HITACHI
Inspire the Next

THE ARKANGEL PLATFORM

INTELLIGENT SECURITY

ArkAngel is the single pane of glass through which to view your entire organizational security posture. This platform unifies the various types of technical security data along with tools for translating those inputs into clear information about business risk, divided in relevant categories and scored with probability down to the individual asset level. ArkAngel is technology-agnostic, meaning that it can accept any data source that produces textual output. It brings together logs from various security controls, along with vulnerability scan results and intrusion detection and any other security-relevant data that you have in your environment.

While many tools are purposely built to be generalized to any organization and thus require a year (or years, in certain cases) of configuration to tune properly, ArkAngel was built in-house specifically to support our own security practice. It facilitates the expert analysis of our Information Security Analysts by unifying all of the most relevant data while simultaneously excluding the clutter of non-urgent contextual information. The end result is that we can be up and running within months, not years, and our team can catch any breaches that occur almost as fast as they occur instead of getting bogged down in an ocean on non-critical information.

RISK AWARE

ArkAngel gives you a 360 degree view of your IT risk and security posture, allowing you to monitor and manage your risk level continuously to your own defined standards.

COLLABORATIVE

ArkAngel allows our security experts to collaborate with our customers in a secure environment, protect their networks and critical IT assets and respond to threats quickly and effectively.

TECHNOLOGY AGNOSTIC

ArkAngel was designed as a technology-agnostic tool that monitors all and any of your security devices and networks, ensuring that your IT environment is secure at all times.

INTELLIGENT

The automated log and security event correlation from distributed devices facilitates threat detection and significantly improves the efficiency of the incident response management process.

But it's not just about catching breaches. Instead we work together proactively to reduce your organization's vulnerability to attack. At Hitachi Systems Security, our approach is to work collaboratively with you to help you improve your internal security practice on an ongoing basis.

The platform contains tools for unifying log monitoring and vulnerability management and immediately feeding that into clear risk management data based on continual review and guided improvement of your internal security practice. The system makes continuous suggestions for improvement to security and can even warn you of assets that might be vulnerable to new Zero Days as they are discovered before we even scan for their presence.

- **ALWAYS ON**
  Nagios hardware and network monitoring verifies the health of all sensors and components, informing Analysts immediately if any service degrades. Each of ArkAngel's running services reports once a minute so Analysts will know immediately if any of them stop. There are safeguards in place to ensure transmission of relevant data even in the event of network failure. Finally, sensors can be set up in parallel to back each other up as needed.

- **A SINGLE PANE OF GLASS**
  The entire security operation and risk profile is visible through one unified source: the ArkAngel portal. There is no need to translate technical vulnerabilities into risk or asset values, because it is already integrated in one comprehensive panel.

- **SECURE COMMUNICATION CHANNELS**
  Access the ArkAngel Portal at all times through a secure channel—encrypted VPN requiring a login and password on a URL that only you know. Rest assured that your critical data is always available to you, but to no one else.

- **BUILT-IN RISK MANAGEMENT**
  Instead of simply reviewing your organization's incidents one by one, you can quickly evaluate your organization's security posture and apply strategic risk management principles. Our guidance on best practices will help you decrease your risk to an acceptable level within your specific business context and show you how to continually improve your organizational security posture through ongoing improvement of your internal security practice.

- **CLEAR LEADERSHIP ON BEST PRACTICES**
  The Governance Module, one of ArkAngel's key components, is based on the 20 CIS Critical Security Controls to ensure conformity with one of the most comprehensive information security control frameworks. A principal benefit of these controls is that they prioritize and focus a smaller number of actions with high pay-off results. The controls are effective because they are derived from the most common attack patterns highlighted in the leading threat reports and vetted across a very broad community of government and industry practitioners.

  That said, the Governance Module is also flexible enough to be applied to a variety of other industry-relevant frameworks and standards, such as NIST, ISO 27002, PCI DSS and HIPAA.

- **VULNERABILITY MANAGEMENT**
  ArkAngel comes optionally installed with the Saint vulnerability scanner, providing another layer of valuable information to organizations who wish to be more proactive in their security practice. This information also allows the specialists in the Security Operations Center (SOC) to further prioritize incidents because attacks can be matched against information about the suspected target's vulnerabilities.

TECHNOLOGY-AGNOSTIC DATA INTEGRATION

ArkAngel's technology-agnostic approach allows you to easily integrate with any security device in the network to collect and aggregate alerts, logs and other device-specific information. Whether they are legacy systems, virtual systems, BYOD (Bring Your Own Device) or even Cloud environments, ArkAngel integrates logs from third-party security systems such as Radware's anti-DDoS, IBM AS/400 iSeries systems, Linux/Unix Platforms, Windows Operating Systems and more.

ARKANGEL MANAGED SECURITY SERVICES

Hitachi Systems Security's Managed Security Services offer advanced protection of your most critical IT assets as well as corporate and customer data. MSS also covers a host of regulatory requirements, simplifying your path to compliance with various vertical-specific requirements such as GLBA, PCI DSS, ISO 27001, and HIPAA. Our ArkAngel Managed Security Services are customizable and flexible to adapt to your needs.

ALL PACKAGES INCLUDE THESE BASIC FEATURES:

24/7 REAL-TIME ANALYSIS AND EVENT CORRELATION – Working around-the-clock, Hitachi Systems Security's experts use the ArkAngel platform to monitor and detect system threats in real time. Sensors do packet-level inspections to consolidate and analyze alerts and logs emanating from your networks, servers, operating systems and applications. This results in hundreds of thousands of messages which are then automatically narrowed down to a few relevant security incidents. These incidents are instantly prioritized and analyzed by our security experts based on their potential impact to your operations.

UNIFIED SECURITY PORTAL – Hitachi Systems Security's ArkAngel portal offers consolidated security management of all your cyber security operations. Review your security reports, manage and respond to security incidents and threats, review your security and compliance policies and interact with our security experts. ArkAngel is your one-stop IT security solution in a highly secure environment.

INCIDENT RESPONSE MANAGEMENT – As soon as a security alert is detected, an expert Information Security Analyst investigates the alert. If the alert is determined to be a threat to your network, it will be escalated according to the parameters established collaboratively.

MONTHLY SECURITY SERVICES MEETING – At least once a month, a Senior Information Security Analyst from our SOC team will sit down in a teleconference with your internal IT team to keep the collaboration on track. This could be a review of the monthly security posture report, an overview of what happened during the month, a discussion of remediation or patching efforts or whatever else is required to keep the security of your organization on an ever-increasing trajectory.

2-HOUR LOG REVIEW GUARANTEE – Every piece of relevant security information will be reviewed by a human analyst who will create a security incident within a maximum of two hours for 95% of security incidents, often closer to half an hour in practice. Many organizations practice daily log review—this is all that is required by even strict compliance frameworks such as PCI. A lot can happen in twenty-four hours. We mitigate this considerable risk by reviewing the data continuously in a reasonable time.

15-MINUTE ESCALATION OF DISCOVERED THREAT ACTIVITY – On top of our aggressive monitoring, we guarantee escalation of threats within 15 minutes of their discovery. The form of this escalation is defined by you according to rules that are as granular as your organization requires. It could be anything from an email to a system administrator for a minor vulnerability discovered on one of their servers, to a 4 AM phone call to your CISO for serious breaches.

SELF-SERVE VULNERABILITY SCANNING – Whether or not your organization has subscribed to the Vulnerability Management service, the scanning tool is still deployed on the sensor in your environment and is available for unlimited scans through self-service. Simply log in and schedule them, or even set them up as recurring and they'll keep recurring forever with no further effort.

Regular vulnerability scans provide an extra layer of analysis that synergizes powerfully with the core monitoring services.

With a regular scanning program, it is additionally possible to:

- Establish a baseline (and thus see potentially dangerous anomalies)
- Track effects of patching and remediation efforts
- Report to management (PCI compliance)
- Identify vulnerabilities before they impact your organization

MONTHLY SECURITY POSTURE REPORT – A detailed report containing all relevant information about the ongoing threat monitoring service is created each month, starting with a high-level assessment of your security posture and descending through detailed analysis of every facet of your chosen services. The information is also presented as trends over four months so that it is possible to track the performance of your organization from various angles: number of incidents, time to resolution of incidents, overall number of vulnerabilities and others. From a Governance perspective, this permits your organization to self-audit and correct course in the early stages of less than optimal trends before they become damaging.

Every month, the report also contains an update on the security landscape with special recommendations for your organization, personally made by a Senior Information Security Analyst who works with your environment on a weekly basis, who knows how you operate and how you could do so more securely.

DEDICATED INFORMATION SECURITY SPECIALIST – We understand how important it is to have access to security experts and will assign a dedicated Information Security Specialist (ISS) to each of our managed security service customers. This way, you will have direct contact with a technical security expert who will be able to answer your questions, provide customized recommendations based on your environment and industry best practices and standards, and help you improve your security posture.