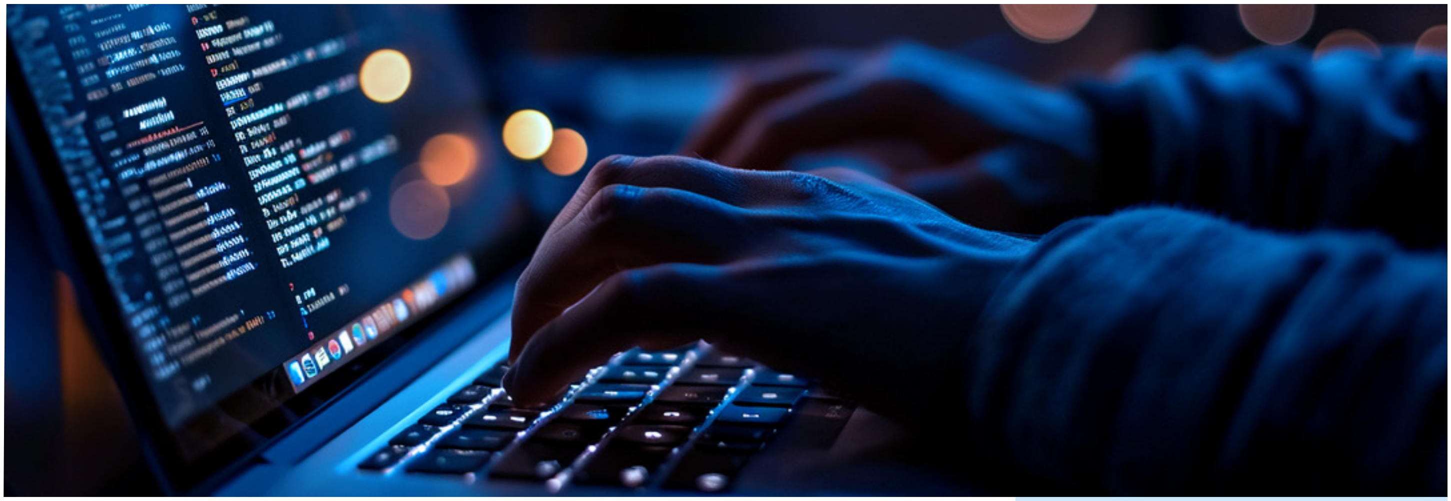
LevelBlue

PRODUCT BRIEF

Threat Detection and Response for Financial Institutions



Protect Your Customers' Financial Data

Financial institutions have long been a top target for cyber criminals and as these organizations broaden their digital footprint, their risk profiles change, and their attack surface widens. Financial institutions are racing to modernize and deliver a smarter and more reliable experience for their customers who are turning more to mobile and online banking. Paying with cash, in-person financial consultations, and even ATMs are all becoming things of the past.

For businesses, the shift in the way they do business means the need for an array of security products, security specialists, and up-to-date threat intelligence to identify and respond to evolving threats. Financial leaders must think differently about their security and make their digital interaction exceptional in order to lead the pack of the new fintech landscape.

LevelBlue can help. With LevelBlue Managed Threat Detection and Response, we can help you detect and respond to advanced threats and exposed risk to protect your business and your brand. A sophisticated managed detection and response (MDR) service, it provides threat management in one service, including 24/7 proactive security monitoring, alarm validation, and incident investigation and response. With it, you can quickly establish or augment your threat detection and response strategy while helping reduce cost and complexity.

Financial Challenges

Digital Transformation Increases the Attack Surface Area

Whether the goal is to improve customer experience, streamline operations, or reduce costs, financial services organizations are becoming increasingly dependent on technology. The shift to more digital banking has caused organizations to change the way they do business. But as they bring on new technologies, organizations also bring on new vulnerabilities for cybercriminals to exploit.

Potential Benefits

- **Improved security monitoring**
  Centralizes security visibility across public cloud environments, on-premises networks, and endpoints
- **Simplified security**
  Combines multiple security essentials to help you deliver smarter, more trusted interactions
- **Automate threat hunting**
  Our continuous threat intelligence and log data help fuel early threat detection so we can respond quickly
- **Accelerate compliance**
  Simplify and accelerate the compliance process with pre-built reporting templates for PCI DSS, FFIEC, and more
- **Powerful threat intelligence**
  Helps to prepare you to face future threats with our unrivaled visibility and provides actionable intelligence from LevelBlue Labs resulting in a faster response

With LevelBlue Managed Threat Detection and Response, you have a flexible solution that readily adapts to your changing IT environment. As you bring on more tools and SaaS applications, the LevelBlue USM Anywhere platform makes it easy to extend security orchestration and automation capabilities with other IT security and operations products and business-critical applications through BlueApps, helping to unify your security architecture and orchestrate your threat detection and response activities from a centralized platform.

Constant Attack Evolution

As technology grows more sophisticated, so do malicious actors. Financial institutions are relying on more advanced technology and more remote endpoints, creating more entry points for a cybercriminal to try to exploit. Because of the high value of financial data, finance companies are a top target for cybercriminals and more susceptible to malware, social engineering, and data manipulation. To defend against the ever-evolving cyberthreats, organizations must stay up to date with the latest threat intelligence and be able to constantly monitor their critical networks and devices on-premises, in the cloud, and in remote locations to identify and contain potential threats before they cause harm. Yet, a truly effective threat detection and response program is difficult to achieve.

LevelBlue Managed Threat Detection and Response is fueled with continuously updated threat intelligence from LevelBlue Labs, providing that your defenses are up-to-date and able to help detect emerging and evolving threats. LevelBlue Labs, the threat intelligence unit of LevelBlue, produces timely threat intelligence that is integrated directly into the LevelBlue USM Anywhere platform in the form of correlation rules and other higher-order detections to automate threat detection. The SOC analyst team is in constant communication with LevelBlue Labs to understand the evolving threat landscape and help to fine tune the new detections that are sent to the USM Anywhere platform daily.

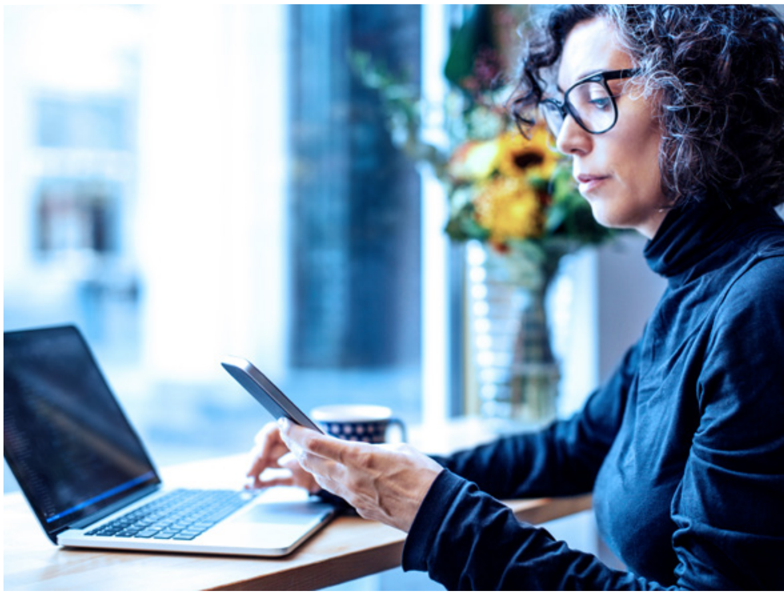
Maintaining Compliance Requirements

Today's businesses face a variety of compliance requirements to help protect consumers. Because of the sensitive nature of customer data, financial services companies in particular are heavily regulated. But compliance can be difficult to maintain and report, and failing to comply is expensive and can damage brand reputation.

LevelBlue Managed Threat Detection and Response helps to support your compliance and risk management goals in multiple ways. The USM Anywhere platform delivers a comprehensive library of predefined report templates for PCI DSS, NIST CSF, and ISO 27001, as well as 50+ predefined event reports by data source and data type. As part of your Threat Model Workshop, we address your specific compliance requirements and your security monitoring environment is tuned accordingly. For example, we can help you to create an asset group that contains the assets required for certain regulations.

Shortage of Skilled Security Personnel

It's no secret that the cybersecurity industry is facing major talent shortage with little relief in sight. Skilled security professionals are in high demand, making it a challenge for organizations to hire and retain top talent. To make matters worse, already understaffed security teams often struggle to focus on strategic security projects as they're busy dealing with the daily operations and maintenance of their security tools, reviewing and investigating noisy SIEM alarms, and manually updating security policies across their systems in response to incidents or vulnerabilities.



The LevelBlue Managed Threat Detection and Response security operations center (SOC) analyst team monitors your environment and critical IT assets 24/7. They handle the daily security operations of monitoring and reviewing alarms and work to reduce false positives so that your team can focus on responding to actual threats, rather than sifting through noise.

In addition, our analysts conduct in-depth incident investigations, providing your incident responders with rich threat context and recommendations for containment and remediation, helping your team to respond quickly and efficiently. Our analysts can even initiate incident response actions, taking advantage of the built-in security orchestration and automation capabilities of the USM Anywhere platform.

How It Works:

Managed 24/7 by Our SOC Experts

Building on experience in delivering managed security services to some of the world's largest and highest-profile companies, the LevelBlue Security Operations Center (SOC) has a dedicated team of security analysts who are solely focused on helping you to protect your business by identifying and disrupting advanced threats around the clock.

The LevelBlue Managed Threat Detection and Response SOC analyst team handles daily security operations on your behalf so that your existing security staff can focus on strategic work. Responsibilities include:

- 24/7 proactive alarm monitoring, validation, and escalation
- Identifying vulnerabilities, configuration errors, and other areas of risk
- Incident investigation
- Response guidance and recommendations
- Orchestrating response actions towards integrated security controls (BlueApps)
- Reviewing your security goals regularly and providing recommendations on policy updates and additional security controls

Built on Unified Security Management

LevelBlue Managed Threat Detection and Response utilizes our award-winning USM Anywhere platform. Key capabilities include asset discovery, vulnerability assessment, network intrusion detection (NIDS), endpoint detection and response (EDR), SIEM event correlation, and long-term log management, incident investigation, compliance reporting, and more.

With these capabilities working in concert, the USM Anywhere platform is able to provide broader threat coverage and deeper environmental context than point solutions alone, helping to enable early detection, reduce false positives, and streamline incident investigations.

Threat Intelligence Powered by LevelBlue Labs

We bring together near-real-time intelligence, innovative threat detection and leading data scientists at LevelBlue Labs to help provide that you're ready to face and defend against cyberthreats, so you can accelerate your digital transformation. LevelBlue Labs goes beyond simply delivering threat indicators to performing deep, qualitative research that provides insight into adversary tools, tactics and procedures (TTPs). By identifying and understanding the behaviors of adversaries and not just their tools, we can help power resilient threat detection, even as attackers change their approach or your IT systems evolve.

LevelBlue

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.

Contact us to learn more, or speak with your LevelBlue sales representative.