On the Front Lines of Cybersecurity

The Essential Elements to Detect and Respond to Threats

Security-aware Technology, People, and Process are critical in securing your business from breaches. The advancement of persistent threats is outpacing the abilities and resources of IT teams today. Every company, regardless of size, need a comprehensive defense-in-depth approach to securing systems and data by extending beyond traditional protections to swiftly detecting and responding to threats. Work with KeyNet, as an extension of your team, to provide a best-fit security solution and protection for your organization backed by a 24x7 Security Operations Center (SOC).

KeyNet Advanced Cybersecurity Includes:

- 24x7 Security Operations Center
- Endpoint Detection & Response
- Security Awareness Training
- Host Based Intrusion Detection
- Data Loss/Leak Prevention
- File Integrity Monitoring
- 400 Day Unlimited Log Storage
- Behavior Analysis
- Dark Web Monitoring
- Managed SIEM
- MITRE ATT&CK Integration

Gain advanced threat mitigation – before, during, and after a cyber incident.

Before a cyber incident: DISCOVER. ENFORCE. HARDEN.

Work with KeyNet to help you understand your infrastructure so you know how to protect and defend it. Discover existing vulnerabilities in your devices and take corrective action to reduce your attack surface. Develop your incident response framework to stay prepared.

During a cyber incident: DETECT. BLOCK. DEFEND.

Quickly identify and stop cybersecurity incidents to minimize disruption. Accurate, real-time threat detection identifies malicious activity across networks and on devices—including advanced malware and zero-day attacks. Taking advantage of advanced software, machine learning, and human interactions allow for active attacks to be identified quickly and stopped so the remediation process can begin.

After a cyber incident: SCOPE. CONTAIN. REMEDIATE.

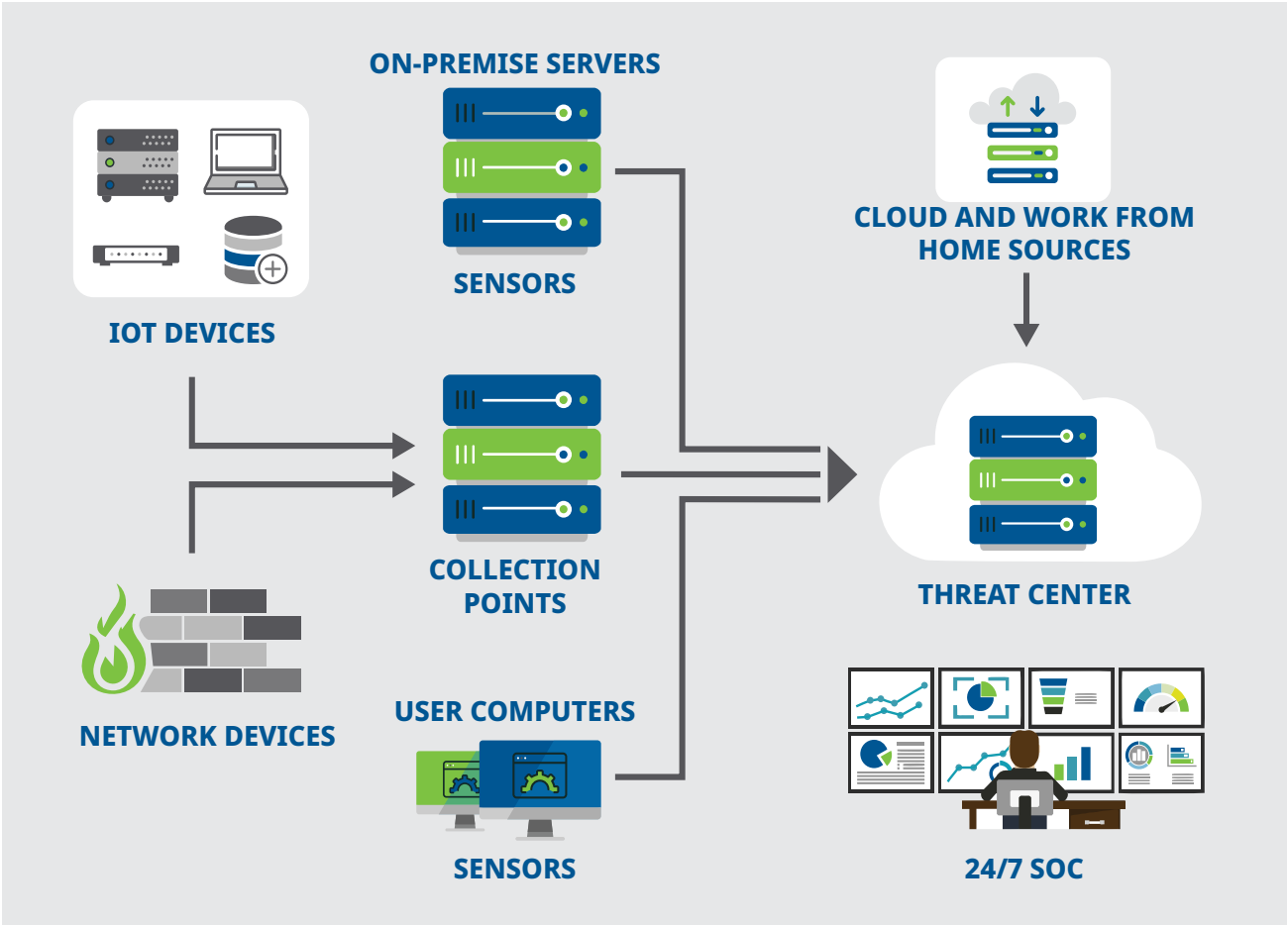
React to incidents efficiently and determine the next steps for remediation. We determine the damage's scope, contain the event, remediate, contact law enforcement as required, and return operations to normal post-incident. After business operations return to normal, we complete a full after-action report and implement and document changes to systems or user behaviors and training based on lessons learned.

KeyNet Advanced Cybersecurity Architecture

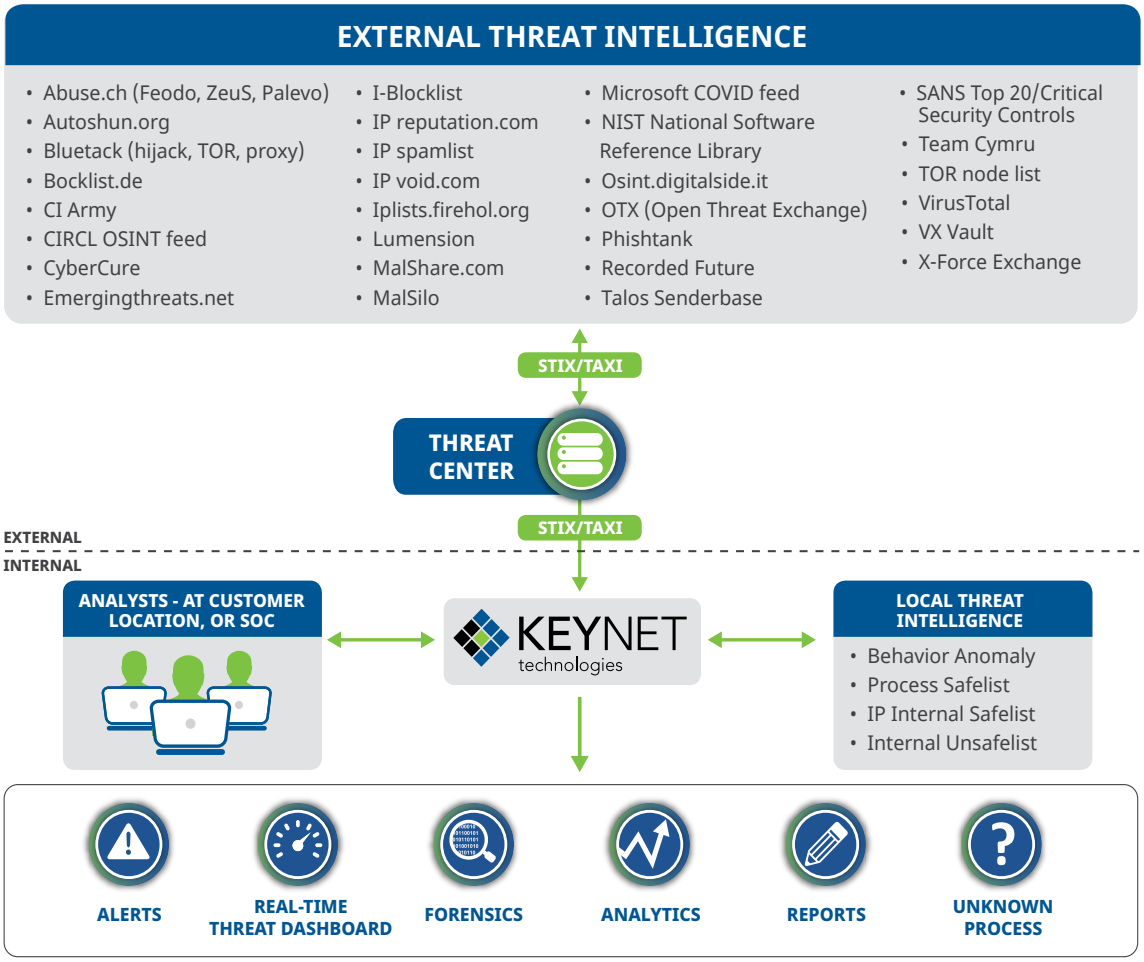
Beyond Traditional Protection and Detection Systems

Comprehensive and actionable threat intelligence is the cornerstone of any cybersecurity solution. The more intelligence a security platform has access to, the more scalable and capable it becomes. KeyNet Advanced Cybersecurity integrates with your on-premise servers, network devices, IoT devices, desktops, laptops, and cloud sources sending log intelligence to the Threat Center for processing and near real-time threat response. While not all incident or breach attempts begin or end within the same threat vector, our advanced Threat Center also accounts for point-in-time and continuous event data from global threat sources to defend against and detect breach attempts. This platform is flexible for any environment with protections that reach beyond the data center walls to corporate devices being utilized for work from home. Here are some of the advantages:

- 24/7 ISO 27001-Certified SOC
- US Based Data Centers
- Unlimited Storage
- 400-Day Retention
- Machine Learning
- Near Realtime Detection & Response
- Global Threat Feeds
- Integrated SIEM & EDR Platform (SE Labs AAA Rated)
- Cloud Platform Integration (AWS/M365/Azure)
- 2,200 Pre-Defined Reports
- Log Correlation & Enrichment
- MITRE ATT&CK Integration
- Global Threat Intelligence Integration
- Local Threat Intelligence Integration
- Security Orchestration & Automation
- Critical Observation Reports
- Compliance Reporting
- Local Threat Intelligence
- Threat Hunting



KeyNet Advanced Cybersecurity Threat Center



The Threat Center is an integrated platform for commercial and open source threat feeds. By integrating the valuable threat data provided by ecosystem partners and open source providers with the machine data collected from throughout the enterprise, Threat Center enables quick and accurate threat detection and response.

Threats are dynamic and attack vectors change constantly. Respond quickly and minimize damage by using the rich external context enabled by threat intelligence. Immediately know about dangerous IP addresses, files, processes, and other risks in your environment.

Threat Center intentionally incorporates threat intelligence from STIX/TAXII-compliant providers as well as commercial and open source feeds all via an integrated threat intelligence ecosystem. This threat intelligence includes data, such as low-reputation IP addresses and URLs, file names, processes, and user agent strings. Using this data, the platform reduces false positives, detects hidden threats, and prioritizes your most concerning alarms, including:

- Known command & control hosts
- Attack response rules
- Compromised hosts
- Potentially compromised systems that try to “phone home”
- Exploit rules for detecting Windows exploits, SQL injections and other attacks
- User-Agent strings for known malware
- Web server attack detection rules
- Unknown or bad processes running on your internal systems
- Anomalous login attempts
- External systems with poor reputation communicating with inside systems

KeyNet's Advanced Cybersecurity Capabilities At-a-Glance

Identify and Stop Cybersecurity Incidents to Minimize Disruption

When you partner with KeyNet, you can be confident that you and your business are thoroughly covered and protected around the clock. KeyNet and our Advanced Cybersecurity Services plug into your team to provide access to a 24x7 Security Operations Center (SOC). The SOC is the 24x7 command center where security experts monitor, detect, analyze, and respond to potential threats and breaches of your data, applications, computers, servers, infrastructure, and cloud services. Review KeyNet's Advanced Cybersecurity key capabilities below:

Security & Information Event Management (SIEM)

At the core of KeyNet Advanced Cybersecurity is the cloud hosted SIEM. The SIEM is used to uncover cyber threat intelligence hidden inside the logs that are sent to the threat center. On top of security benefits, the SIEM assists with operations, reporting and compliance requirements.

eXtended Detection & Response (XDR)

While endpoint protection is crucial as over 70% of data breaches occur via compromised endpoints, expanding detection and response across your entire technology stack to a unified platform increases the efficiency of detection and response. Legacy endpoint protection alone has proven ineffective against morphing attackers and advanced threats. XDR combats today's threats with a comprehensive approach that brings all relevant global and local security data together for improved security operations productivity. Our enhanced detection and response capabilities across the entire technology stack Identify, Protect against, Detect and Respond to Zero-day threats, advanced persistent threats (APTs), ransomware, and file-less attacks with unmatched speed and fewer false positives.

Intrusion Detection

Continuously monitor your entire business infrastructure for unusual patterns and anomalies. Intrusion detection is a critical and core component of the Advanced Cybersecurity solution.

Security Operations Center (SOC)

A SOC allows organizations to fully monitor, detect, investigate, and respond to cyber threats 24/7. But the obstacles to build and maintain an in-house SOC are significant. The high cost of hardware and software alone is daunting, but even more expensive is the process of recruiting, training, and retaining a team of qualified cybersecurity analysts. Let KeyNet Advanced Cybersecurity mature your security posture quickly and at scale.

Threat Detection & Response

Continuously detect and respond to advanced threats efficiently and effectively by combining machine learning-enabled technology and a team that protects your business 24/7. Extend your detect and respond capabilities to your data center, remote offices, teleworkers, work from home employees and the Microsoft 365 services.

Threat Hunting

Threat hunting is needed to uncover threats that might not be otherwise discovered until a breach is found, typically months later. For this reason, the Threat Center is integrated with the MITRE ATT&CK knowledge base of real-world adversary tactics, techniques and procedures. This integration improves threat hunting by understanding how hackers actually operate updating adversary knowledge over time as the threat landscape evolves to give all businesses capabilities previously only available to larger enterprises.

Enhance Your Security Posture with a Trusted Security Partner

Leverage KeyNet to Reduce and Mitigate Cybersecurity Risk

LET'S START A CONVERSATION TODAY!

About KeyNet

The experiences of our client partners define our intentional approach to business technology partnerships. We believe our mindful and caring approach to every engagement sets us apart from the standard IT provider. Through our process of Intentional Design, we plan with clients to align their digital workspace with enhanced end-user and client experiences, while also forecasting trends and making informed recommendations for their success. Through this approach, our execution is invariably aligned with defined business initiatives and outcomes. Our success as a business technology partner is measured by the improvements our partners realize from working with KeyNet.

KEYNET technologies

941 Wheatland Avenue Suite 301
Lancaster, PA 17603
717-517-9604

keynettech.com