Fact Sheet
Fujitsu Security SAMURAI Platform™
(Security Advanced Monitoring and Unified Remediation with Artificial Intelligence)

Keeping up with the dynamic and constantly evolving cyber threat landscape

Keeping up with the dynamic and constantly evolving cyber threat landscape has become a major focus of resources – both from specialized technical staff and budget perspectives. Organizations don't have the capability to protect themselves from the continual and varying attacks on their systems and networks.

The Fujitsu Security Advanced Monitoring and Unified Remediation with Artificial Intelligence platform (SAMURAI) integrates the best-of-breed security industry solutions, with an OpenStack® exchange layer and Artificial Intelligence learning and management to bring the same dynamism and evolutionary capability to security incident identification and response.

Challenges

For many organizations, trying to keep ahead of the cyber threat landscape is a difficult, if not insurmountable task. Just some of the challenges they face include:

- Pressures to keep capital budgets down, while needing to upgrade their security infrastructure
- Silos of control between Network, IT and Security Management
- Tying together disparate sources of data to create a holistic view of the security landscape and environment
- Difficulties in attracting and maintaining enough trained, experienced staff who can handle security and privacy incidents quickly and effectively

Many of the available Managed Security Services vendors work in their own silos – with a particular vendor solution, or with proprietary tools which do not integrate well with the organization's infrastructure, processes or culture.

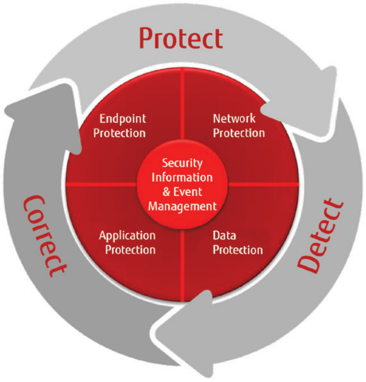
How we can help

The Fujitsu SAMURAI Platform integrates our advanced AI (artificial intelligence) with industry leading solutions from our partners to provide a complete *Protect, Detect and Correct* shield of cyber security services. The result is a "next-generation" intelligent Security Operations Center that proactively predicts and eliminates a threat and removes intruders across the total security landscape. SAMURAI helps to break down the control silos by automating and reusing knowledge around vulnerabilities and exploits all layers of the IT stack. It provides a "single pane of glass" view and configuration management (rules, signatures, etc.) of security devices such as Intrusion Detection and Prevention (IDS & IPS). The AI built into SAMURAI applies machine learning to the End-to-End SIEM platform which focuses on analysis, remediation and human/machine collaboration providing complete protect, detect and correct capability. This allows staff to focus on the extraordinary occurrences, instead of being tied up with mundane tasks. A pattern recognition engine enables a pro-active approach to security management and response.

Benefits

The benefits of SAMURAI to your organization include:

- SAMURAI will grow as you continue to grow
- No vendor lock-in as an open-API architecture enables you to integrate into the platform as your needs grow



The problem

Today's threat landscape includes over 7 million (known) cyber-attacks a day. Between ransomware, identity theft and fraud, the expected cost to users and organizations is over $100 billion per year. With the growth of sensors and other IoT devices, it is estimated that there will be over 20 billion connected devices (and possible points of entry) by the year 2020.

Organizations are finding it increasingly difficult to build the necessary protection and monitoring systems to find and neutralize these threats as the hackers and criminals find new ways to infiltrate, infect and exfiltrate valuable data. In addition, there is a global scarcity of trained, experienced staff.

- Able to bridge the gap during IT modernization as it can support your legacy systems and newer services across all layers of the IT infrastructure which enables agility. As you move to a more modern infrastructure, you can leverage the full capabilities of SAMURAI
- Implement the Protect/Detect/Correct shield at any of the 5 areas (endpoint protection, network protection, vulnerability management, compliance management or SIEM) and expand as required
- Consistent quality levels that enhance your path to compliance and reduce risk

What we offer

Fujitsu SAMURAI is a full-service, integrated, end-to-end next-generation security management offering from our global network of Security Operation Centers. It provides the full gamut of security services, including:

- Security Management
- Endpoint Protection
- Endpoint Detection and Response
- Data Security
- Network Security
- Web Security
- Threat Intelligence
- Threat Sandboxing.

Best of breed, industry vendor solutions from our partners are integrated and managed by state-of-the art, Fujitsu testing AI engines, which provides both forensic and pro-active security management capabilities. In addition, the open architecture of the design allows the SAMURAI solution to work with clients' existing security infrastructure.

How it works

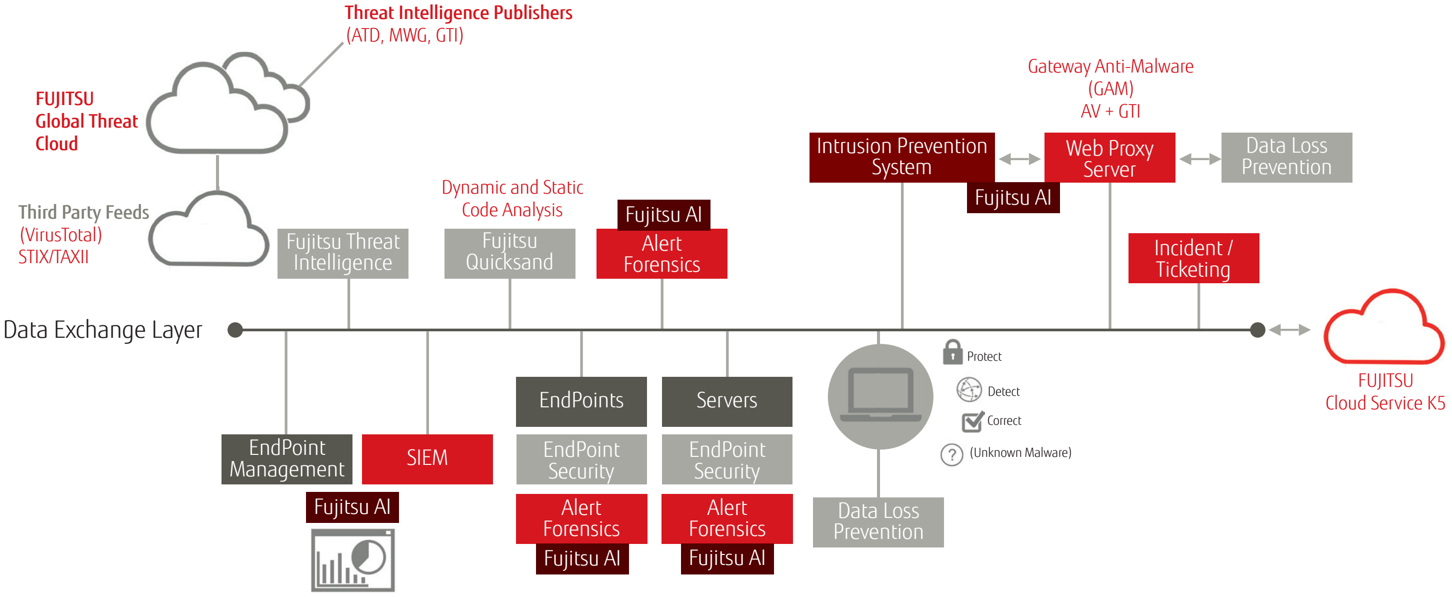
SAMURAI starts with an open-source standard data exchange framework, which allows for the integration, communication and management of information between the various security services.

Using this framework, the components of the solution platform are able to communicate and share information regarding threats and appropriate responses, including access to our global Threat Cloud, consisting of input and threat signatures from multiple vendor, industry and governmental sources. Coupled with the AI engine, SAMURAI is able to learn how common threats and situations are handled and begin the process of automating the responses – relieving humans of the need to deal with mundane, repetitive tasks, and allowing them to focus on the new, extraordinary situations.

While the SAMURAI offering encapsulates a full suite of end-to-end security capabilities, SAMURAI can be approached in two ways – as a full service end-to-end offering, or a modular approach. Fujitsu understands that organizations and their security needs are different – reflecting different approaches, risk tolerances and cultures. Because of the open architecture of SAMURAI, it can be tailored to meet organizational requirements – picking only those elements required, integrating them with existing processes and tools – and allowing for growth as the organization evolves into further levels of security maturity.

Why Fujitsu?

The Fujitsu SAMURAI platform breaks down the silos between networking, IT, and security by automating and reusing knowledge around vulnerabilities and exploits all layers of the IT stack. Its machine learning, end-to-end SIEM platform focusses on analysis, remediation and human/machine collaboration. SAMURAI uses open-source architecture which allows it to operate in a multi-tenant, legacy, and/or hybrid environment, while being completely IoT support ready. The Pattern Recognition engine built into the AI component enables a proactive approach to security management.



About Fujitsu Americas

Fujitsu America, Inc. is the parent and/or management company of a group of Fujitsu-owned companies operating in North, Central and South America and Caribbean, dedicated to delivering the full range of Fujitsu products, solutions and services in ICT to our customers in the Western Hemisphere. These companies are collectively referred to as Fujitsu Americas. Fujitsu enables clients to meet their business objectives through integrated offerings and solutions, including consulting, systems integration, managed services, outsourcing and cloud services for infrastructure, platforms and applications; data center and field services; and server, storage, software and mobile/tablet technologies. For more information, please visit: http://solutions.us.fujitsu.com/ and http://twitter.com/fujitsuamerica

Digital Transformation

New digital technology is becoming incorporated into the heart of business and society. Digital is not a single technology, rather a set of connected technologies such as cloud, mobile, Internet of Things (IoT), analytics, Artificial Intelligence (AI) and supporting security technologies.

Digital technology can radically transform how the world works. For instance, a manufacturer can leverage a connected, digitalized production line to gain a real time view of its operations, and make changes more quickly, transforming its efficiency. Connectivity greatly reduces transaction costs, and therefore improves the bottom line. Digital technology fundamentally changes an organization, how it operates and how it creates value. Digital transformation is metamorphosis. A core change, not a cosmetic change or an extension. A reconfiguring of a business to provide higher value products or services.

Digital technology has grown through four major waves of development. The first wave, the internet, made computing technology available to all, and was the first platform for digital services. The mobile internet followed by making digital services accessible anywhere.

Find out more at:
http://www.fujitsu.com/us/vision/digital-transformation/

More information

For more information, please visit:
www.fujitsu.com/us

Disclaimer

Technical data are subject to modification and delivery subject to availability. Any liability that the data and illustrations are complete, actual or correct is excluded. Designations may be trademarks and/or copyrights of the respective manufacturer, the use of which by third parties for their own purposes may infringe the rights of such owner.

Fujitsu green policy innovation

Fujitsu Green Policy Innovation is our worldwide project for reducing burdens on the environment. Using our global know-how, we aim to resolve issues of environmental energy efficiency through IT. Please find further information at: www.fujitsu.com/global/about/environment/

Copyright

The statements provided herein are for informational purposes only and may be amended or altered by Fujitsu America, Inc. without notice or liability. Product description data represents Fujitsu design objectives and is provided for comparative purposes; actual results may vary based on a variety of factors. Specifications are subject to change without notice.

FPC65-7745-03 06/17
17.0626.0325bh

Contact
FUJITSU AMERICA, INC.
Address: 1250 East Arques Avenue Sunnyvale, CA 94085-3470, U.S.A.
Telephone: 800 831 3183 or 408 746 6000
Website: www.fujitsu.com/us
Contact Form: www.fujitsu.com/us/contact

Have a question? Email us at: AskFujitsu@us.fujitsu.com