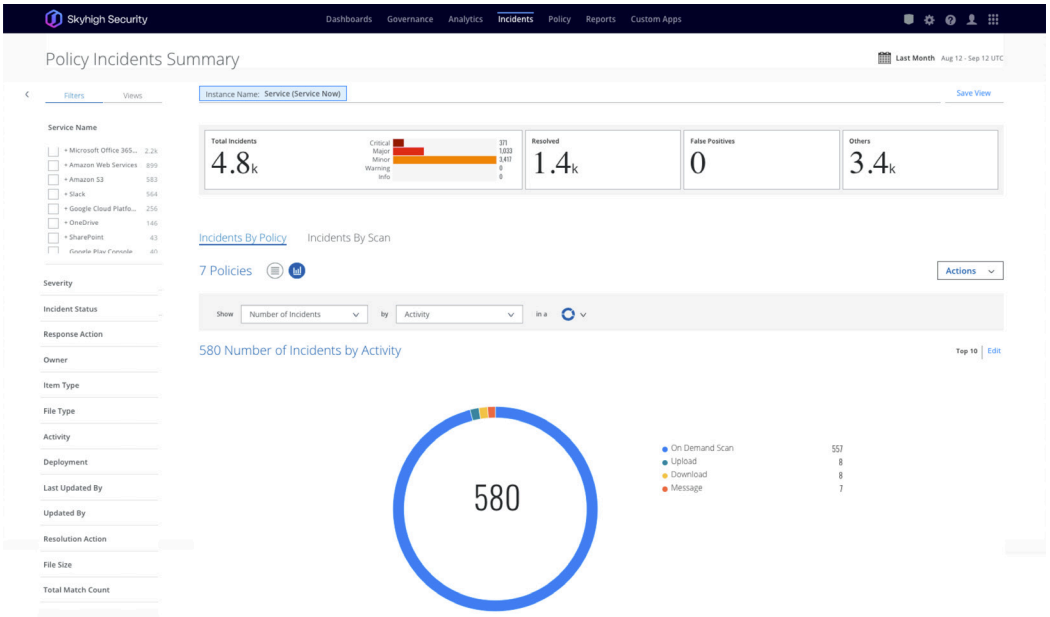
DATA SHEET

Skyhigh Security for ServiceNow

KEY USE CASES

- Detect and remediate insider threats, compromised accounts, and privileged user threats
- Enforce data loss prevention policies to prevent violations in real-time
- Encrypt structured and unstructured data with enterprise-controlled keys
- Enforce access control policies to data based on device, user, and location
- Limit the download of sensitive data to unmanaged BYOD devices
- Capture a complete audit trail of user and administrator activity for forensic investigations

Skyhigh Security for ServiceNow helps organizations securely accelerate their business by providing total control over data and user activity in ServiceNow



Key Features

Unified Policy Engine

Applies unified policies to ServiceNow and all cloud services across data at rest and in transit. Leverage policy templates, import policies from existing solutions, or create new ones.

Policy Creation Wizard

Defines customized policies using rules connected by Boolean logic, exceptions, and multi-tier remediation based on incident severity.

Pre-Built Policy Templates

Delivers out-of-the-box policy templates based on business requirement, compliance regulation, industry, cloud service, and third-party benchmark.

Usage Analytics

Identifies all users and groups accessing ServiceNow and reveals which users are accessing sensitive data.

User Groups

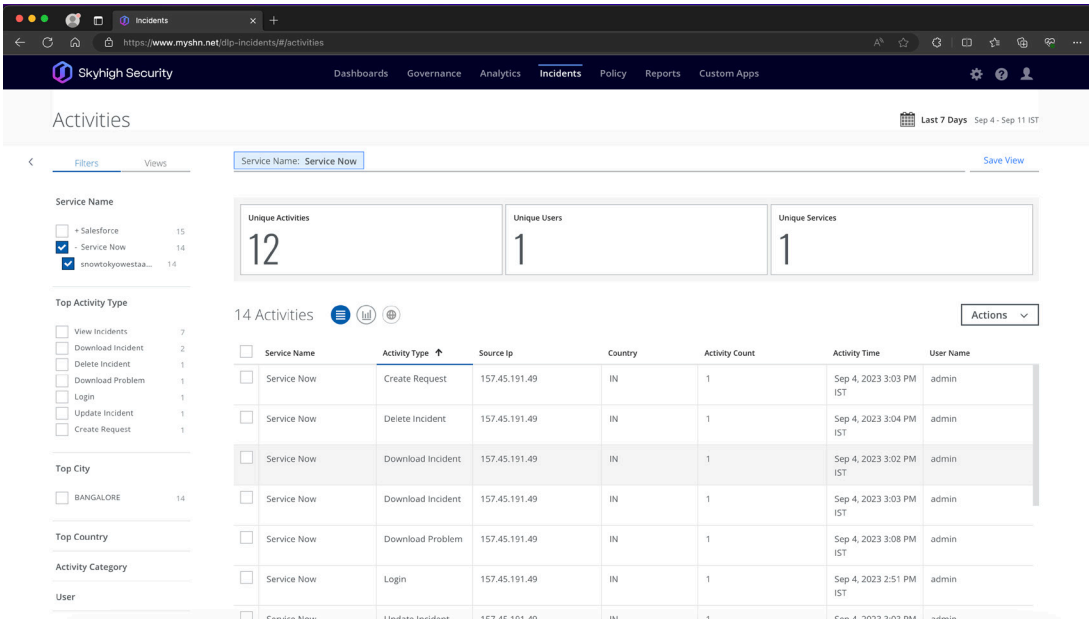
Discovers and groups users from directory services and ServiceNow. User groups can be leveraged for analytics and policy enforcement.

ServiceNow SOC

Delivers a threat dashboard and incident-response workflow to review and remediate insider threats, privileged user misuse, and compromised accounts.

Cloud Activity Monitoring

Provides a complete audit trail of all user and admin activities to enable post-incident forensic investigations.



User Behavior Analytics

Automatically builds a self-learning model based on multiple heuristics and identifies patterns of activity indicative of user threats.

Account Compromise Analytics

Analyzes login attempts to identify impossible cross-region access, brute-force attacks, and untrusted locations indicative of compromised accounts.

Privileged User Analytics

Identifies excessive user permissions, inactive accounts, inappropriate access, and unwarranted escalation of privileges and user provisioning.

Guided Learning

Provides human input to machine learning models with real-time preview showing the impact of a sensitivity change on anomalies detected by the system.

Cloud Data Loss Prevention

Enforces DLP policies based on data identifiers, keywords, and structured/unstructured fingerprints across standard and custom fields and files.

Multi-Tier Remediation

Provides coach user, notify administrator, block, and apply rights management options and enables tiered response based on severity.

Policy Violations Management

Offers a unified interface to review DLP violations, including content that triggered the violation, with remediation workflow.

Match Highlighting

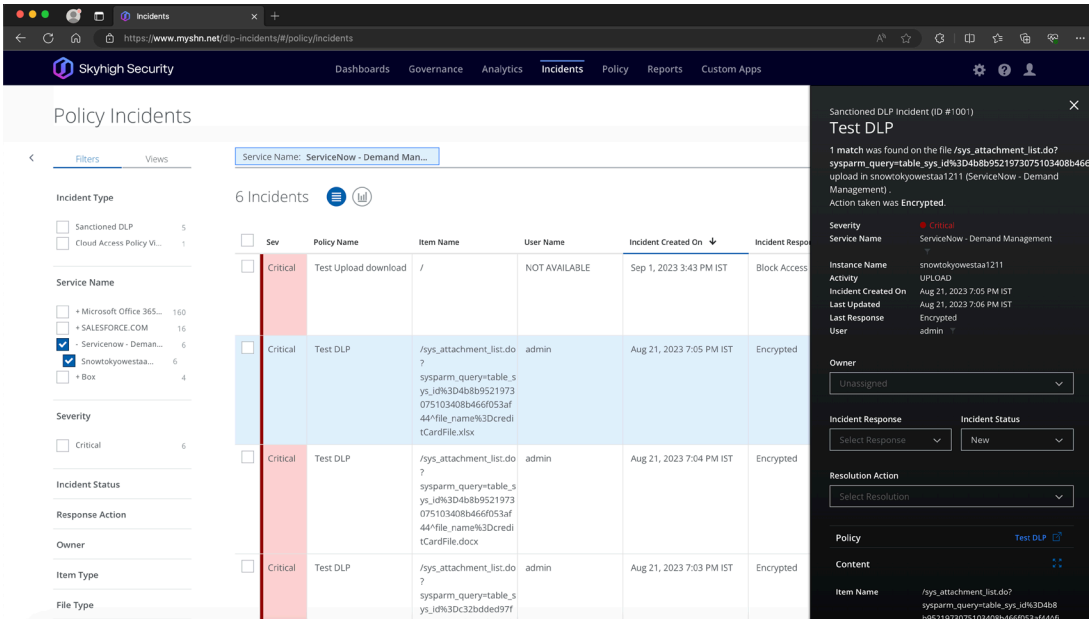
Displays an excerpt with content that triggered a violation. Enterprises, not McAfee, store excerpts, meeting stringent privacy requirements.

Structured Data Fingerprinting

Fingerprints billions of unique values stored in enterprise databases and systems of record and supports exact match detection of each value.

Unstructured Data Fingerprinting

Fingerprints sensitive files and detects exact match and partial or derivative matches with a policy-defined threshold for percentage similarity to the original.



Device-based Controls

Enforces policies based on user, managed and unmanaged device, and geography with coarse and activity-level enforcement.

Contextual Authentication

Forces additional authentication steps in real-time via integration with identity management solutions based on pre-defined access control polices.

Encryption

Delivers peer-reviewed, function-preserving encryption schemes using enterprise-controlled keys for structured and unstructured data.

Encryption Key Brokering

Integrates with enterprise key management solutions to broker the management and rotation of enterprise encryption keys across multiple ServiceNow instances.

Information Rights Management

Applies rights management protection to files uploaded to or downloaded from ServiceNow, ensuring sensitive data is protected anywhere.

SIEM/SOC Integration

Integrates with enterprise SIEM devices to deliver incidents, threats, anomalies, and audit logs.

About Skyhigh Security

When your sensitive data spans the web, cloud applications, and infrastructure, it's time to rethink your approach to security. Imagine an integrated Security Service Edge solution that controls how data is used, shared, and created, no matter the source. Skyhigh Security empowers organizations to share data in the cloud with anyone, anywhere, from any device without worry. Discover Skyhigh Security, the industry-leading, data-aware cloud security platform.

For more information visit us at skyhighsecurity.com

Skyhigh Security

3099 North First Street
San Jose, CA 95134
888.847.8766
skyhighsecurity.com

September 2023. DS-EN-000018-01