# Threat Insights

New security vulnerabilities are reported every day. New attacks to exploit these vulnerabilities appear in the wild regularly. Thousands of variants of new malware are released every day. New IP addresses that are part of the attackers' infrastructure appear every day. If you focus on detecting known vulnerabilities, exploits, malware, ransomware, and IP addresses, you will always be behind the curve.

## CHALLENGES

The known issues are easy, such as protection against DDoS attacks. **But today, rather than protecting the network or the node/endpoint, protecting crucial valuable data is key. This is accomplished by validating the user, their device used for access, and a whole lot of contexts and situational awareness, which are key parts of steps to establishing Zero Trust Security.** Traditional firewalls and IDS/IPS were not designed for this approach. Observability is key for user and entity behavior analytics and for effective threat intelligence and security posture management solutions. Additionally, the disjointed approach of ITOps and SecOps leads to configuration or access policy changes that unknowingly impact performance or can completely shut down application access to users.

Security also does not have to come at the cost of application/network performance. **In any network, comprehensive hybrid-cloud security monitoring is accomplished via multi-vendor and multi-domain collaboration, each providing their part to deliver security assurance and protection.**

# SOLUTION

Ennetix' goal is to establish full provenance of every packet on the network and every application executed on a computer. For a packet, we should know the device that generated it, the application on that device that sent it, how that application was started, what organization compiled the application, the user that ran the application, where the user logged in from, and how the user authenticated him/herself.

Ennetix xVisor's observability and discovery – with its foundation and starting point being the user-application relationships – provides continuous **User Entity Behavior Analytics (UEBA) that are critical to succeed in the new paradigm of Trust Nothing.** xVisor seamlessly combines network traffic (both North-South and East-West) and endpoint data along with third-party threat intelligence data to provide complete end-to-end visibility of the user-application relationships. xVisor focuses on detecting behaviors and kill chains common to many attacks. This allows us to stay ahead of the curve.

xVisor's innovative analytics techniques include classification and prediction of process and entity behaviors, application/process/provider provenance, identifying novel attack kill chains, etc. xVisor can correlate performance degradations from access denials, security policy changes, etc. Furthermore, xVisor also enables software supply-chain security management through DevSecOps integrations using third-party application codebase analyses, developer team integrity and provenance assurance, etc.

## CONCLUSION

AIOps is incomplete without threat insights and preemptive validation of potential performance impacts or degradation due to security posture changes; we do our part to make the network secure through comprehensive integrations of network and endpoint data as well as third-party threat intelligence sources. How far do you take Ennetix xVisor's threat intelligence solutions to automate remediation is in your hands!

## CONTACT US

Visit us at
https://ennetix.com

For more details
info@ennetix.com