Galaxite solutions

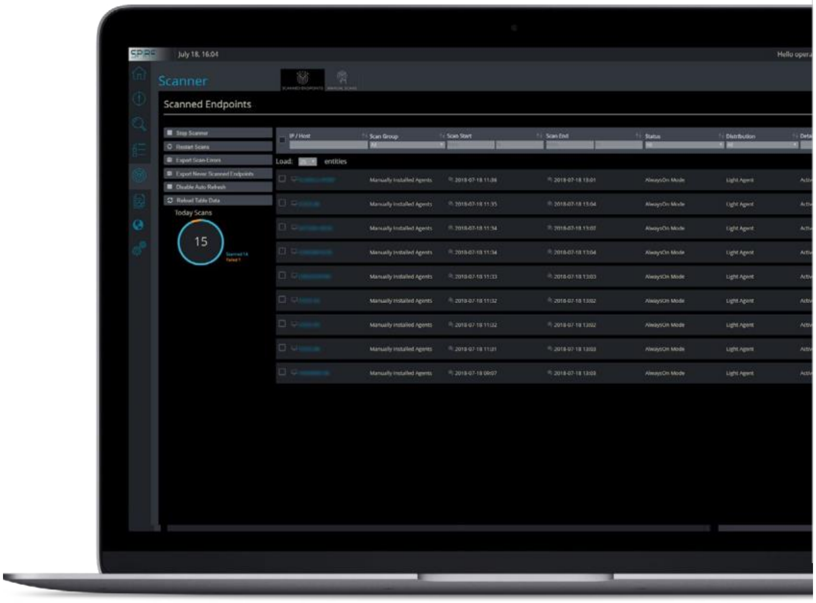
GALAXITE 360

GALAXITE is designed for organizations who want enterprise-grade security with complete protection within the perimeter - defending endpoints, network, files and users - without the heavy burden of deep cyber expertise and the overhead of integrating and managing multiple products.

By fully embracing a cloud-based architecture, GALAXITE eliminates the need to deploy and maintain multiplesecurity solutions and services and is compatible withany infrastructure.

GALAXITE converges and brings synergy with technology: endpoint protection, EDR, vulnerability management, deception, threat intelligence, network and end-user analytics, and expertise: a 24/7 cyber SWAT team for incident response, malware analysis, threat hunting andforensics.

GALAXITE deploys in hours with no installation or setup andsimplifies management with automated monitoring tocomplement any sized staff. With a 360 view across users, network, files and endpoints, organizations
gain unparalleled visibility to control, understand and mitigate threats.



IP / Host	Scan Group	Scan Start	Scan End	Status	Distribution	Deta
[illegible]	Manually Installed Agents	2018-07-18 11:36	2018-07-18 13:01	AlwaysOn Mode	Light Agent	Activ
[illegible]	Manually Installed Agents	2018-07-18 11:35	2018-07-18 13:04	AlwaysOn Mode	Light Agent	Activ
[illegible]	Manually Installed Agents	2018-07-18 11:34	2018-07-18 13:02	AlwaysOn Mode	Light Agent	Activ
[illegible]	Manually Installed Agents	2018-07-18 11:34	2018-07-18 13:04	AlwaysOn Mode	Light Agent	Activ
[illegible]	Manually Installed Agents	2018-07-18 11:33	2018-07-18 13:03	AlwaysOn Mode	Light Agent	Activ
[illegible]	Manually Installed Agents	2018-07-18 11:32	2018-07-18 13:02	AlwaysOn Mode	Light Agent	Activ
[illegible]	Manually Installed Agents	2018-07-18 11:22	2018-07-18 13:02	AlwaysOn Mode	Light Agent	Activ
[illegible]	Manually Installed Agents	2018-07-18 11:01	2018-07-18 13:03	AlwaysOn Mode	Light Agent	Activ
[illegible]	Manually Installed Agents	2018-07-18 09:07	2018-07-18 13:03	AlwaysOn Mode	Light Agent	Activ

Only with the GALAXITE 360 Security Platform organizations enjoy:

Complete 360 visibility and protection:

- → Enjoy a complete defensive portfolio including malware, insider threat, ransomware and more for organizations of any size.
- → Complete attack visibility across endpoint, users, files and network.
- → Aggregated alerts

Dramatically simplified deployment and maintenance.

Cloud-based approach deploys in hours with no long-term maintenance costs and no installation or setup.

Complement in-house with complementary security expertise-especially if you don’t have any.

Only GALAXITE includes continuous monitoring means by an experienced security operations center-regardless of experience.

Technology

Endpoint protection platform (EPP)

Rapidly detects threats across thousands of endpoints. Unlike other endpoint technologies GALAXITE performs critical component whitelisting,memory protection and credential protection. Other capabilities include:

- → Anti malware
- → Anti ransomware
- → Anti exploit
- → Fileless attack prevention
- → Nextgen AV
- → Sandboxing

Endpoint detection and response (EDR)

GALAXITE's EDR provides a detailed play-by-play of what took place on an endpoint during and after an attack to detail how a hacker mounted an attack and moved laterally. With GALAXITE's EDR, organizations can cut off potentially infected machines from the network to preventfurther damage. GALAXITE's EDR capabilities include:

- → Full and automated response & remediation
- → Threat hunting
- → Endpoint configuration discovery

User and entity behavior (UBA) analytics

Unlike other UBA tools, GALAXITE can ask employees to self-verify their behavior. Other capabilities include analytics to detect:

- → User behavior anomalies
- → Insider threats
- → Lateral movement
- → Privilege escalation

Converged network analytics

Unlike other network analytics tools, GALAXITE collects and correlates the broadest set of input including TAP/port mirroring/syslog integrate with threat intelligence, endpoint and firewalls to provide full visibility and analysis of network traffic to detect. Capabilities include:

- → Data exfil prevention
- → Network attack detection, including
  - Port, SMB and IP Scanning
  - ARP and DNS Poisoning
  - ICMP, HTTP, C&C and DNS Tunneling
  - Lateral movement: Pass the hash and pass the token.

Technology

Vulnerability management

Capabilities include:

→ Application patch management

→ OS patch management

→ Agent verification

→ Risky application discovery

Correlated threat intelligence

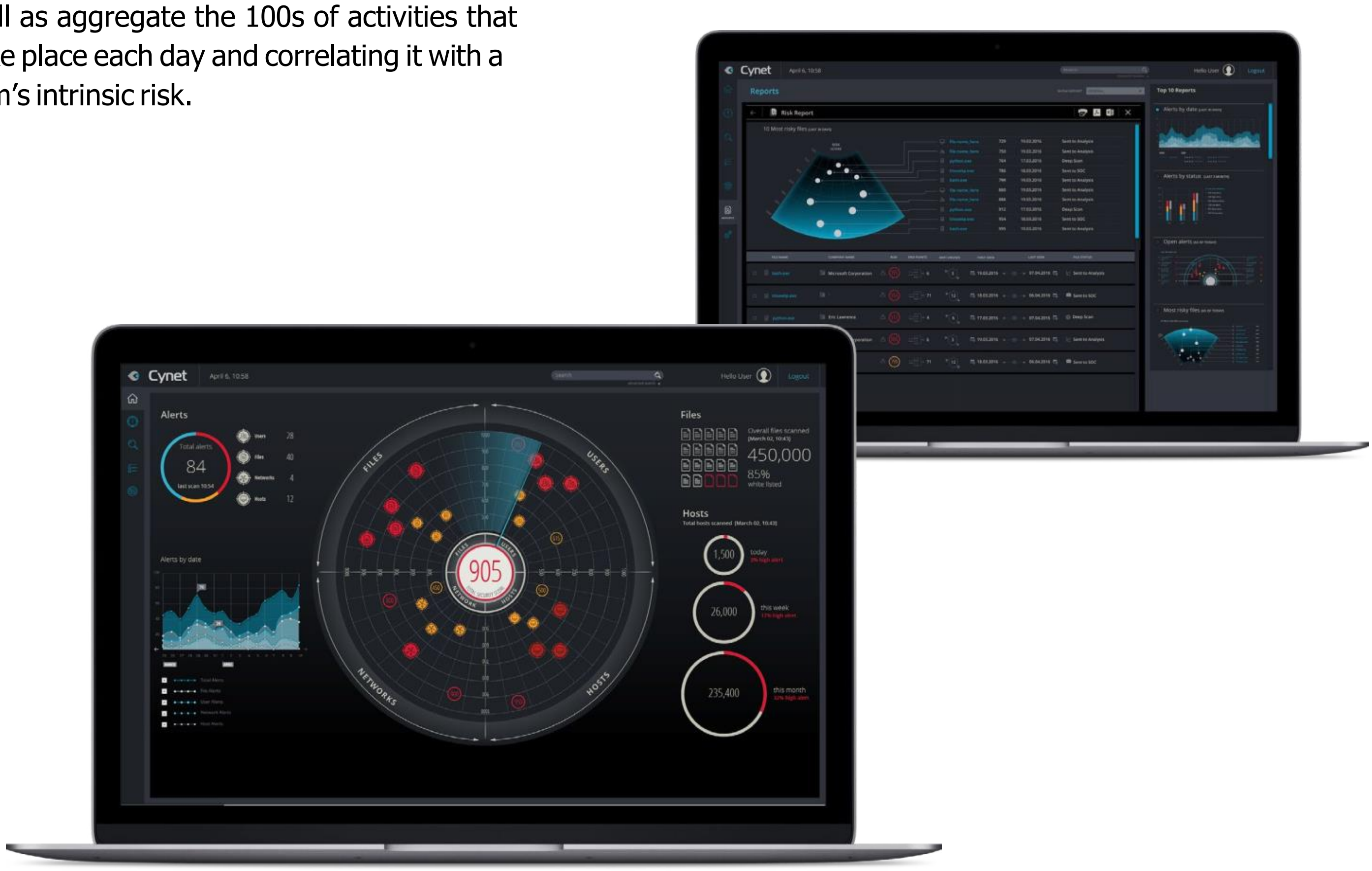
Leverage 20+ external threat intel sources as well as aggregate the 100s of activities that take place each day and correlating it with a firm's intrinsic risk.

Deception

Unlike other deception tools, GALAXITE inserts customizable beacons into documents. In addition, since GALAXITE's endpoint technology already lives on endpoints, we bypass the need for incremental honeypots. Other capabilities include:

→ Placing decoy files, credentials, configurations and network behavior to lure an attacker to pre-deployed traps.

→ Tracking mechanisms then monitor and provide a clear picture of attacker activity.



Expertise

At no additional cost, GALAXITE includes a 24/7 cyber SWATteam to provide expertise to ensure organizations stay safe even with a fast-evolving threatscape. Unlike othermanaged services that just focus on endpoint, GALAXITE's telemetry encompasses complete attack visibility across endpoint, users, files and networks for extreme fidelity. More importantly, using the GALAXITE platform, organizationseliminate infrastructure management headaches.

GALAXITE's 24/7 cyber SWAT team includes:

Essential staff

- **Tier 1:** security analysts
- **Tier 2:** security researchers
- **Tier 3:** malware researchers

Essential services

Incident response (IR): Led by a team of highly seasoned security experts, GALAXITE provides organizations under attack with 24/7 global IR when needed.

Forensics: Deep dive forensic investigations, enabling them to rapidly identify and investigate suspicious incidents.

Threat hunting: Combing through network, endpoint, file and user data to uncover advanced threats.

Malware analysis: Identify the capability, origin and potential impact of malware uncovered within your organization.

Benefits

Reduce risk with complete protection from cyber attacks behind a single pane of glass with one dashboard and agent for a consolidated risk visibility and simplicity

Optimized security spend: Increase the efficiency and effectiveness of your security team and current technical investments at an affordable price.

Total protection in hours: Install and deploy in just a few hours. Easily comply with audits

Streamlined security operations with fully automated security response capabilities including:

- Automated remediation and incident response
- Kill process, delete or quarantine malicious files
- Disable users and run commands
- Shut down or restart hosts
- Isolate or block traffic

Precisely scope security events to reduce false positives and negatives: identify more attacks as well as increase the accuracy of blocking and investigation.

Provides full visibility across the network. Cross correlation across networks, users, files and endpoints.