At-a-Glance

Big Data Discovery for Security Analytics on Cisco UCS with Platfora

Maintaining infrastructure and data security has never been more challenging. Today’s networks extend beyond traditional walls and include data centers, endpoints, virtual environments, branch offices, and the cloud. They constantly evolve and spawn new attack vectors, including mobile devices, web-enabled and mobile applications, hypervisors, social media, web browsers, home computers, and an increasing number of smart devices. By 2020, 50 billion connected, data-producing devices will dramatically increase an enterprise’s potential attack surface.

Mitigation of security risk in today’s advanced threat environment is a race against time. Advanced threats are often long-term efforts in which a hacker can appear like a normal user. To identify a threat, security analysts need to search massive quantities of security, business, and operational data to recognize anomalies as well as the sequence of the attack. But, they face significant challenges that limit their effectiveness and productivity:

• **Complexity and fragmentation**—Most enterprises use more than 50 different security solutions which are not designed to work together, creating silos of information and obstacles to visibility and speed of threat detection and response.

• **Traditional SIEMs are insufficient**—Today’s SIEMs (Security Incident Event Management system) lack the flexibility to adapt to a dynamic security environment, analyze multistructured data, retain adequate historical data, and deliver the scalability and performance required to support enterprise-scale security analytics.

• **Inefficient, ineffective security investigation processes**—Security analysts must use multiple tools to access and correlate silos of data and write proprietary code to identify patterns. Using Hadoop for these tasks requires significant, rare MapReduce coding and data modeling expertise.

---

**Highlights**

- Dramatically accelerate threat discovery with a dynamic, end-to-end security platform that transforms and connects multistructured data, analyzes petabytes of data at scale in memory, and more quickly offers insight through rapid data iteration and sophisticated visualization techniques.

- Complement your existing investment in security and analytics solutions, delivering comprehensive, continuous visibility to massive quantities of data that is easily stored and retrieved from a single Hadoop repository.

- Support enterprise-scale security analytics with massive scalability, outstanding performance, and low total cost of ownership (TCO) to efficiently keep pace with growth in data and in the number of simultaneous users.
Dramatically Accelerating Discovery of Targeted Attacks

The Cisco Unified Computing System™ (Cisco UCS®) and Platfora provide a security analytics solution that dramatically accelerates the detection of targeted attacks with a high-performance, scalable solution that speeds discovery of insights, patterns, and anomalies across petabytes of security, application, business transaction, operational, and device data. The solution:

• Uses Hadoop as the single data repository to provide comprehensive visibility of all security, business, and operational data—both real-time and historical.
• Is built natively on Hadoop and uses high performance scale-out technologies including Spark, YARN and MapReduce to analyze petabytes of data at scale.
• Allows security analysts can to investigate incidents related to:
  - Inappropriate/unusual use of enterprise resources by employees
  - Externally-sourced enterprise access attempts correlating to targeted threats
  - Identification of unusual data infiltration and exfiltration patterns
  - Device communication anomalies indicating operational or security-related threats
• Platfora’s ability to accelerate incident identification, containment, and remediation not only reduces security risk, it also reduces labor costs associated with those activities.

Analytics software can only perform as quickly as the infrastructure it is running on. Cisco UCS is a powerful and efficient foundation to help security analysts win their race against time.

• Industry-leading scalability is essential to keep pace with the large volumes of real-time and historical security and nonsecurity data that are critical to threat detection. The Cisco UCS portfolio can scale up to 6,000 servers, so enterprises can be confident that they can scale to support the massive quantities of data required for effective security analytics today and tomorrow.
• Enterprises require consistently outstanding performance to support large quantities of complex, forensic searches and growing numbers of simultaneous users. Cisco UCS delivers industry-leading performance that has been proven in more than 100 world-record benchmarks, including the TPCx-HS benchmark for big data performance. Real-world customers have seen Cisco UCS deliver reliably outstanding performance for Platfora environments with large volumes of analysts simultaneously investigating petabytes of security data resident in Hadoop.
• Cisco UCS’ innovative design helps customers maintain a low TCO, reducing the need for cables and switches by 77 percent, power and cooling costs by 54 percent, and management costs by 61 percent compared with traditional servers.

© 2015 Cisco and/or its affiliates. All rights reserved.
Extend the Power of Existing Security and Analytics Solutions

Security Analytics on Cisco UCS with Platfora is an excellent complement to your existing security and analytics solutions. Use of Hadoop eliminates the fragmentation and complexity caused by use of multiple security solutions, creating a single, scalable repository to collect and retain security data—as well as the business and operational data that security products are not designed to analyze. And by using Hadoop to integrate with other analytics software you’re already using, you can add the benefit of Platfora’s advanced big data discovery capabilities to the functionality delivered by those solutions.

Next Steps

Security Analytics on Cisco UCS with Platfora can help you detect—in just hours or days—advanced threats that used to take you weeks or months to find. To accelerate deployment and reduce risk, Cisco and Platfora developed a reference architecture that specifies the optimal configuration of Platfora on Cisco UCS servers. Platfora also has a 2–4 week structured pilot process that includes a customer trial with their own live data—providing insights into patterns they can act on immediately. And visit www.cisco.com/go/bigdata to learn more about the value of Cisco UCS for your big data and analytics deployments.