tierpoint

FACT SHEET

TIERPOINT CLEANIP™ XDR

The platform, intelligence, and expertise for a proactive approach to security.

The cybersecurity threat landscape is evolving at a rapid pace, from massive OEM breaches to weaponized zero-day exploits. However, most organizations lack the technology or personnel to even detect these emerging cybersecurity threats. A recent study shows the average time between a data breach and discovery is 280 days – that's over 9 months! Today's threats and compliance guidelines require organizations of all sizes to collect, correlate, and analyze security information from all IT systems to enable rapid detection and remediation.

It's time for organizations to take a more proactive approach. At TierPoint, security is the foundation of all our solutions. Our architects and engineers leverage a security-first approach that helps ensure your data is secure by design. TierPoint CleanIP™ XDR is a unified security incident detection and response platform that brings together visibility and correlation with security analysts and engineers providing SOC (Security Operations Center) services.

Get More Out of Your Security Investments: Security and risk management leaders struggle with a myriad of security tools from different vendors with little integration of data or incident response. XDR provides a holistic view of your IT infrastructure without any of the headache or capital investment of traditional solutions.

Augment Your Security Expertise: Many organizations struggle to hire and retain qualified security professionals and/or staff a 24x7 Security Operations Center (SOC) to respond to threats. Let TierPoint's cybersecurity professionals augment your team with our SOC services, providing Daily Cyber Security reviews. Additionally, you can further reduce the burden on your team with our Enhanced SOC services.

Address Regulatory Requirements: Compliance is increasingly complex and a requirement of many businesses. Failure to comply can result in breaches or fines. XDR's daily SOC reviews, along with purpose-built reports, are specifically designed to meet regulatory requirements for cybersecurity monitoring with PCI, HIPAA, GLBA, and other compliance mandates.

Improve Your Security Posture: While many organizations have several best-of breed security solutions, configurations are not actively maintained or tested for effectiveness and are too infrequently upgraded. XDR consolidates multiple security products into a cohesive security incident detection and response platform, all managed by our team of experts.

Increase Productivity: XDR provides a holistic view of the entire IT environment and integrated response options. Coupled with a daily review of all events by an experienced team of SOC analysts, this solution can improve operational security staff productivity.

CleanIP XDR

Detect

Identify internal and external threats faster with a patented and distributed correlation engine backed by a world-class SOC team, before they result in an infection or data breach.

Respond

Our SOC team provides in-depth response guidance on incidents and can be consulted in real-time.

Remediate

With client approval, our teams can respond and remediate threats directly in TierPoint-managed customer environments / infrastructure.

Your Expert Partner

TierPoint helps organizations like yours reduce risk through proactive monitoring of data, applications, and infrastructure. As your trusted cloud and managed services partner, we are already managing your critical systems and infrastructure. When combined with TierPoint CleanIP™ XDR, we are able to rapidly and securely connect into those systems and remediate any threats. Our ability to escalate to internal teams to mitigate threats allows us to quickly and efficiently safeguard each layer of your environment.

Next Gen, Proactive Threat Detection and Response

Daily Cybersecurity Review (DCR) – all incidents manually reviewed by SOC analysts for hidden threats, suspicious trends, and cross comparison daily, alerting our clients of any key findings requiring further investigation.

Enhanced SOC as a Service – add on our ESOC services and receive all support included in the DCR plus immediate investigation to critical severity Incidents to determine if immediate action is required to stop and active or imminent threat.

Enhanced Notifications and Response Guidance - augmented notifications with known threat indicators, country of origin, and additional curated intel allowing response personnel to make faster decisions.

Security Intelligence – unification of diverse sources of data including FortiGuard Threat Intelligence and Indicators of Compromise (IOC) and Threat Intelligence (TI) feeds from commercial, open source, and custom data sources

Distributed Real-Time Event Correlation – complex event patterns can be detected in real time leveraging a FortiSIEM patented algorithm.

Dynamic User Identity Mapping – connects network identity to user identity dynamically – makes it possible to create policies of perform investigations based on user identity instead of IP address.

Component	Description	DCR	ESOC
Daily Cybersecurity Review (DCR)	All incidents manually reviewed by analysts for hidden threats, suspicious trends, and cross comparison. Separate review for each customer daily.	●	●
Executive Summary Reports	Short reports highlighting the number of events, incidents, and notifications processed for the previous month including analyst reviews and escalations.	●	●
Enhanced Notifications	Augmented notifications with known threat indicators, country of origin, and additional curated intel.	●	●
Enhanced Response Guidance	In-depth response guidance embedded with important alerts that include background information and specific steps to investigate and respond.	●	●
Advisory Services	Expert security consultation to help explain impacts and provide specific response / remediation recommendations.	●	●
24x7 Critical Incident Response Support	Analysts available to assist in responding to Emergency-severity or High-severity incidents.	1 Hour	30 Minutes
24x7 High Severity Incident Investigation	Analysts manually investigate these incidents immediately and notify client of any required action within 60 minutes.		●
24x7 Emergency Severity Incident Assistance	Emergency incidents are confirmed by our automated analytics and SOC team. Immediate action is required. An automated alert sent to client within 3 minutes, plus analyst follow-up call within 60 minutes to assist with proper response.		●
First Priority Daily Reviews	Daily Cybersecurity Reviews performed before 8 a.m. EST daily.		●

Learn More

Let us help you improve your security posture with TierPoint CleanIP™ XDR. Call **844.267.3687**, e-mail **sales@tierpoint.com** or visit **tierpoint.com** to find out more.

tierpoint

About TierPoint

A leading national provider of hybrid IT solutions, TierPoint helps organizations drive performance and manage risk. No U.S. provider comes close to matching TierPoint's unique combination of thousands of clients; more than 40 edge-capable data centers and 8 multitenant cloud pods coast to coast; and a comprehensive portfolio of cloud solutions, colocation, disaster recovery, security and other managed IT services. With white-glove customer service, TierPoint professionals customize and manage agile solutions that address each client's unique needs.

tierpoint.com