 2024

Service Level Agreements:

Below is the breakdown of SLA adherence for all service requests from October 1st, 2023 to March 31st 2024

*due to details in descriptions, summaries for the service requests failing to meet response SLA's are available to members upon request.





All Serice Requests Response SLA (%)	# of Tickets
Outside SLA	8
Meets SLA	846

All Serice Requests Resolution SLA (%)	# of Tickets
Outside SLA	11
Meets SLA	843

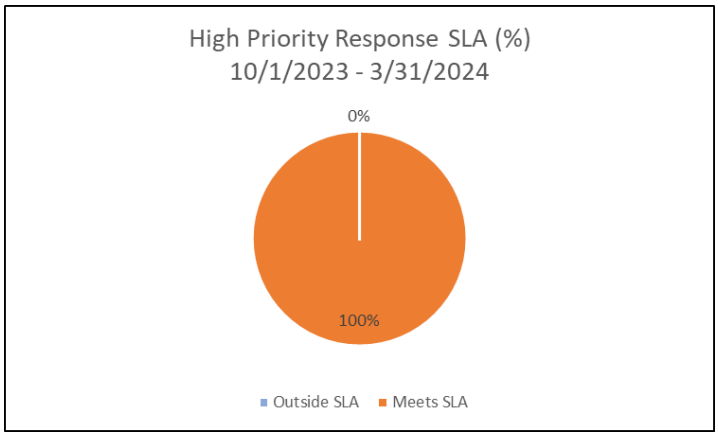
Critical Priority

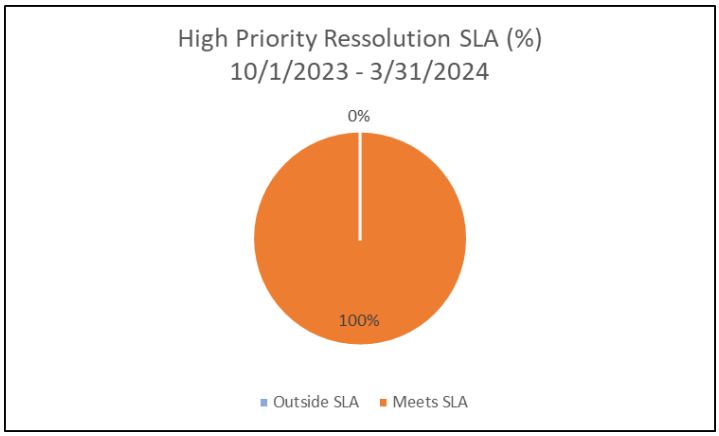
PRIORITY	DEFINITION	RESPONSE TIME		TARGET RESOLUTION TIME	
	Percentage of requests/incidents	90%	100%	95%	100%
One - Critical	A problem or issue impacting a significant group of users or any mission critical IT issue affecting a single customer with no acceptable workaround to the problem.	15 min	30 min	2 hours	4 Hours

There were no Critical priority requests during this period

High Priority

PRIORITY	DEFINITION	RESPONSE TIME		TARGET RESOLUTION TIME	
	Percentage of requests/incidents	90%	100%	95%	100%
Two - High	Non-critical but significant issue affecting a single user or an issue that is degrading the performance and reliability of supported IT services; however, the services are still operational, and a workaround is available.	30 min	1 hour	4 hours	8 hours



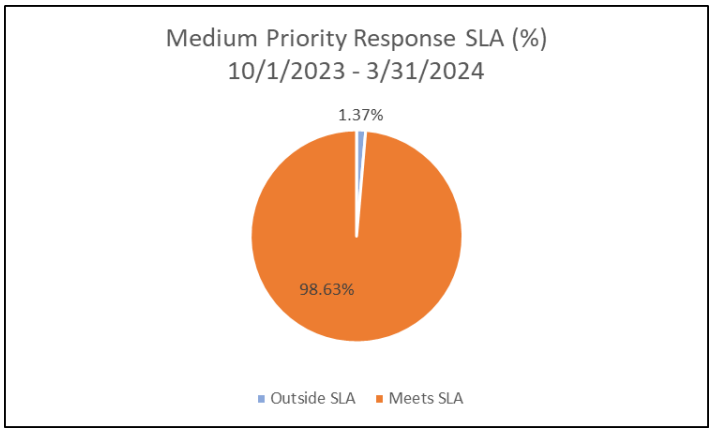


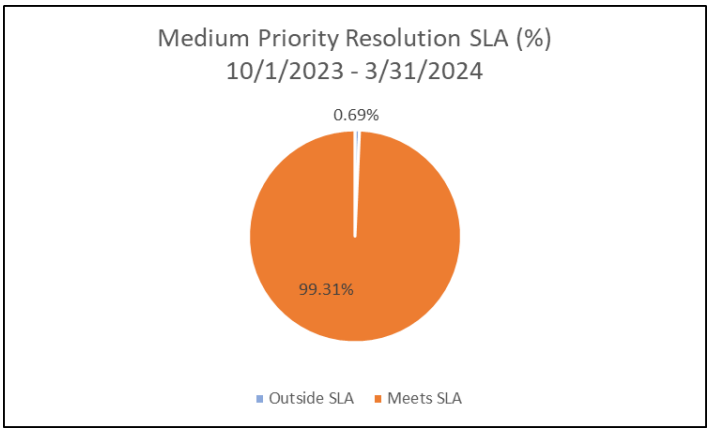
High Priority Response SLA (%)	# of Tickets
Outside SLA	0
Meets SLA	7

High Priority Resolution SLA (%)	# of Tickets
Outside SLA	0
Meets SLA	7

Medium Priority

PRIORITY	DEFINITION	RESPONSE TIME		TARGET RESOLUTION TIME	
	Percentage of requests/incidents	90%	100%	95%	100%
Three - Medium	Priority for routine support requests that impact a single user or noncritical software or hardware error. Productivity may be impacted but not impaired. A workaround may or may not be available.	2 hours	4 hours	2 business days	4 Business days



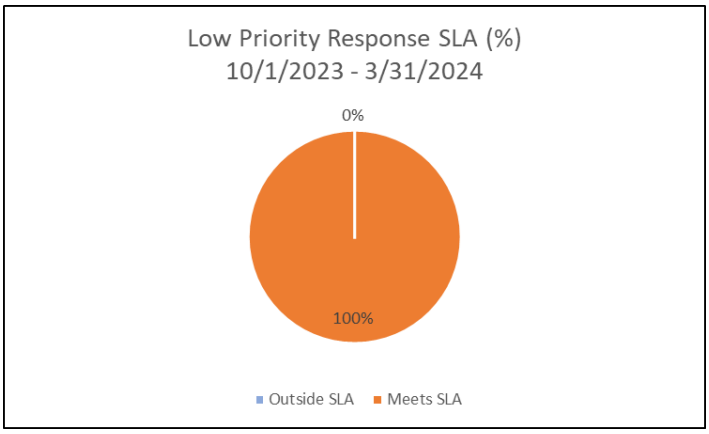


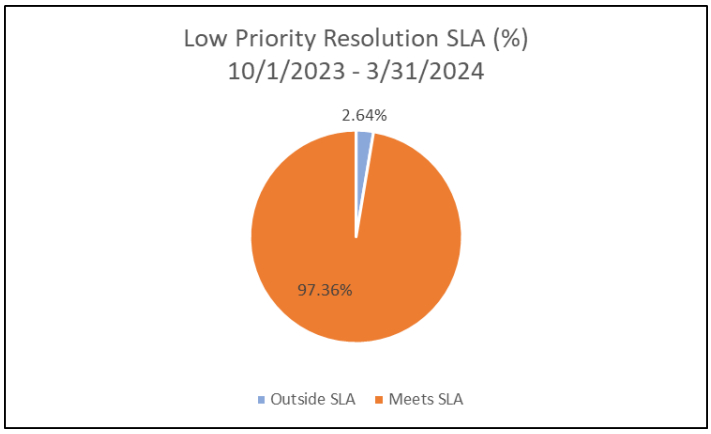
Medium Priority Response SLA (%)	# of Tickets
Outside SLA	8
Meets SLA	574

Medium Priority Resolution SLA (%)	# of Tickets
Outside SLA	4
Meets SLA	578

Low Priority

PRIORITY	DEFINITION	RESPONSE TIME		TARGET RESOLUTION TIME	
	Percentage of requests/incidents	90%	100%	95%	100%
Four - Low	A minor service issue, general inquiry, or request to modify or add services.	8 hours	Next Business Day	5 business days	7 Business days





Low Priority Response SLA (%)	# of Tickets
Outside SLA	0
Meets SLA	265

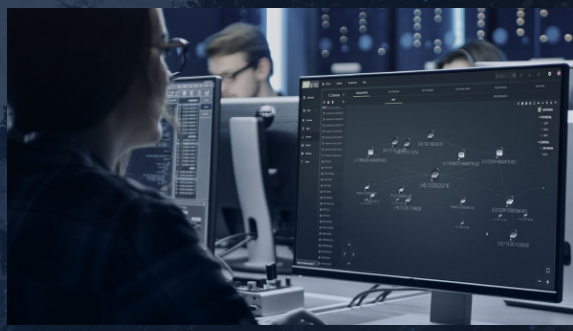
Low Priority Resolution SLA (%)	# of Tickets
Outside SLA	7
Meets SLA	258

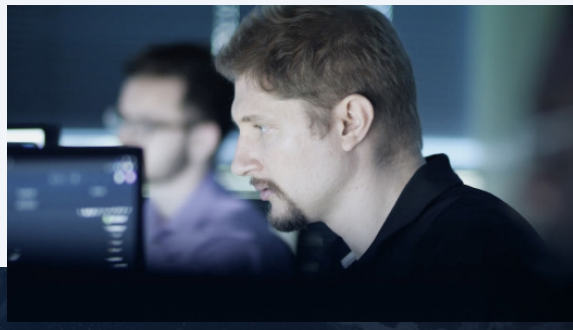
blackpoint

WHY BLACKPOINT CYBER?

Streamlined. Robust. Action-Focused.

Never let cyber adversaries get the best of you. With Blackpoint Cyber, experienced security analysts use state-of-the-art MDR technology to catch what others miss and take action at the first sign of threat. Trust us to do the hard work so you don't have to.





The Blackpoint Cyber Difference

We win the unfair cyber fight while helping others protect what's most important to them. Bringing pain to the adversaries, our team takes out the advanced persistent threats found in today's cyber landscape before they can even see us coming. ***Our mission?*** Provide 24/7, unified detection and response services to organizations of all sizes around the world.

Blackpoint Cyber is proudly built by former US Department of Defense and Intelligence security experts. We are focused on stopping malicious tradecraft and safeguarding MSP operations, full stop. With decades of real-world cyber experience, we leverage insider knowledge to help you fight back and thrive, not just survive in the threat landscape.

Why Blackpoint Cyber?

Cybersecurity Leadership

Blackpoint values ownership, strong ethics, and quality execution. Our leadership team is committed to defending the cyber community so you can focus on supporting your customers.

Commitment to Our Partners

We are proud to serve our partners and deliver true protection from adversaries threatening your livelihood. From our technology to our operations, Blackpoint keeps our partners' needs top of mind.

Real-World Threat Expertise

Founded by former National Security Agency (NSA) cyber operations experts, our team continues to bring nation-state-grade technologies and tactics to our partners around the world.

24/7 MDR Protection

Our Managed Detection and Response solution provides 24/7 protection against even the most advanced of modern-day cyberthreats. Sleep easy knowing we guard your business around the clock.

Rapid Detection & Response

Faster than any other solution on the market, our world-class Security Operations Center (SOC) combines network visualization, tradecraft detection, and endpoint security to detect lateral movement in its earliest stages and stop the spread.

True, Action-Focused Approach

Blackpoint detects and detains threats on your behalf immediately. By the time you hear from us, the threat has already been triaged and removed from your environment. Trust us to provide real action, not just notifications.

OUR MDR-POWERED OFFERING

Start Winning with Blackpoint in Your Corner

Businesses choose our ecosystem of integrated solutions to get ahead of various cybersecurity challenges and requirements.

MDR

Disrupt the hacker timeline. Our patented MDR solution is the first contextually aware breach detection and response program on the market. Stop advanced attacks immediately with unparalleled visibility into hacker tradecraft, lateral spread, and remote privileged activity.

MDR FEATURES

Ransomware Response

Automatically detain ransomware. Automatically stop all types of ransomware deployments, including drive-by attacks that occur within seconds.

Managed EDR

Streamlined managed endpoint security. Elevate your EDR with support from our 24/7 SOC and MDR technology to remediate threats in real time.

Managed Defender for Endpoint

Get the most out of your Microsoft 365 investment. Manage and apply Defender for Endpoint policies to multiple customers with ease.

Cloud RESPONSE

Active response for your cloud. Extend the power of MDR and bring 24/7 expert security monitoring and unified response capabilities to your cloud workflows. Trust leading edge cybersecurity to actively defend your Microsoft 365 and Google Workspace environments.

CLOUD RESPONSE FEATURE

Identity Response for Azure

Contextual alerting for unauthorized logins. Gather contextual analysis about the unauthorized use of Azure SSO logins to better protect your connected services.

MANAGED Application Control

Curated zero trust. Harness our Curated Block List, based on real-world threat insight, in addition to custom application settings, for oversight into what matters most, without the operational bottlenecks.

Vulnerability Management

Security visibility unlocked. Discover and address vulnerabilities within your internal, external, and cloud environments.

BLACKPOINT ADD ONS

Dark Web MONITORING

Integrated credential breach insights. Protect clients with automated dark web surveillance for compromised domains and credentials. With Dark Web Monitoring, you can provide detailed breach reports, delivering value proactively, regardless of breach status.

LogIC

Hyper-efficient logging and compliance. Transform network security logs and telemetry into actionable insights for real-time threat hunting and response, streamlining log integration, compliance reporting, and adherence to numerous requirements.

See Blackpoint MDR in action

Our partners rely on Blackpoint for high-performance, easily upgradeable, and robust cybersecurity that can protect against today's and tomorrow's threats every time. Win the unfair fight with us in your corner.

DEMO TRUE MDR NOW

blackpoint

blackpointcyber.com

blackpoint

Cloud RESPONSE

ACTIVE RESPONSE FOR YOUR CLOUD

Evolving Cloud Security with Human Response

Considering Security for Cloud

Businesses continue to take the digital journey, moving their workloads to the cloud at a rapid pace. Many organizations use their cloud as a conduit for growth as it increases flexibility and productivity, along with reduced operating costs.

However, with the popularity of cloud adoption and remote work, the need for robust security tailor-made for cloud technology does so too. Cloud environments are not immune to cyberthreats and organizations' top challenges include data loss, privacy and compliance issues, and compromised credentials and resources.

INDUSTRY STATISTICS

Email makes up **98%** of the vectors for social engineering incidents.

Verizon 2023 Data Breach Investigations Report

79% consider cloud security as their primary challenge.

Resmo

The average data breach cost for organizations using a public cloud is **$5.02m**.

Resmo

True 24/7 MDR Securing Your Cloud

To support the ever-growing shift to hybrid and cloud environments, we designed Cloud Response – an industry-leading solution offered within our product bundle, Blackpoint Response. Cloud Response takes the power and effectiveness of our proprietary managed detection and response technology and extends it to your cloud.

Focus on your day-to-day operations knowing that our 24/7 security operations center (SOC) leverages MDR to safeguard your cloud platform. While most solutions on the market alert you to take action, Blackpoint provides fast, active response to adversarial threats on your behalf.

Currently, Cloud Response supports:

- Microsoft 365: Azure Active Directory (AD), Exchange, and SharePoint
- Google Workspace: Google Account and Gmail

See Your Cloud Infrastructure Actively Secured

The Power of MDR for Your Cloud

Get peace of mind with Cloud Response which extends our MDR technology and expert SOC analysts to the cloud. Know that you are protected against even the fastest, most advanced types of cyberthreats targeting your third-party cloud platform.

Active Monitoring & Response

Cloud Response allows the 24/7 SOC to provide immediate response to adversarial threats. Rather than alerting you to take action, we take decisive actions against any malicious activity on your behalf. Trust active monitoring and unified response to protect your cloud.

Streamlined Setup & Onboarding

Simple setup? Check. Cloud Response is seamlessly integrated with our MDR technology making the onboarding process simple. In just one day, you'll have Cloud Response guarding one of the most critical IT systems your business uses.

Why Cloud Response?

- Extends Blackpoint's MDR capabilities into Microsoft 365 and Google Workspace cloud environments.
- Enables our 24/7 SOC to see contextual data within your cloud environment and provide immediate and active response against anomalous behavior.
- Allows you to set up policy features to implement cyber hygiene processes across all users and monitor events through custom notifications.
- Our Cloud Response web application has the following abilities:

Microsoft 365

- Manage your Microsoft Azure AD and Exchange policies
- Control and customize Azure AD, Exchange, and SharePoint event email notifications across a tenant
- Set up alerts for malicious login analytics
- Set up detection alerts for malicious email forwarding rules
- Enable our SOC's ability to disable an account, should a threat arise
- Control and customize individual user event email notifications within a specific tenant, including future travel dates
- Gather contextual analysis about the unauthorized use of Azure SSO logins

Google Workspace

- Monitor for malicious Google Account login analytics, such as Login from Unapproved Country and Suspicious Login
- Monitor for malicious Gmail detections, such as Suspicious Email Filter Rule Creation and External Email Forwarding Rule Created
- Enable our SOC to respond and disable a Google Account

Ready to bring active response to your cloud workflows?

SIGN UP TO SEE A DEMO

For more information, or to read our Frequently Asked Questions, refer to our Cloud Response page at blackpointcyber.com/solutions/cloud-response.

blackpoint

blackpointcyber.com

blackpoint

MANAGED Application Control

Curated zero trust, by Blackpoint

Zero trust is a popular piece of many businesses' cybersecurity stacks, with the remote workforce expanding environments to include the cloud, BYOD, IoT, and the use of unsecured networks. But constant maintenance, monitoring, and validation to prevent unauthorized access can be cumbersome. Legitimate users may be denied access, leaving bottlenecks that lead to slow operations and decreased productivity.

That's where Blackpoint's Managed Application Control comes in. This innovative solution takes a modern look at Zero Trust, delivering a prepackaged list of policies designed to block known, bad applications that have been observed by our Security Operations Center in real attacks.

In addition to Blackpoint's curated policies, you can create custom rules for your various customers' specific needs. Trust our 24/7 team of experts and streamlined cybersecurity technology to immediately detect and block the request, based on our combined settings, on your behalf.

With Managed Application Control, you will experience:

- **Simplified security management**
- **Increased operational efficiency**
- **Increased IT visibility**
- **Reduced false positives**

INDUSTRY STATISTICS

73%
of IT professionals said that application control helped them prevent security incidents. (McAfee)

84%
of surveyed organizations reported an increase in application attacks in 2020. (F5)

56%
In the first quarter of 2021, 56% of all cyberattacks were targeted at web applications. (Positive Technologies)

Blackpoint vs The Hacker Timeline

Best-in-Class Protection:

Cover the Pillars of Defense and Resilience with Blackpoint Response

Blackpoint's cybersecurity product bundle is designed to provide layers of protection against advanced threats. In Blackpoint Response alone, partners benefit from solutions for Asset Visibility, Network Hardening, Threat Detection, and Real-Time Response, all for one cost-effective price.

Managed Application Control is a crucial component of the ecosystem, as it fills security gaps by providing partners with a managed list of applications to block, around-the-clock threat detection of unauthorized application use, and real-time response to threats, on your behalf. This ensures that only authorized applications are running on a device, reducing the risk of unauthorized activity or malware infiltration. By leveraging Managed Application Control, partners can further enhance their security posture, adding an additional layer of protection to their overall cybersecurity strategy.

Ready to streamline your zero-trust strategy?

BOOK A DEMO

For more information, or to read our Frequently Asked Questions, refer to our Managed Application Control page at blackpointcyber.com/solutions/managed-application-control.

blackpoint

MDR

Disrupt the Hacker Timeline Now

Blackpoint Cyber's 24/7 managed detection and response (MDR) platform combines network visualization, tradecraft detection, and endpoint security to rapidly detect and neutralize lateral movement in its earliest stages.

Faster than any other solution on the market, we designed our technology with MDR objectives and workflows in mind. Our solution harnesses metadata around suspicious events, hacker tradecraft, and remote privileged activity to catch what others miss and take real action before cyberthreats can spread.

THE THREAT LANDSCAPE — A STARK REALITY

$4.45M USD

Average total cost of a breach

IBM Security's Cost of a Data Breach Report 2023

Only 1 in 3

Only 1 in 3 breaches are identified by an organization's own security team or tool(s)

IBM Security's Cost of a Data Breach Report 2023

Cyberattackers have you in their sights.
What's your next move?

The only constant in the threat landscape is that it is always changing. As threat actors target managed service providers (MSPs) and their clients, building up a strong cybersecurity strategy is crucial. Don't bulk up your security stack with ineffective, non-scalable tools. Take a proactive, offensive approach to stay ahead of cybercriminals by adding continuous monitoring, real-time threat detection, and active response to your arsenal.

At Blackpoint Cyber, we win the unfair fight by giving hackers hell and helping our MSP partners protect what's most important to them. Our mission? Provide unified, 24/7 detection and response services to organizations of all sizes around the world.

Blackpoint vs The Hacker Timeline

When an attack occurs, detection and response times determine whether attackers succeed in their efforts. Blackpoint offers true, 24/7 MDR to fight back threats within minutes and close the gap between the identification of an event and the actual response and remediation. By immediately isolating endpoints, Blackpoint's technology stops the threat from moving laterally into other systems.

See How We Fight

Patented Real-Time Threat Detection

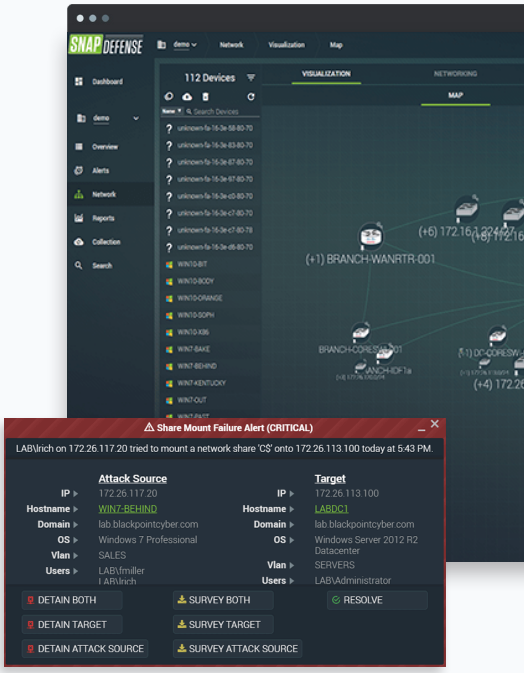
Blackpoint Cyber catches them fast and hits them hard. Using our proprietary security operations and incident response platform, SNAP-Defense, our world-class SOC hunts for active threats in your environment and neutralizes them in their earliest stages. Our technology is built from the ground up to give our analysts the ability to continuously monitor and respond to the modern threat landscape.

24/7 Incident Monitoring & Response

Established by former US government cybersecurity operators, the Blackpoint SOC leverages its deep knowledge of hacker tradecraft and real-world cyber experience to provide absolute and unified detection and response services. Our fully managed SOC team monitors your unique environment around the clock so you can focus on running your business.

Rapid Agent Deployment

Our world-class, nation-state-grade cybersecurity ecosystem is designed to serve our partners by completing the hard work for you. While other services on the market take days and weeks to tune events, we offer same-day agent deployment and start protecting your diverse environments within minutes. Trust Blackpoint Cyber to provide a streamlined on-boarding experience so you can get coverage without compromising your efficiency.



See Blackpoint MDR in action

Rely on Blackpoint for robust, comprehensive, and high-performing cybersecurity that protects against today's and tomorrow's threats. Win the unfair fight with us in your corner.

DEMO TRUE MDR NOW

blackpoint

BLACKPOINT SECURITY OPERATIONS CENTER

24/7 Fully Managed SOC Protecting MSPs

The Stark Reality: Cyberattack Immunity is a Myth

In today's cyberthreat environment, MSPs are targets of cyber attackers who see you as the perfect access point to a wealth of networks and industries. Instead of targeting a single network, they can target many through you. Immunity to cyber threat doesn't exist, so staying agile and building a proactive defense is critical in protecting your and your clients' operations.

More and more, traditional cyber technologies such as anti-virus or anti-malware are not enough. As more MSPs face a high demand for affordable and effective cybersecurity, ***how will you respond when modern, advanced adversaries set their sights on you?***

45%

of businesses have seen a sharp increase in cyberthreats and security incidents

"The State of Security Operations 2020" – a CyberEdge report sponsored by Micro Focus

57%

of businesses are seriously concerned about the current skill shortage in cybersecurity roles

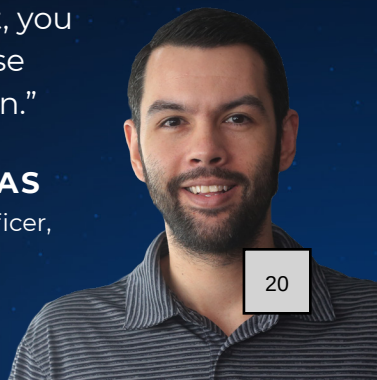
"How to Minimize the Impact of the Cybersecurity Skills Shortage" – Osterman Research for Trustwave

Defining the Value of a SOC

Protecting your business is synonymous with protecting your customers. That's why MSPs who are serious about their cybersecurity invest in a SOC to benefit from in-depth security expertise, human threat analysis, 24/7 monitoring, and immediate incident response. Having a SOC means responding faster, minimizing damages and costs, and safeguarding data and business continuity.

"Many security services place the burden of response and action on their customers. They're under siege but expected to understand the threat, figure out the system internals, and then validate the cleanup. Partnering with Blackpoint Cyber's active SOC means we do the heavy lifting for you, immediately. With Blackpoint, you get true response you can count on."

XAVIER SALINAS
Chief Technology Officer,
Blackpoint Cyber



THE ULTIMATE LONG-TERM CYBER STRATEGY

Combining SOC with True 24/7 MDR Services

A SOC is equipped to identify and prevent cyberthreats in real-time. Regardless of how many endpoints, networks, assets, or locations an organization spans, SOCs provide a centralized view to ensure that they are monitored and performing as needed. *However, is there a way to level up your cybersecurity strategy further?*

SOC MDR

Blackpoint's SOC: Firm Up Your Defense

Blackpoint's SOC team helps streamline how MSPs help their clients face modern, advanced cyberthreats. Our 24/7 SOC team is focused on catching breaches and rapidly responding to contain them. Made up of former US Intelligence cyber experts with real-world experience, their only mission is to monitor your and your clients' networks and detain advanced threats before they can laterally spread across your systems.

Blackpoint's MDR: Build Out Your Offense

As the SOC collects and monitors various data sources within the organization, they add context to make the information more valuable and actionable within the overall threat management process. To bring MSPs a comprehensive cybersecurity solution, Blackpoint's SOC operates in our proprietary MDR technology to combine network visualization, insider threat monitoring, anti-malware, traffic analysis, and endpoint security into an end-to-end, offensive strategy.

Thrive, not survive, in the threat landscape

At Blackpoint, our world-class, nation state-grade MDR technology and SOC team work seamlessly to serve our partners and win the hard unfair fight for you. Have your managed detection and response service installed and protecting your business within a matter of days. Trust Blackpoint Cyber to provide a streamlined onboarding experience so you can get coverage without compromising your efficiency.

GET 24/7 PROTECTION TODAY

blackpoint

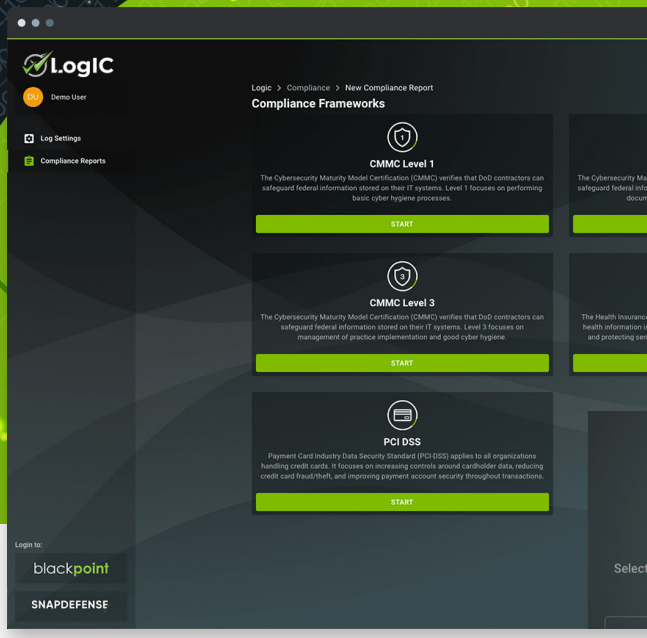
1.410.203.1604
blackpointcyber.com

blackpoint

LogIC

INTELLIGENT LOGGING AND COMPLIANCE

The future of true security + compliance is here



Combine the power of MDR with intelligent logging

During a security event, cutting down on response times is crucial to safeguarding sensitive data. While logging is a start to collecting data and ensuring visibility across an IT environment, true value is in real-time data interpretation allowing for immediate action.

True, 24/7 Managed Detection and Response (MDR) *enhances* the value of security logging. Maximize the power of integrated logging and compliance by pairing it with active threat hunting and immediate response.

66%
Of companies see compliance mandates driving spending. (CSO Online)

45%
Increase in the cost of non-compliance since 2011. (Diligent Compliance)

31%
Of security leaders say lack of visibility of sensitive data is a compliance concern. (Censuswide for Panaseer)

Streamlined, hyper-efficient compliance is finally here

To help MSPs meet the growing demand for both compliance and robust cybersecurity, we designed Blackpoint LogIC – our newest MDR add-on focused on logging with integrated compliance. LogIC is built to be hyper-efficient and provide real-time data collection, helping MSPs collect the data needed for future audits while keeping you and your clients secure.

With LogIC, auto-map against hundreds of compliance requirements all at once, so you can understand where your current security products and services are covering you in terms of compliance. Trust LogIC to make your journey towards regulatory compliance easier.

Building a streamlined, end-to-end stack? Blackpoint can help.

Simple Logging Setup and Configuration

Log collection setup is usually complicated, often requiring additional hardware, appliances, and agent rollouts. LogIC leverages our existing nation-state grade MDR technology for an easy, push-button setup. Adding LogIC to your existing MDR service is as simple as clicking a few buttons. Use our self-service web application to manage and customize all aspects of event and log collection.

Robust Compliance Framework Support

LogIC's hyper-efficient logging architecture supports real-time collection of device logs, file integrity monitoring (FIM) events, and any other application or system that supports syslog*. It currently supports and maps to PCI-DSS, HIPAA, NIST 800-171, CMMC, and CISv8 security frameworks while storing your log data as read-only in 3 different zones with standard AES-256 encryption. Additional compliance standards are to come, ensuring that LogIC will continue to help you collect valuable data.

*Syslog source data will allow 100GB of event data per month. Utilization above this will be charged in $25 increments per 100GB.

Intelligent Mapping to Compliance Standards

Compliance requirements include complicated levels of processes, practices, and qualifiers. Based on the products and services you have with Blackpoint, LogIC's auto-answer capability does the heavy lifting for you by mapping against hundreds of compliance requirements all at once. Then, use our self-service, guided web application to answer any remaining controls. With LogIC, streamline how you prepare for future audits and assessments.

WHY LOGIC?

- ✓ Leverages Blackpoint's proprietary MDR technology for easy, push-button setup.
- ✓ Customize and manage log collection in LogIC's Compliance Report web application.
- ✓ Collected logs are stored in compliance with SEC rule 17a-4, PCIDSS, HIPAA/HITECH, FedRAMP, EU GDPR, and FISMA data storage regulations.
- ✓ Includes 365 days of hyper-optimized, complimentary log storage with options for additional log retention durations.
- ✓ Automatically maps hundreds of compliance controls to Blackpoint technology and services, reducing reporting and assessment efforts.
- ✓ Embeds LogIC information to Blackpoint's monthly MDR reports.

Ready to streamline your compliance and cybersecurity?

Request Demo

For more information, or to read our Frequently Asked Questions, refer to our LogIC page at **blackpointcyber.com/logic**.

Blackpoint LogIC's logging architecture bolsters your cybersecurity posture by supporting real-time collection of file integrity monitoring (FIM) events, device logs, and any other application or system that supports syslog. While LogIC collects key data to assist users in understanding where they are covered in terms of compliance, users must consult with a regulatory compliance authority and/or compliance auditor to guide them through the official assessment.

blackpoint

1.410.203.1604
blackpointcyber.com