



Fortified Cybersecurity Command with Verastel SPARK



PROBLEM

Ongoing issues with identifying and managing asset configurations effectively, compounded by a lack of automated tools for real-time monitoring of these assets and their corresponding cybersecurity threats. This lack of visibility and control exposes the organization to potential security risks and inefficient resource allocation.

KEY ISSUES

- **Incomplete Security Oversight:** Creates a deceptive perception of safety due to missing or incomplete asset data.
- **Vulnerability Exposure:** Leaves gaps that are easy for cyber adversaries to exploit, increasing the security risk.
- **Resource Misallocation:** Drives focus towards low-impact issues, diluting efforts on more critical vulnerabilities.
- **Communication Gaps:** Hinders effective risk reporting and obscures the true maturity of the security program.

CONSEQUENCES

- **Organizational Risk:** Asset misconfigurations expose critical data and systems, increasing vulnerability to cyberattacks due to lack of real-time visibility.
- **Cyber Reinsurance Impact:** Inadequate asset management complicates obtaining favorable cyber reinsurance terms, potentially leading to higher premiums or coverage denial.
- **Ransomware and Phishing Risks:** Lack of automated, real-time monitoring heightens the risk of ransomware and phishing attacks by allowing cybercriminals to exploit system vulnerabilities

ADDRESSING CHALLENGES WITH



FROM



ENHANCED REAL-TIME VISIBILITY AND MONITORING:

Verastel SPARK provides comprehensive monitoring capabilities that ensure continuous visibility across both IT and OT infrastructure. This enables organizations to detect and address misconfigurations in real-time, reducing the risk of exposing critical data and systems to cyber threats.

AUTOMATED CONFIGURATION AND THREAT MANAGEMENT:

The platform automates the process of tracking and managing asset configurations and cyber threat postures. This automation extends to updating and patching systems efficiently, thereby closing security gaps more quickly and reducing the administrative burden on IT staff.

IMPROVING CYBER REINSURANCE POSTURE:

By implementing Verastel SPARK, organizations can demonstrate a robust cybersecurity management framework to insurers. This includes detailed asset management and proactive threat detection capabilities, which are critical for obtaining favorable cyber reinsurance terms. Verastel SPARK's advanced monitoring tools help in maintaining compliance and showcasing a commitment to best-in-class cybersecurity practices, potentially leading to lower insurance premiums and better coverage options.

MITIGATING RISKS OF RANSOMWARE AND PHISHING ATTACKS:

Verastel SPARK's advanced threat detection algorithms are designed to identify and mitigate ransomware and phishing threats effectively. The system uses real-time data analytics to detect anomalies and potential breaches, enabling rapid response to prevent attacks from escalating. This not only secures the organizational network but also reduces the downtime and operational disruptions associated with such cyber incidents.





PRODUCT FEATURES



COMPREHENSIVE RISK MODELING

Device classification and standards-based policy configurability for risk and vulnerability assessment



REAL-TIME THREAT DETECTION

Continuous monitoring of risks based on chosen standards, criticality and ROI driven scoring



MISCONFIGURATION DETECTION

Proactive detection of policy violations and prescriptive config change management



PROFILING AND ROOT CAUSE INFERENCE

Automated code evaluation to identify problematic component; high level to individual device config trend analytics



AUDIT AND CUSTOM REPORTING

Generate custom reports for risk and compliance to fulfill SOX, HIPPA, PCI and other audits



API INTEGRATIONS

Device classification and standards-based policy configurability for risk and vulnerability assessment



ALERTING AND EMAIL INTEGRATION

Email, SMS and in-application alerting mechanisms providing real-time visibility



CLOUD AND ON-PREM SUPPORT

360-degree infrastructure and network monitoring for both on-prem and cloud ecosystems

TAKE GUESS WORK OUT

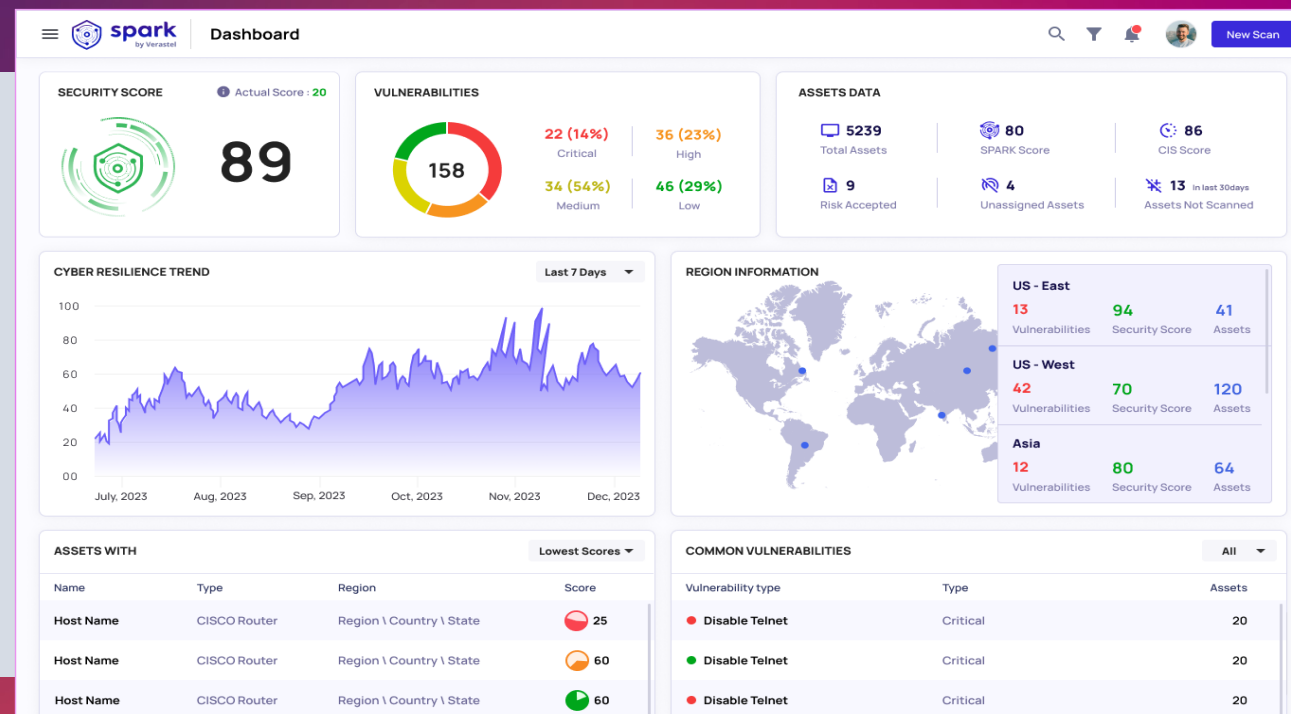
3 CLICKS TO ROOT CAUSE

EXPEDITED REMEDIATION,
RESILIENT RISK POSTURE



HOW YOU CAN BENEFIT?

Verastel SPARK equips organizations with the tools needed to build a fortified cybersecurity command center. By enhancing visibility, improving compliance and insurance interactions, and proactively addressing cyber threats, Verastel SPARK turns cybersecurity management into a strategic advantage, safeguarding assets while ensuring operational continuity and resilience.



Impact on ROI

Save Time
Automates vulnerability management and compliance checks, reducing manual tasks for IT teams

Save Cost
Reduces risks of breaches and fines from non-compliance

Save Resources
Allows teams to focus on strategic initiatives rather than reactive troubleshooting



Ready to elevate your cybersecurity strategy? Reach out to our team at josiahd@eficens.com to learn more about how SPARK can transform your security and compliance posture

