Data Sheet

NTT Security ActiveGuard® Investigator

Cloud-Based Raw Log Search

ActiveGuard Investigator (AGI) provides cloud-based, real-time access to raw log data to enable efficient investigations and support security, IT and business initiatives. Accessible through the ActiveGuard Portal, AGI is available as a value-added service for our Security Log Monitoring and Log Management clients.

Cloud-Based Raw Log Search

Organizations develop a lot of information from the systems in their IT infrastructure. In many cases, however, those logs are difficult to access, require support from IT staff and are only used in the event of an audit or security incident. With easy access and fast search capability, that log data can become an asset for the security team, the IT team and the rest of the organization.

Forensically-Sound, Raw Log Storage

As ActiveGuard collects and analyzes logs, it also archives a copy of the raw logs in a secure, cloud-based and forensically-sound repository. AGI provides online access to those raw logs through the ActiveGuard Portal without the need for additional on-premise equipment or an up-front capital investment.

This accessibility enables data-mining of the logs for efficient security and compliance incident investigations. It also supports the measurement of security controls, IT programs and business adoption. Search results can be filtered and mass exported to .XLS format for further analysis.

Enable Efficient Investigations

Incident investigations require fast, efficient access to needed log data. Too often, this involves manually pulling logs from multiple sources to be analyzed. This process can waste precious time and may involve understanding and accessing multiple interfaces to get to the required log data.

AGI provides a single source to access raw logs, allowing the security team to immediately investigate incidents instead of spending time locating and accessing necessary logs.

Support Security Initiatives

Security teams can use raw log data to track the implementation and effectiveness of new security and compliance controls. With the fast, easy search capability of AGI, security teams are able to easily access this information to help measure the security and compliance program.

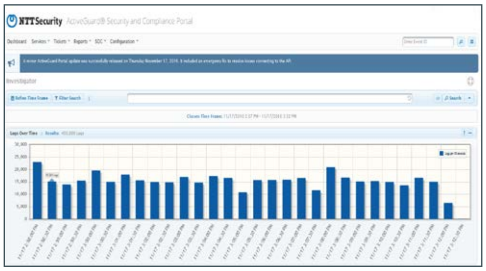
Uncover Hidden Value

IT and business organizations can realize tremendous value by mining the log data gathered to meet security and compliance needs. This can evolve to be a source for business analytics, allowing the security investment to be more of a business enabler. Data-mining the raw logs allows IT and business teams to troubleshoot, monitor performance and measure the adoption of new tools, technologies and services.

Big Data Infrastructure

AGI is built on a big data infrastructure, including Hadoop™ for storing large data sets, MapR™ for efficient queries, Elasticsearch® for indexing and Apache Lucene™ for simple and complex searches. These components allow for fast, flexible searches, delivering query results in seconds. Users can create queries using Boolean and wildcard searches.

Because the log data is stored in a cloud-based, centralized repository, NTT Security is also able to perform global analytics to develop insight into emerging threats, rolling probes and attacks, and ongoing trends.



Features Include:

- Cloud-Based, Real-Time Access to Raw Log Data
- Accessible Via the ActiveGuard Portal
- Big Data Infrastructure for Fast, Efficient Searches
- Fast, Easy and Flexible Log Search
- Iterative Drill-Down Capability
- Forensically-Sound Log Storage
- Export Search Results to .XLS

Add-On Services:

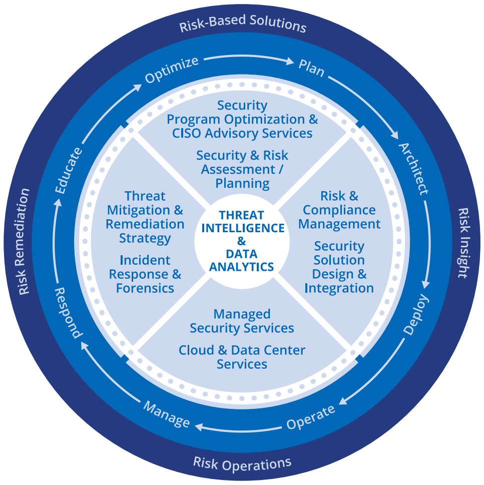
- Professional Services

A Partner You Can Trust

We don't believe that one size fits all. That's why we deliver a cybersecurity, risk management and compliance program that is as unique as your business. Our goal is to ensure that every organization develops the cyber resilience required to make the most of every business opportunity. We can provide the solution you need in the manner best suited to your specific situation and help you to avoid technical blind alleys, missed exits and roads that lead to nowhere.

The Full Security Life Cycle

NTT Security has created a Full Security Life Cycle model based on many years of providing efficient and effective security, risk and compliance services to organizations around the world. We deliver these services using local resources that leverage our global capabilities.


Risk-Based Solutions
Risk Insight
Risk Operations
Risk Remediation
Optimize
Plan
Architect
Deploy
Operate
Manage
Respond
Educate
Security Program Optimization & CISO Advisory Services
Security & Risk Assessment / Planning
Risk & Compliance Management
Security Solution Design & Integration
Managed Security Services
Cloud & Data Center Services
Threat Mitigation & Remediation Strategy
Incident Response & Forensics
THREAT INTELLIGENCE & DATA ANALYTICS

Plan & Optimize

We'll build a plan that considers your level of risk, potential regulatory and financial impact, ICT environment and staff capabilities; and work with you to optimize your existing security and compliance processes and controls. With a focus on enabling meaningful success criteria, budget and specific solutions to be implemented, our recommendations may range from a straightforward review and suggestions for improvement, to a study of alternative or supplementary solutions.

Architect & Deploy

Getting the most value from security solutions requires experience and expertise in both market-leading technology and delivering change, to reduce risk and make new implementations work seamlessly with your organization's business processes. Our security experts have the training and experience to ensure the right solutions are architected, configured and deployed to solve your security challenges.

Manage & Operate

High-performing security and compliance programs are built on processes and controls that are executed efficiently and consistently while producing the data necessary to monitor and manage their effectiveness within your organization. Effectively managing and operating the controls in your security and compliance program will increase your organization's understanding of your security posture, security and compliance exceptions, effectiveness of controls, and demonstrate cost-effectiveness to executive management.

Respond & Educate

Cyber resilience is based on the premise that incident avoidance is not always possible – you need to be ready and able to effectively respond to a security incident. Should the worst occur, our incident response team can be quickly engaged either remotely or on site. They will identify, document, contain and remediate a security incident to minimize the impact to your organization. We can also develop a comprehensive program for the security education of your organization.

The NTT Security Difference

We provide the necessary services across the entire information and communications technology (ICT) stack and throughout the Full Security Life Cycle. Our services portfolio covers every aspect of information security and risk management, from initial assessment through to strategic program planning, hands-on deployment and around-the-clock management and support. Service options include:

- Security Program Optimization and Enterprise Advisory
- Security Planning and Risk Assessment
- Risk and Compliance Management
- Security Solution Design and Integration
- Managed Security Services
- Cloud and Data Center Services
- Threat Mitigation and Remediation Strategy
- Incident Response and Forensics

Get Started Today

See how NTT Security can help optimize security, improve efficiency and ease compliance. Contact NTT Security (US) today at us-info@nttsecurity.com or visit our website: www.nttsecurity.com.

About NTT Security

NTT Security seamlessly delivers cyber resilience by enabling organizations to build high-performing and effective security and risk management programs, with controls that enable the increasingly connected world and digital economy to overcome constantly changing security challenges. Through the Full Security Life Cycle, we ensure that scarce resources are used effectively by providing the right mix of integrated consulting, managed, cloud, and hybrid services – delivered by local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest information and communications technology (ICT) companies in the world. For more information, visit **www.nttsecurity.com.**