Verint Threat Protection System™

NEW PERSPECTIVE. NEW DEFENSE.

VERINT®

More Informed.
More Effective.
More Timely Decisions.

Verint Threat Protection System™ (TPS) is a pre-integrated, intelligence-driven platform that marks the onset of a new era in cyber security. Rather than reacting to the last attack, TPS lets SOC teams hone in on attacks as they happen. By orchestrating and automating intelligence across detection, forensics, investigation and response, TPS brings the full attack storyline to analysts' fingertips, enabling better decisions and faster remediation.

CYBER ADVERSARIES ARE STILL SLIPPING THROUGH THE CRACKS

Advanced cyber attacks continue to cause significant financial, operational and reputational damage to government and commercial organizations. These attacks exploit the gaps in traditional security approaches, such as a lack of shared intelligence among siloed security tools, excessive alerts, insufficient automation and a shortage of skilled cyber analysts.

Organizations need a completely new paradigm for cyber defense. One that eliminates guesswork and partial views by letting analysts dive deeper, gather accurate information and gain a complete understanding of what's going on.

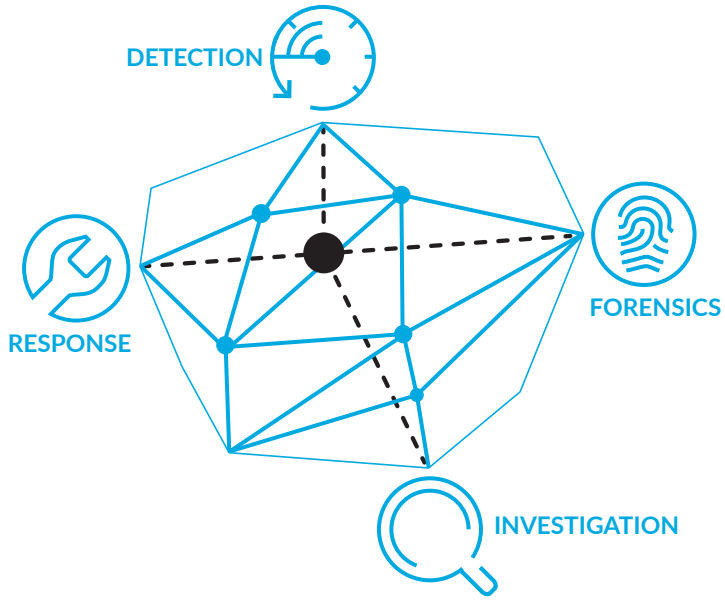
"Security operations centers must be architected for intelligence, embracing an adaptive security architecture to become context-aware and intelligence-driven."

Gartner, The Five Characteristics of an Intelligence-Driven Security Operations Center, November 2015

VERINT THREAT PROTECTION SYSTEM – THE INTELLIGENCE TO PINPOINT EVEN THE STEALTHIEST ATTACKS

Verint® Threat Protection System™ (TPS) revolutionizes the way organizations defend themselves against cyber threats. TPS uniquely combines intelligent multi-vector attack detection, automated investigation, deep forensics and actionable response – all in one, pre-integrated platform. Providing a new perspective on cyber defense, TPS continuously gathers evidence and intelligence, gleaning insights on-the-fly to confirm or refute an attack and presenting its findings in a unified workspace. This approach provides analysts with the accurate, localized threat intelligence they need to stop attacks in their path.

TPS monitors payloads, network and endpoints, automatically detecting attacks across the attack cycle. Multiple detection engines send indicators of compromise to a central TPS brain for analysis and cross-validation, effectively reducing false positives. Patent-pending automated forensic investigation transforms thousands of alerts into dozens of incidents, each complete with the attack story and recommendations for incident response.



Orchestrating intelligence across a single platform for a new kind of cyber defense

ONE PRE-INTEGRATED PLATFORM FOR A CLEAR, CHRONOLOGICAL ATTACK PICTURE

Unlike other solutions, TPS offers a complete array of pre-integrated and automated tools that enable analysts to see the full attack storyline.

Detection – Specialized detection engines use machine learning, anomaly detection and heuristic technologies to identify malware within files, command & control communications, lateral movement and infected endpoints across the network. The sensors share intelligence and automatically glean insights to reduce false positives.

Investigation – TPS automates the investigation process, fusing thousands of alerts into a handful of prioritized and confirmed incidents and providing visualized attack maps for rapid response.

Forensics - A full set of network and endpoint forensics tools enables native access to raw data for additional evidence gathering and better understanding of the attack source and methods.

Response - Automated investigation engines hand over the incidents - each complete with the full attack story and recommended next steps - to the SOC analyst for fast remediation

KEY BENEFITS

SIMPLIFY CYBER INVESTIGATIONS
Unified workflows, integrated investigation tools and visualized attack maps create a clear picture of the attack.

FAST & ACCURATE DETECTION
Intelligence-driven detection engines continuously gather and orchestrate local threat intelligence to hone in on attacks

REDUCE NOISE & FALSE POSITIVES
Frees analysts to focus on the more complex investigations by transforming alerts into meaningful incidents with recommendations for response

FLEXIBLE AND OPEN ARCHITECTURE
Lets you integrate with existing or future security investments and stay ahead of future threats, while supporting various deployment options

DOMAIN EXPERTISE
Trusted partner with over 20 years' experience in building and deploying Actionable Intelligence™ solutions for thousands of organizations worldwide

About Verint Systems Inc.

Verint® (Nasdaq: VRNT) is a global leader in Actionable Intelligence® solutions with a focus on customer engagement optimization, security intelligence, and fraud, risk and compliance. Today, more than 10,000 organizations in 180 countries — including over 80 percent of the Fortune 100 — count on intelligence from Verint solutions to make more informed, effective and timely decisions.

Learn more about how we're creating A Smarter World with Actionable Intelligence® at www.verint.com

www.verint.com/cyber | Info.cyber@verint.com

VERINT®