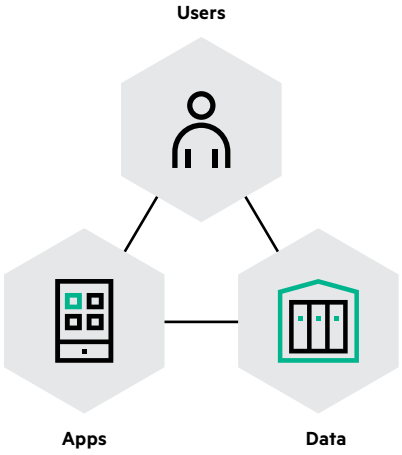
Brochure

Protecting the digital enterprise

Hewlett Packard
Enterprise



Protect your most prized assets and their interactions, regardless of location or device

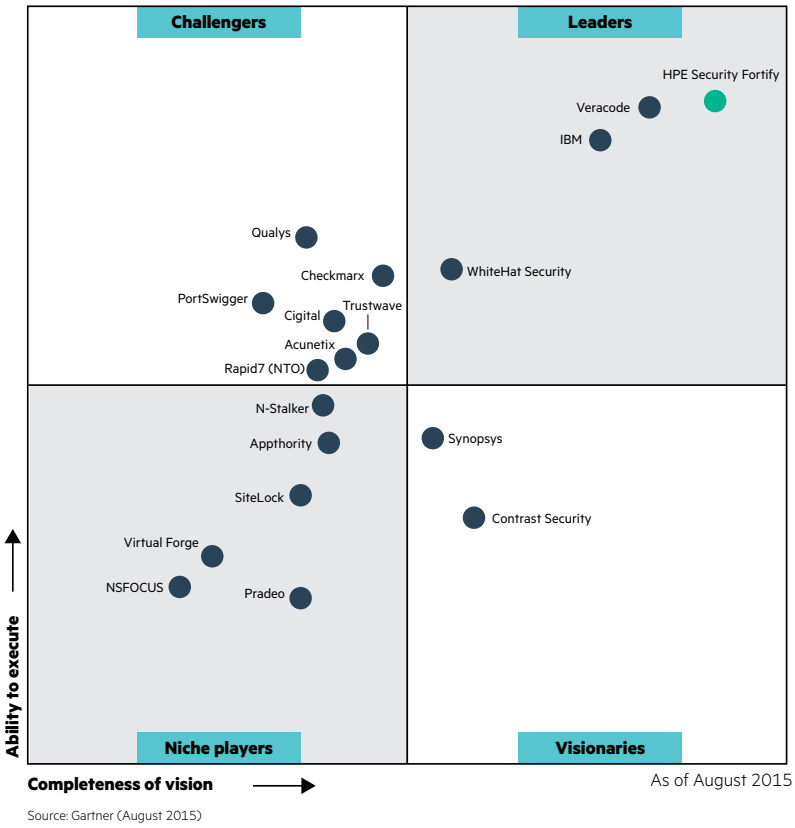
The transition to the cloud, the embrace of Big Data, and the expansion of mobility and the Internet of Things (IoT) have had a positive impact on businesses and the IT architectures that support them. While these technologies increase organizational productivity, they do so by making applications and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

HPE 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.

With devices, applications, and hybrid environments quickly becoming the new normal, the digital world is expanding like never before. However, that expansion also means being exposed to more threats.



Source: Gartner (August 2015)

In 2015, Gartner named HPE Security Fortify a leader in every Magic Quadrant for Application Security Testing they have ever produced.

More than 1,000 organizations worldwide are standardized on HPE Security Fortify—nine of the top 10 major banks, nine of the top 10 software companies, 10 of the top telecom, many major branches of U.S. Department of Defense (DOD), and five of the top insurance firms.
hpe.com/software/fortify

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 HPE 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. **HPE 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.

HPE 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. **HPE Security Fortify** products and services that can help organizations secure their applications against attack include:

HPE Security Fortify on Demand
With application security-as-a-service, HPE 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.

HPE 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.

HPE 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.

HPE 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.

HPE 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.

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

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

HPE 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.

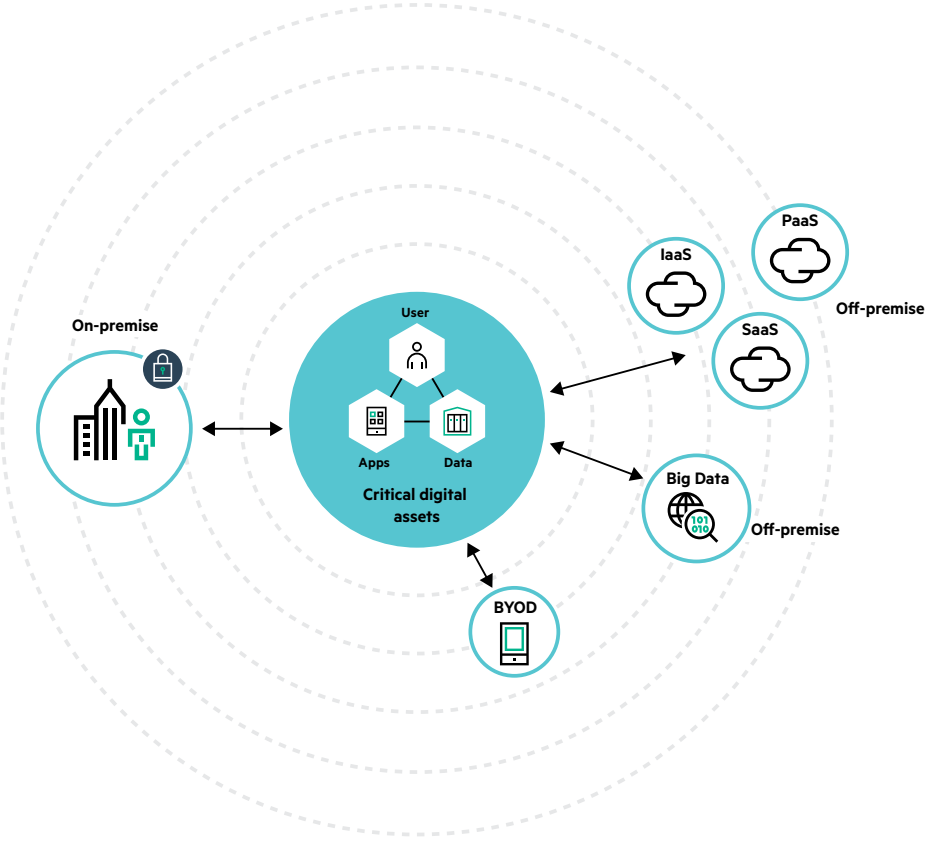


Figure 1. The expanding perimeter and increased attack surface

Data security with HPE Security
In the modern era, protection must accompany data no matter where it travels. The **HPE Security** approach includes methods for protecting data wherever it resides, whether at rest, in use, or in motion. Instead of prioritizing perimeter defenses, organizations need to adopt a data-centric data protection approach that calls for de-identifying the data as close to its source as possible. In addition, it requires replacing sensitive data elements with usable, yet de-identified equivalents that retain their format, behavior, and meaning.

This protected form of the data can then be used in subsequent applications, analytic engines, data transfers, and datastores. In other words, the data de-identification process obscures any sensitive data such as personally identifiable information. These include account numbers, social security numbers, personal health information, or payment card data—so that should a data breach occur, the "data" obtained by the perpetrator(s) will be of no value, and won't disrupt business processes.

HPE Security — Data Security is a leading expert in **data encryption** and **tokenization** solutions for:

- Many of the world's largest merchants and retailers
- Seven of the nine top U.S. payment processors
- Eight of the 10 top U.S. banks who utilize HPE Security — Data Security solutions
- Thousands of mid-sized businesses including healthcare organizations, regional banks, and insurance providers, transportation, retail, high tech, telecom, and public sector

HPE Security — Data Security products and offerings that help businesses protect their digital enterprise include:

HPE Atalla HSM Network Security Processor
This reliable payment processing solution uses a tamper-resistant hardware security module (HSM) for cryptography.

Millions of individuals use HPE SecureMail to secure sensitive information in emails sent to local healthcare providers, law offices, and insurance brokers.

HPE SecureData Enterprise
Delivers complete data protection, PCI scope reduction, and enablement of secure analytics with HPE Format-Preserving Encryption (FPE), HPE Secure Stateless Tokenization, and stateless on-demand key management. This secures data as it is captured, processed, and stored across databases, applications, data warehouses, Big Data, IoT, and cloud environments.

HPE SecureData Suite for Hadoop
Protects sensitive data used in Hadoop. And with Big Data technologies, the suite offers advanced security features such as industry-standard and next-generation FPE that is highly scalable, high performing, easy to implement, use, and manage.

HPE SecureData Payments
Provides data-centric, end-to-end protection of payment card data from the point of capture to the host payment processor to secure data for retail credit and debit transactions. Moreover, SecureData Payments enables PCI scope reduction and protection of PAN data without the massive IT disruptions traditionally associated with these technologies.

HPE SecureData Mobile
SecureData Mobile provides security at data capture on the mobile endpoint and enables end-to-end sensitive data protection from the native mobile iOS and Android applications through the entire enterprise data lifecycle as well as payment data stream. Data is protected as it moves anywhere it resides and however it is used.

HPE SecureData Web
Enables seamless end-to-end protection of sensitive data from the user's browser to the trusted payment host, which helps to shield sensitive payment and personal customer data collected at the browser from theft in front-end and intermediate systems.

HPE SecureMail
Provides policy-based, end-to-end encryption for email and mobile messaging, which offers internal, external, and cloud-based deployment models that are scalable. This enhances the security of sensitive data such as personally identifiable information (PII) and personal health information (PHI).

HPE Enterprise Secure Key Manager
HPE Enterprise Secure Key Manager (ESKM) is used to create, protect, serve, and audit the use of business-critical encryption keys, for data-at-rest at the infrastructure level.

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 HPE 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. **HPE 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. HPE Security counters this problem in several ways.

One is by utilizing threat intelligence—crowd-sourcing vulnerable information, **HPE Security Threat Central** can provide reliable threat intelligence to help users detect attacks faster and more accurately. HPE 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.

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

HPE 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.

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

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

HPE 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.

HPE 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.

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

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

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

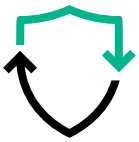
HPE Security Applied Data Sciences
Delivers immediate value in protecting your digital enterprise via use-case-driven models developed by data scientists and security researchers with deep domain knowledge who utilize machine learning and predictive analytics.

Managing risk via comprehensive security solutions

HPE Security services are delivered by a group of world-class, globe-spanning security professionals whose varied and vast experience gives **HPE Security** the unique ability to help secure information across any technology and configuration. The scale of **HPE 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 **HPE Security**), HPE 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:

HPE 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.

HPE 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.

HPE 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.

HPE 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.

HPE 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 HPE 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.

HPE 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.

HPE 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.

HPE 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.

HPE 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 HPE 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.

HPE 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.

HPE 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.

HPE 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.

HPE 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.

HPE 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. **HPE Security** solves modern security challenges through a three-pronged approach:

Prevent
Modern protection efforts mean building security from the ground up. **HPE Security** provides the means to do this. **HPE 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. **HPE 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. HPE Security delivers this capability via **HPE Security ArcSight**. HPE 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. **HPE 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. **HPE 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**.

Hewlett Packard Enterprise 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 **HPE Security** a unique security solutions provider.

HPE Security offers products and services designed to help organizations protect their most-prized digital assets, whether on-premise, 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.

Brochure

For more information about how HPE Security helps protect the digital enterprise, visit:

Main: HPE Security

Twitter: @HPE_Security

Blog: Protect Your Assets

LinkedIn: HPE Security

Learn more at
hpe.com/security

Sign up for updates

Hewlett Packard Enterprise

4AA6-7257ENW, September 2016, Rev. 1