Expanse with Splunk

Bring Whole-Internet Visibility to Security and IT Ops

Security Starts with Knowing What to Protect

Organizations are managing more Internet-connected assets than ever before. But with the rise of cloud, remote workers, and the decentralization of IT, it's challenging to monitor and secure these assets and their communications, since a central inventory of all of these assets is nearly always incomplete, inaccurate, or stale.

That's where the power of Expanse with Splunk comes in. With Expanse, you get whole-Internet visibility that dynamically provides a complete, current, and accurate inventory of your Internet-connected assets and their behavior. With Splunk, you get a comprehensive system to interact with this invaluable information from Expanse and data from other sources to improve efficiency and reduce risk.

Expanse with Splunk for Security

Expanse empowers security teams to mitigate risk and improve their cybersecurity posture by continuously discovering Internet-connected assets and monitoring those assets for configuration changes, vulnerabilities like exposed remote access protocols, or suspicious behavior. Using Splunk, security teams can further operationalize data from Expanse to manage security threats, including across assets they previously were unaware of or did not have visibility into.

In just one quarter in 2018, Expanse found 70 of the Fortune 100 had an RDP exposure.

Use Cases:

- ✓ Attack Surface Reduction: With automatic alerts to any exposures on your network, you can quickly triage any potential security events and remediate the issue, including on assets not found by any other tool or system.
- ✓ Identifying Risky Behaviors: Get automatic alerts of risky and out-of-policy network communications, without any need for network deployment, so you can rapidly investigate and remediate them.
- ✓ Enhanced Event Data: Enrich network assets inside Splunk with service, attribution, and ownership data from Expanse, enabling your team to take actions with better context.
- ✓ Automatic Remediation: Trigger orchestration workflows off Expanse findings in Phantom for automatic remediation.
- ✓ Executive Reporting: Provide accurate, complete, and easy-to-understand reports on attack surface reduction progress to executive stakeholders.

Benefits:

- ✓ Boost security team productivity with Internet-wide visibility into assets, exposures, and risky communications.
- ✓ Improve your security posture by reducing your organization's attack surface and rapidly identifying and remediating any exposures or risky communications.
- ✓ Reduce mean time to detect (MTTD) with continuous monitoring of all of your organization's Internet-connected assets.
- ✓ Reduce mean time to resolution (MTTR) with continuous visibility and rapid troubleshooting.

Expanse with Splunk for IT Operations

Expanse equips IT operations with a continuously updated inventory of all your organization's Internet-connected assets on-prem and in the cloud. Using Splunk, you can correlate date from Expanse with other sources to prevent, predict, monitor, and remediate IT problems across all of your Internet-connected assets.

For all customers, Expanse has identified anywhere from **3% to almost 70%** more Internet-exposed assets than previously known or tracked.

Use Cases:

- ✓ Internet Asset Lifecycle Management: Get a complete, continuous, and accurate inventory of your company's Internet-connected assets, including IP addresses, domains, and certificates, and manage their lifecycles.
- ✓ Cloud Asset Discovery and Consolidation: Discover shadow cloud infrastructure to bring unknown assets under management.
- ✓ Executive Reporting: Provide accurate, complete, and easy-to-understand reports on IT operations and events to executive stakeholders.

Benefits:

- ✓ Improve IT operations productivity with simplified Internet Asset lifecycle management and reporting.
- ✓ Boost customer and stakeholder satisfaction with improved remediation of service issues.
- ✓ Prevent business interruption and outages by proactively monitoring your on-prem and cloud Internet-connected assets.

How Expanse Works

Expanse indexes the entire Internet to collect data about every device connected to it. From there, we build out a comprehensive inventory of your organization's Internet-connected assets, including IP ranges, certificates, and domains. Our indexing surfaces any exposures present on each of those assets that could be attacked or exploited. By combining observed Internet traffic and active sensing data, we also surface risky and out-of-policy communications between your assets and others on the public Internet.

With this knowledge, Expanse is able to provide you with a comprehensive, continuously updated inventory of all of your Internet-connected assets and their details, including associated exposures, non compliant configurations, and risky communication behaviors. Our products are agentless and connect with Splunk via API and our technical add-on.

"Expanse lets you find data a lot faster than other tools out there."

Customer Quote