Context Aware Security Intelligence
Table of Contents

Security Industry Overview ................................................................. 3
Main Providers of Context-Aware Security Products .............................. 4
BeyondTrust: Company Background .................................................. 5
Conclusion ...................................................................................... 5
About BeyondTrust ........................................................................... 7
Security Industry Overview

In a world where rapid IT expansion must adapt to the requirements of cloud computing amid the risks of increasingly sophisticated cybercrime, enterprises of all sizes are rethinking their IT security. Gartner has predicted that one of the newest preferred methods of implementing IT security will be through the use of a context-aware methodology. These new security technologies will allow enterprises to cope with emerging threats as they evolve their business requirements for greater openness. Neil MacDonald of Gartner described context-aware security as the use of supplemental information to improve security decisions at the time they are made, resulting in more accurate security decisions capable of supporting dynamic business and IT environments.

Vendors of cutting edge endpoint, network, application and data protection platforms are starting to incorporate context into their security information and event management platforms. Gartner recommends that chief information security officers begin migrating to context-aware and adaptive security infrastructure as they replace legacy and static security infrastructure.

Another vital recommended change is the removal of hard-coded, static security policies from applications and systems, and their transformation to externalized security policy enforcement points capable of consuming real-time context information.

Joseph Feiman, Vice President of Gartner, emphasizes the importance of being adaptive as it relates to IT infrastructure. Additional context during security decision making is now beginning to appear in next-generation endpoint, application, network, data protection platforms security information and event management.

The concept of context aware security is not new. As early as 2002, Michael Covington presented the IEEE paper A Context-aware Security Architecture for Emerging Applications. He describes an approach to creating security services for context-aware environments very much foreshadowing today's emergent product architectures. In his design approach discussions, he focuses on security services incorporating the security-relevant context, making policy enforcement and access control flexible within a system-level service architecture. Inherent components in this concept of context-aware security services are enhanced authentication services, flexible access control and an adaptable security subsystem responding to current conditions in the environment.

A DARPA supported CMU project on context sensitive security resulted in the paper, Interleaving Semantic Web Reasoning and Service Discovery to Enforce Context-Sensitive Security and Privacy Policies by Jinghai Rao and Norman Sadeh.

Increased Web use by both individuals and organizations now demands a more robust security policy with flexible means of enforcement. Enterprises must meet an emerging need to selectively grant access to sensitive information based on dynamic relationships, or restrict information sharing under certain conditions. These new, vital access requirements require context-sensitive security and privacy policies; policies that are inherently variable and cannot be defined in a static model. They are challenging to implement for the following reasons:

- Sources of information available to enforce these policies may vary from one entity to another. For example, it's likely that different users will have a variety of sources of location tracking available depending on cell phone operators.

- Existing sources of information for the same principal can change with time.

- Available information sources may not be known in advance. As a result, enforcing context-sensitive policies in open domains requires the ability to dynamically incorporate policy reasoning with dynamic identification and access to relevant sources of contextual information.
Main Providers of Context-Aware Security Products

Only one of the leading security providers offers a comprehensive suite of context aware security products, and that is BeyondTrust. The following is a brief list of security product features other major security vendors offer that are related to this topic:

- Context aware firewall services and secure remote access services.

- A major hardware firm is now working on a framework for next-generation context-aware computing. The company is in the process of discovering what it will take to identify commonalities between studies and to create a general framework for context aware computing utilizing known cloud and database techniques. Asking how applications and systems can be contextually adapted to improve performance is one of the goals. This vendor does not currently have a context aware security product.

- Software for consolidating threat, risk and event data to provide security intelligence, timely incident response and ease of log management compliance reporting is available but not as a context aware security solution.

- One firm combines real-time threat prevention with a comprehensive URL database and application identification. It limits unauthorized data and file transfers, detects and blocks malware as well as targeted and unknown threats. It provides some context aware security features. Context aware network security products are available.

- Cloud-based security, context-aware data protection and mobile device management are available from one company.

Though some of the other leading security firms offer some partial context aware security solutions, only BeyondTrust has a complete suite of security products with this superior trending technology. Furthermore, only BeyondTrust can generate unmatched operational efficiencies and reduce the number of hours spent in performing security based tasks.

BEYONDTRUST

Through Context Aware Security Intelligence, BeyondTrust’s products provide the ability for enterprises to effectively take command of their information and systems’ security throughout the entire IT stack including Unix, Linux and Mac OS X servers, Windows desktops and servers as well as mobile devices and the cloud. User permissions can be efficiently and seamlessly managed down to the most granular level. Our tools empower IT teams through a consistent platform that helps them accelerate their decision-making, risk reduction and compliance reporting. Having the integrated environment provided by our Retina CS product, for example, frees teams of cumbersome multi console, multi-application security management tools.

Immediate, effective response to cyber threats requires immediate, reliable intelligence. Products embedded within an enterprises’ information and systems security suite provide the fastest, most efficient way to address this time critical need. IT systems and security staff must quickly make decisions, select and deploy the correct countermeasures and monitor their effectiveness. Retina Insight supports this dynamic response environment, by providing teams with instant analysis of risk posture, attacks, patch processes, privileges and compliance activity.

Using Retina Insight, teams can quickly view, correlate and analyze the risk management lifecycle across information and systems’ assets. This information is critical in gauging vulnerability and response to cyber-attacks, threat levels and the potential enterprise-wide impact of breaches. The information from Retina CS is also invaluable in providing immediate, comprehensible access to the security data necessary for threat and risk assessments.

THE INSIDER THREAT

Organizations must protect themselves from insider threats which menace them from within. Current employees, former employees, businesses and contractors having inside information connected with security practices, computer
systems or data are potential enemies. Insider threats can result in substantial monetary losses and controls should be set in place to mitigate insider opportunities. Intellectual property loss, damages caused by fraud, and destruction of information resources can all be averted by the right control measures.

Organizations are encouraged to extend their existing insider security infrastructure, policies and compliance reporting to their private clouds, hybrid clouds and public clouds. To the end, BeyondTrust has collaborated with Symplified to provide customers with a security foundation that incorporates access control and policy enforcement against insider threats in the cloud.

BeyondTrust’s, PowerBroker product received the platinum distinction in the IT software/hardware category for the 2012 Govies Government Security Awards from Security Products Magazine. The PowerBroker portfolio assists in the creation of privilege environment within government agencies and other enterprises to reduce the risk of insider threats. BeyondTrust has developed a single user-interface and data repository for privileged identity management across Linux/Unix and Windows in servers, desktops, applications, databases and devices in virtual and traditional environments.

**BeyondTrust: Company Background**

Many security focused companies are currently in the conceptual and design phases of context aware security. BeyondTrust, though, is the only security solution vendor actually providing Context-Aware Security Intelligence today. BeyondTrust customers receive the visibility and controls necessary to reduce their IT security risks, while at the same time simplifying their reporting.

We ensure that our customers are empowered to protect their infrastructure and data across the entire IT landscape by making every device, regardless of location, as secure as possible. Our solutions identify and remediate the vulnerabilities that are the nucleus of cyber-attacks and mitigate internal threats that arise from the accidental or intentional misuse of system or device privileges. We protect from both external and internal threats.

BeyondTrust offers consistent policy-driven vulnerability and privilege management, role-based access control, monitoring, logging, auditing and reporting to protect internal assets from the inside out. The company’s products empower IT and security personnel alike to strengthen security, improve productivity, drive compliance and reduce expense across physical, virtual, mobile and cloud environments.

PowerBroker and Retina product lines provide:

- Intelligent, context-aware security of systems, people, and data
- Integrated protection for both internal and external threats
- Comprehensive logging and reporting for security and compliance auditing purposes

By using our products, our customers can certify compliance initiatives with clarity.

Visit us at BeyondTrust to see how our solutions can help you.

**Conclusion**

Today, attacks against your organization are much more likely to be targeted, stealthy and slow moving. Starting with an initial compromise through targeted e-mail or Web attacks, sophisticated attackers move laterally and quietly within your organization, exploiting employees’ access permissions, misconfigured servers and weakly protected assets to obtain sensitive data, including customer information, financial records and intellectual property. In the coming years, security investments need to shift and focus more towards the context of the event, instead of simply continuing to add
layers of perimeter defenses. BeyondTrust’s context aware security measures provide scalable, adaptable solutions to help counter the ever-evolving dangers of cyber threat and cybercrime.

BeyondTrust offers a wide range of security and compliance solutions for your network needs, including Least Privilege, Vulnerability Management, and Endpoint Protection. Targeted solutions for your Active Directory identify operations and actionable threat intelligence. We bring you the intelligence and information you need to improve your security decision making process.

Context is an essential factor differentiating BeyondTrust from other solutions; this Context-Aware Security Intelligence is derived from our security tools and provided to IT/security staff in order to maintain continuous availability of intelligent data for informing protection strategies.

Our two security solution suites are Privilege Identity & Access and Enterprise Vulnerability Management. Our Context Aware Security Intelligence is based on these products. Our security and compliance solutions are comprehensive and include end user privilege assignment, device security and remediation, and directory compliance and auditing. Here are four ways in which your IT organization and management can benefit:

• IT Security – leverage context in the form of actionable information used to optimize controls such as root access and/or privilege or machine’s network access based on active threats which may impact your enterprise.

• Management –Those in management are able to better prioritize investments, accelerate or decelerate deployment schedules and better allocate resources.

• IT Operations – The context we provide answers one of the most basic of questions in IT: how to intelligently prioritize critical work. As the front line of risk reduction for the organization, the positive impact to overall security and operations health is a significant contributor to ROI.

• Team members in Risk and Audit/Compliance can automate their reporting requirements and easily identify noncompliant areas.

BeyondTrust’s context aware security measures provide scalable, adaptable solutions to help counter the ever-evolving dangers of cyber threat and cybercrime and to meet the needs of security and compliance effectively.
About BeyondTrust

With more than 25 years of global success, BeyondTrust is the pioneer of Privileged Identity Management (PIM) and vulnerability management solutions for dynamic IT environments. More than half of the companies listed on the Dow Jones Industrial Average rely on BeyondTrust to secure their enterprises. Customers include eight of the world’s 10 largest banks, seven of the world’s 10 largest aerospace and defense firms, and six of the 10 largest U.S. pharmaceutical companies, as well as renowned universities. The company is privately held, and headquartered in Carlsbad, California. For more information, visit beyondtrust.com.

CONTACT INFO

NORTH AMERICAN SALES
1.800.234.9072
sales@beyondtrust.com

EMEA SALES
Tel: + 44 (0) 8704 586224
emeainfo@beyondtrust.com

CORPORATE HEADQUARTERS
550 West C Street, Suite 1650
San Diego, CA 92101
1.800.234.9072

CONNECT WITH US
Twitter: @beyondtrust
Facebook.com/beyondtrust
Linkedin.com/company/beyondtrust
www.beyondtrust.com