Brochure

Security

Protecting the Digital Enterprise

MICRO FOCUS

Table of Contents

page

The transition to the cloud, the embrace of Big Data, and the expansion of mobility and the Internet of Things (IoT) have had a positive impact on businesses and the IT architectures that support them. While these technologies increase organizational productivity, they do so by making applications and data more accessible and often more insecure.

Enterprise security has not kept pace with this innovation, as traditional efforts of protecting critical assets have remained focused on locking down users and limiting their access to applications and data. Meanwhile, the costs associated with cybercrime, the numbers of successful attacks organizations suffer per year, and the costs to contain security incidents—all continue to rise.

Such trends show that focusing on the perimeter is a strategy that simply can't contend with the modern threat landscape—one where users are no longer tethered but interact with data and applications in the cloud, on mobile devices, and across your network. IT security has unfortunately entered an era where organizations must make the assumption of compromise, and then be able to respond accordingly.

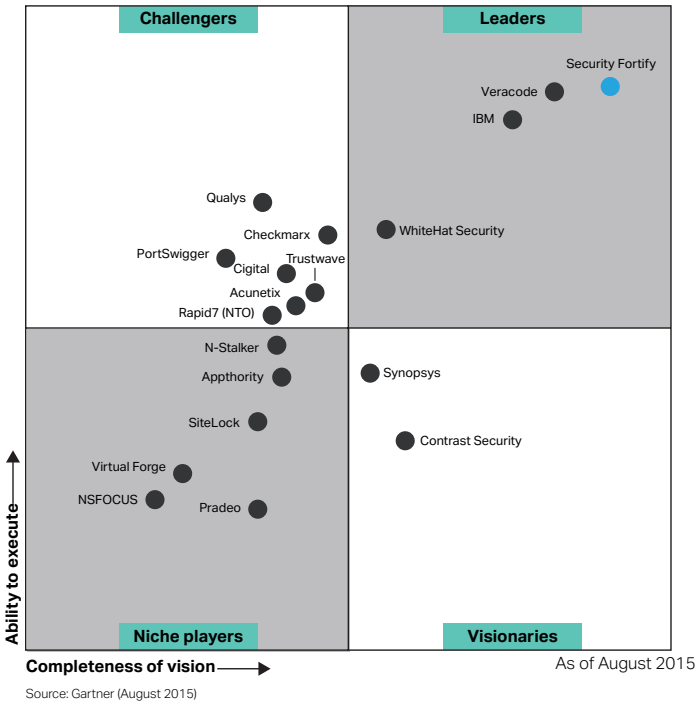

Figure 1. Gartner (August 2015)

Micro Focus® Security supports a new approach that fundamentally builds in protection from the ground up and focuses on protecting the interactions between users, applications, and data, no matter where they occur.

Prevent

To prevent means moving protection away from the perimeter and closer to the data itself. That means utilizing encryption on a variety of levels and focusing on the number one cyber-attack vector—applications.

Application Security with Micro Focus Security Fortify

If an insider does not compromise on network security, then it's likely that it is happening via an application. Applications are available by design, which makes them inherently prone to attack. In fact, applications have dissolved the traditional perimeter and introduced more nuanced risk to the enterprise. Micro Focus Security focuses on Software Security Assurance, a systemic, programmatic approach to securing applications that relies on finding and fixing security vulnerabilities throughout the lifecycle of an application. This approach includes implementing secure coding practices during development, performing repeatable and scalable security testing, and utilizing continuous monitoring to scan for vulnerabilities in live systems.

Security Fortify offers a comprehensive suite of application security solutions including application security testing, software security management, and application self-protection. Managed application security testing is also available on-premise or on-demand. Security Fortify products and services that can help organizations secure their applications against attack include:

Security Fortify on Demand

With application security-as-a-service, Security Fortify on Demand enables organizations to test the application security of a few applications or launch a comprehensive security program without additional investment in software and personnel.

Micro Focus Security DevInspect

A secure coding tool that enables identification and remediation of security vulnerabilities in source code from inside the developer's environment (IDE), helping eliminate security flaws before the code is even compiled.

Security Fortify Static Code Analyzer

An automated static code analyzer that identifies security vulnerabilities in your source code; it pinpoints the root cause of the vulnerability, correlates and prioritizes results, and provides best practices so developers can code more securely.

Security Fortify Software Security Center
A centralized management repository providing visibility to your entire application security testing program. Reviews and manages security-testing activities, prioritizes remediation efforts, enables the measurement of improvements, provides reporting, and controls your enterprise security portfolio.

Security Fortify WebInspect
An automated, dynamic testing offering that identifies security vulnerabilities and prioritizes them in running applications. It mimics real-world hacking techniques and provides comprehensive dynamic analysis of complex Web applications and services.

Security Fortify Application Defender
The application self-protection service provides immediate visibility and actively defends production applications against attacks.

Software Security Research
The experts in application security who provide research insights for the latest threats and solutions. Their expertise is what informs Security Fortify technology and solutions.

Security Fortify Professional Services
Industry-leading application security consulting and Fortify implementation services. A highly skilled workforce that builds world-class application security programs around the Fortify product suite.

Micro Focus Data Security
Micro Focus Data Security drives data-centric security innovation with encryption and tokenization solutions.We enable the world's leading brands to neutralize data breach impact for data at rest, in motion and in use by de-identifying sensitive information.Data Security solves the industry's biggest challenge by simplifying data protection across com¬plex legacy and modern IT.

Scaling Big Data Security: Hyper FPE protects data streaming into data lakes with high performance, enabling analytic insights while lowering exposure to data misuse or breach. Safer, de-identified data can now offer wider access to business leaders and operations teams to accelerate new value creation and IT optimization without increasing risk as data volumes scale.

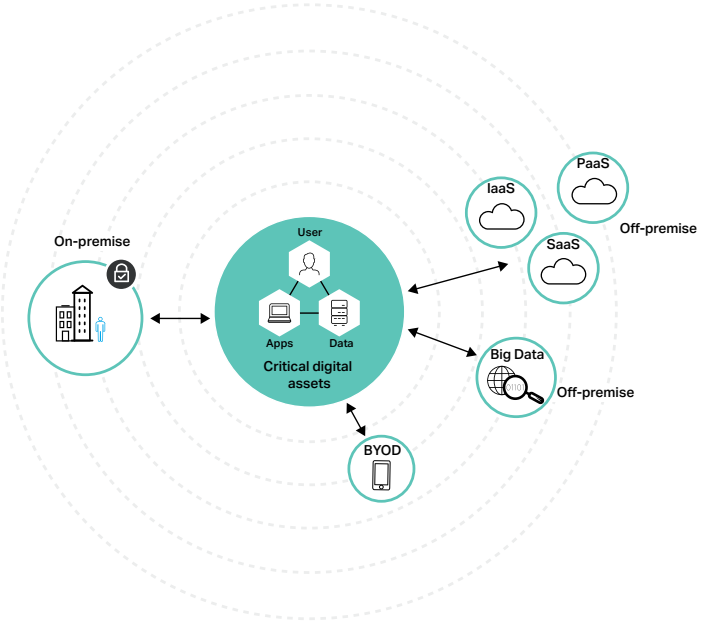

Figure 2. The expanding perimeter and increased attack surface

Reducing High Cost of Compliance: Data is de-identified using a proven, standards-based approach that can meet GDPR and similar mandates for data pseudonymization and anonymization. Format-preserving encryption and hash avoids breaking applications and processes, extending to legacy and hybrid IT. Secure Stateless Tokenization enables audit scope reduction, proven for PCI DSS, in use by leading banks, retailers and payment processors.

Securing Workloads to the Cloud: SecureData cloud-native data protection for application workloads extends from hybrid IT to include legacy on-premises. SecureData enables a platform-agnostic approach to deploying IT that transcends boundaries with a stateless architecture and transparent gateways using SecureData Sentry.

Hardware-Based Trust Assurance: Atalla HSM and Enterprise Secure Key Manager (ESKM) offer hardened security appliances, validated to NIST FIPS 140-2 security assurance, for protecting cryptographic material used in high-trust applications, including payments applications,

and storage and server media key management. Atalla HSM integrates with SecureData software appliances to enable hardware-based root of trust for protecting cryptographic secrets.

Secure Enterprise Messaging: End-to-end encrypted email for desktop, cloud, and mobile that scales to millions of users, while maintaining sensitive data (PII, ePHI, etc.) privacy. Secure communication enables organizations to confidently meet privacy compliance mandates, while lowering exposure to misuse and data breach.

Products

Voltage SecureData Enterprise
End-to-end protection using Hyper FPE and tokenization for complete data-centric security to neutralize data breach impact from point of data creation throughout the information lifecycle—in use, in motion, at rest.

Voltage SecureData for Hadoop and IoT
Enables protection of sensitive data in use for Hadoop and IoT (Kylo, Apache NiFi).

Voltage SecureData Cloud
Cloud-native approach to securing data in application workloads with consistency when migrating from legacy to hybrid IT.

Voltage SecureData Sentry
Transparent encryption using an advanced CASB approach to simplify security deployment and accelerate time to value.

Voltage SecureData Edge Protection
Voltage SecureData Mobile protects data captured on device endpoints and Voltage SecureData Web uses Voltage Page Integrated Encryption (PIE) to secure sensitive data from Web browsers.

Atalla HSM
Leading FIPS 140-2 Level 3-validated hardware security module to pro¬tect cryptographic material and enable card authentication.

Enterprise Secure Key Manager (ESKM)
Cryptographic key management to protect storage and server media infrastructure, supporting the OASIS KMIP standard.

Voltage SecureMail
Global enterprise mail encryption for employees and mobile users ex¬tending to customers and partners.

Detect and Respond
Organizations must now make an assumption of compromise and prioritize detection when an attack has occurred. That is not a suggestion to eliminate perimeter defenses (because they are vital and mostly do a good job), but instead an attempt to deal realistically with modern enterprise security problems. Simply put, blocking every attack in the era of the data breach isn't feasible. However, reducing an attacker's dwell time—the amount of time they can remain inside your defenses without detection—is paramount in limiting the damage that can occur from a successful attack. In fact, security intelligence solutions such as security information and event management (SIEM) tools offer the most powerful ROI available.

Advanced Security Analytics with Micro Focus Security ArcSight
With qualified cybersecurity professionals in short supply, IT relies on solutions that can automate key testing processes and have enough intelligence to recognize both known and unknown threats. Security experts should be able to perform accurate security testing both in terms of scale and depth, but with fewer resources at their disposal. That means employing analytics-driven intelligent solutions for the security operations team, focused on leveraging analytics, correlation, and orchestration to help proactively detect and manage breaches.

A successful security operations organization calls for a holistic approach that includes mastering the basics of security monitoring, incident detection, and breach escalation and response. Once baseline capabilities have been established, organizations can grow their security operations to leverage advanced data science, analytics, and shared intelligence to protect the digital enterprise more effectively.

Building analytics-driven intelligent security operations requires several components:

SIEM: In essence, SIEM technology is at the heart of any successful detect-and-respond program. Security ArcSight collects massive amounts of security data from an enterprise's security technologies, operating systems, applications, and other log sources and analyzes

that data for signs of compromise, attacks, or other malicious activity. Using advanced analytics to detect malicious activity, the product sends alerts to security administrators or initiates an automated response to mitigate the threat.

Threat intelligence: One advantage hackers have held for years has been simple but devastating—communication. Decades ago, hackers created a society of sharing to trade new exploits for status. Now those networks have morphed into an underground marketplace where both exploits and enterprise security weaknesses are for sale. Micro Focus Security counters this problem in several ways.

One is by utilizing threat intelligence—crowd-sourcing vulnerable information, Micro Focus Security Threat Central can provide reliable threat intelligence to help users detect attacks faster and more accurately. Micro Focus Threat Central enables enterprises to collaborate via a community-sourced security intelligence platform that incorporates dynamic threat analysis scoring, producing relevant, actionable intelligence to combat advanced cyber threats.

Micro Focus Security ArcSight offers next-generation cyber defense through security and compliance analytics. Offerings include:

Security ArcSight Data Platform
Collects comprehensive security Big Data and is a massively scalable high-performance data collection and storage engine that forms the basis for searching, reporting, alerting, and analysis.

Security ArcSight Enterprise Security Management
Combines event correlation and security analytics to identify and prioritize threats in real time, and remediate incidents early.

Security ArcSight Express
Provides security event correlation and compliance in an all-in-one entry-level SIEM appliance.

Security ArcSight User Behavior Analytics
It delivers insight, in conjunction with ArcSight SIEM, into the highest-risk users, aggregating activities, and multiple indicators of compromise.

ArcSight DNS Malware Analytics
Analyzes DNS traffic in real time to detect and identify hosts infected with malware, bots, or other unknown threats. It detects breaches before damage is done.

ArcSight Application View
Automatically monitors applications and identifies threats by capturing details on potentially fraudulent user activity.

Micro Focus Security Intelligence and Operations Consulting (SIOC)
Leverage years of security expertise to help you build a mature security operations and cyber defense organization.

Micro Focus Security Monitoring Service
Provides event monitoring and incident response for your ArcSight implementation, which is delivered by Micro Focus security experts.

Micro Focus Security Applied Data Sciences
Delivers immediate value in protecting your digital enterprise via use-case-driven models developed by data scientists and security researchers with deep domain knowledge who utilize machine learning and predictive analytics.

Managing Risk via Comprehensive Security Solutions
Micro Focus Security services are delivered by a group of world-class, globe-spanning security professionals whose varied and vast experience gives Micro Focus Security the unique ability to help secure information across any technology and configuration. The scale of Security also gives us a unique understanding of your legal and regulatory requirements—so we always have the services you need to stay in compliance.

When you extend your capabilities through our managed security services, you get ahead of threats and avoid costly non-compliance consequences.

In addition to software (specific product information is featured earlier in this document and is available via Security), Security offers other distinct capabilities around which organizations can build the solution well suited to their unique needs.

Security consulting is delivered by regional consultants who make sense of the most complex environments. They advise on security roadmaps that support business objectives, transform enterprise security to address gaps, and manage the infrastructure to keep organizations agile and ready to respond quickly to security issues. The offerings include:

Micro Focus Data Protection and Privacy Consulting Services
Provides clients with extensive security expertise and security solution deployment experience, through on-site consulting services. Services

include the design, installation, and integration of data loss prevention, encryption, public key infrastructure, and trust services solutions.

Micro Focus Infrastructure and Network Security Consulting Services

Provides you an extensive security expertise and security solution deployment experience through onsite consulting services. Services include the design, installation, and integration of perimeter, network, endpoint, application, Web and email security, and advanced threat protection solutions.

Micro Focus Security Intelligence and Incident Response Consulting Services

Provides you the ability to understand, detect, and manage global cyber risks, to deal rapidly and effectively with security incidents and with consequent legal and regulatory issues.

Micro Focus Cyber Situational Awareness and Defense (CSAD) Services

Provides you a framework for integrated security protection, security operations, and true visibility of cyber business risk, delivered through specialist security consulting. Services include business-related security metrics, security controls, operational security workflow, and multi-level risk management reporting dashboards.

Micro Focus Security Strategy and Risk Management Consulting Services

Helps you develop full strategic management of cybersecurity risk and compliance through consultancy-led services. It includes security strategy and transformation, risk and compliance management, enterprise security architecture, and cyber assurance.

Threat and Vulnerability Management Consulting Services

Assesses and helps improve your security through consultant-led penetration testing, vulnerability scanning and management, social engineering, and red team assessments.

Advanced Threat Protection Consulting Services from Micro Focus and Mandiant

Protects you from data loss, reputational damage, and financial cost by detecting active threats and compromised assets, containing attacks, mitigating risk, and delivering swift incident response, through a suite of security services underpinned by FireEye advanced threat detection, intelligence, methodologies, and incident response expertise.

Managed security services—monitors and manages security controls. These services, through our 10 security operations centers working 24x7x365, relieve your resources burden, reduce complexity, and help optimize existing security investments.

Micro Focus Data Loss Prevention Services

Provides you an enhanced visibility and control into how critical enterprise information is handled, through a managed security service remotely delivered from leveraged teams. Services include the design, implementation, management, and optional consulting that protects critical data and enables understanding of the use of critical content in an enterprise.

Micro Focus Distributed Denial of Service (DDoS) Protection Services

Detects, identifies, and mitigates DDoS and application layer attacks while helping to preserve site performance and availability of critical business applications and services.

Micro Focus Identity and Access Management Services

Enables control and visibility to users and their access privileges. Services include account provisioning, governance and compliance tools, authentication tools, and privileged account or password policy solutions.

Micro Focus Identity Governance and Administration Services

Enables control and visibility to users and their access privileges. This service helps organizations to manage increasing regulation mandates that can be time-consuming and costly.

Managed Advanced Threat Protection Services from Micro Focus and FireEye

Helps you gain visibility of, greater protection from, and faster response to targeted threats. Services include 24x7 advanced threat protection device monitoring and management with alert investigation, analysis, mitigation recommendations, and response.

Micro Focus Managed Endpoint Security Services

Helps to shield your endpoints from malware and intrusions, and protects data stored on those devices through a managed security service remotely delivered from leveraged teams. Services include anti-virus, personal firewall, host intrusion detection or prevention, and laptop or desktop encryption.

Micro Focus Managed Network Security Services

Offers sound multi-layer protection solutions that facilitate environment safety for you from outside and inside threats. By implementing strong

security frameworks, Managed Network Security Services enable monitoring, detection, and protection against malicious and unauthorized network traffic.

Micro Focus Security Information and Event Management Services

Provides you the ability to improve threat detection, automate compliance, and reduce the complexity associated with security event management. Service includes the ability to collect, consolidate, analyze and correlate log data, and integrate threat intelligence to identify security events quickly and trigger appropriate remedial activities.

Micro Focus Vulnerability Management Services

Provides regular and proactive identification of network vulnerabilities that help prevent hackers or disgruntled insiders from exploiting these network weaknesses. It provides targeted, actionable information to you on vulnerabilities and recommendations for remediation, such as applying critical patches to close them before exploit.

Micro Focus Security—Protecting the Digital Enterprise

Enterprise security must adapt to the new reality of a dissolved perimeter, resolute attackers, and the assumption of compromise. Savvy organizations are abandoning yesterday's bolted-on solutions and embracing a holistic approach to security that emphasizes flexibility, resiliency, and intelligence—because what's not a vulnerability today might very well be one tomorrow.

Remember, no single solution or product can offer an enterprise absolute protection. But a comprehensive, integrated, intelligent approach to security can mitigate your risk, prevent minor incursions from escalating into compromises, and protect your critical business assets. Security solves modern security challenges through a three-pronged approach:

Prevent

Modern protection efforts mean building security from the ground up. Security provides the means to do this. Security–Data Security provides data-centric security safeguarding data throughout its entire lifecycle—at rest, in motion, in use—across the cloud, on-premise, and mobile environments with continuous protection. Security Fortify offers comprehensive application security solutions including application security testing, software security management, and application self-protection.

Detect and Respond

Determining when an intrusion has occurred and being able to respond accordingly is of paramount importance in securing the digital enterprise. Security delivers this capability via Security ArcSight. Security ArcSight offers a comprehensive SIEM solution that enables cost-effective compliance and provides advanced security analytics to identify threats and manage risk. Scaling to capture massive amounts of physical, network, host, application, and user data, ArcSight enriches data and performs real-time correlation with accuracy to reduce the noise. Advanced analytics uncover hidden attacks, improving overall security team effectiveness.

Recover

Mitigating disastrous impacts and meeting compliance demands is more important than ever in an uncertain era. Security backup and recovery solutions protect your information intelligently across physical, virtual, and cloud infrastructures, and give organizations visibility, access, and control of mobile information on any endpoint device. Security ArcSight orchestrates and automates mitigation and remediation response to threats, and facilitates compliance with PCI, HIPAA, NERC, SOX, and more. For more information on how rapid deployment of industry-leading incident responders and breach recovery activities can transform your enterprise security posture, visit Incident Response and Breach Recovery.

Micro Focus can help bring the necessary security functions together. What's more, we can be your true partner in this critical journey. And it's not just the technology, but also the breadth of vision enabled by our dedicated security industry specialists, that makes Micro Focus Security a unique security solutions provider.

Micro Focus Security offers products and services designed to help organizations protect their most-prized digital assets, whether on-premises, on cloud, or in between. We help protect organizations by building security and resiliency into the fabric of their enterprise, proactively detecting and responding to threats, and safeguarding continuity and compliance to mitigate risk effectively.

Learn More At

www.microfocus.com/arcsightactivate

Additional contact information and office locations:
www.microfocus.com

www.microfocus.com