Solution brief

# HPE Converged Security

Protect your digital enterprise

## The barbarians are at the gates. Are you ready?

Long gone are the days when the biggest threat to your company's security was a malicious virus or a service denial typically inflicted by hackers who wanted to create havoc, vandalize, or at worst, wage war on what they saw as evil corporations. You protected your network perimeter with firewalls and intrusion detection, and kept antivirus software up-to-date on all your PCs. These countermeasures did not stop every hacker, but they did a good job and you usually knew when you were under attack. To fend off an attack, you would apply new signature files to your antivirus or harden your firewall a little more, and things usually went back to normal.

This is no longer the world we live in.

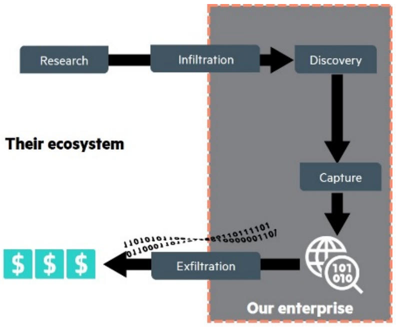
Consider the following statistics[*]:

- 69% of breaches are reported by a third party, and 66% of breaches remain undiscovered for months.
- The cost of attacks is high and getting higher. The annual cost of breaches increased from $7.2M to $7.6M in 2015.
- The time to discover and contain attacks is getting higher. In 2015, it increased by 15% and is now 27 days, on average.
- 99.9% of the exploited vulnerabilities since 1999 were compromised more than a year after the alert was published. 50% were exploited within the first month in 2014.

In short, the odds of being attacked—along with not knowing it until it is too late, and it taking longer and costing more to fix things—are increasing.

## The new reality

It is an unfortunate fact, but the 'bad guys' have gotten better, more organized, and more focused. The geeks in the basement have been replaced by well-funded, sometimes state-sponsored cyber-terrorists and international crime syndicates, and are driven by far more insidious motives—financial fraud, industrial espionage, or cyber warfare. They form an entire ecosystem of expert hackers who work together. While in the movies, hackers still hunch over keyboards typing commands and bypassing firewalls, the reality is that in the majority of significant breaches, the adversary has been on the inside for months, doing their reconnaissance and probing the defenses looking for the mother lode. They got in through phishing or social engineering and mostly appeared like legitimate users.



The adversary ecosystem

To make matters worse, the network perimeter you could rely on as being your line of defense now resembles Swiss cheese. Your infrastructure is moving to the cloud and onto environments that you no longer own. Your employees are using mobile devices that you cannot fully control, installing apps that you are not aware of, and simultaneously connecting to your corporate and the public cellular networks. But even if you could mitigate all of these issues, the network is no longer the battleground: 84% of breaches occur at the application layer.

## Together you stand, divided you fall

Enterprises are investing heavily in security, and that spending grew by about 80% between 2012 and 2014. But all of this spending doesn't seem to help. Why?

The approach IT usually takes is to deploy more technology. The average IT security team often has tens of point solutions, generating massive amounts of data, to a point that it is hard to see the forest for the trees. These tools are usually not well integrated, the data is not properly mined and analyzed, and as a result, the amount of real intelligence is small. Moreover, prioritization is also problematic: Enterprises consider the majority of security initiatives to be a critical or high priority, which ultimately makes none of them uniquely important.

To effectively protect your digital enterprise, you can no longer afford to treat security as an overlay function. You need to start moving toward "security by design" by embedding it in the IT value chain. This means that it's time for your Security, Operations, and Applications teams to better collaborate to embed security throughout

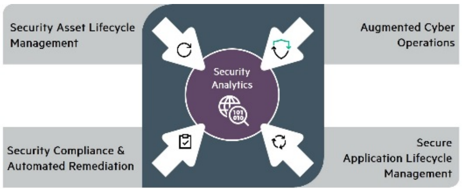
[*] The 2015 Data Breach Investigations Report, Verizon. http://www.verizonenterprise.com/DBIR/2015/
Ponemon Institute 2014 Cost of Cyber Crime Study, based on survey of 257 organizations in six countries

the IT value chain using well-defined use cases.

## Introducing Converged Security

Converged Security is about approaching security as everybody's business. Protecting the digital enterprise is not just the job of IT security, but requires everyone to work together. If security is a bolt on, by the time it takes action, it is too late. So what IT security does (compliance and remediation, protection. threat identification and mitigation), should be combined with what the rest of IT does (monitoring, change management, application development) into a shared context of integrated security and operations from which you can proactively act to reduce your risk

Converged Security is a use-case-driven approach that aims to enable you to overcome silos and gaps by promoting the viewpoint that security needs to be woven into the IT fabric. Converged Security will allow enterprise IT to build security, by design, into its value chain so that it can prioritize those initiatives that most support the business goals.


Security Asset Lifecycle Management
Augmented Cyber Operations
Security Analytics
Security Compliance & Automated Remediation
Secure Application Lifecycle Management

It is important to note that Converged Security is complimentary: it is a means to enhance, not replace, the security strategy you have today.

## Pillars of Converged Security

Have you ever had to contend with:

- Changes being applied, violating a security policy, because IT security is not involved in the change control process?
- IT Security needing to remediate what they detect as a vulnerable system but unable to because they have no idea what they may break?
- IT Operations deploying servers without the knowledge of the security team, potentially introducing vulnerabilities into the environment?
- Applications released with security-related bugs?

These are all symptomatic of a silo approach to protecting your digital enterprise—introducing duplications, overlaps and inefficiencies.

So what can you do to address these issues?

### Secure Application Lifecycle Management

Driven by DevOps, rapid application release is now the name of the game, and in an application lifecycle context, security is still often considered as a non-functional area. However, because we now deploy apps on mobile devices or in the cloud, requiring them to integrate with our on-premise core systems, security can no longer be non-functional. It now needs to be designed into the application architecture holistically and made an integral part of your application lifecycle.

This means that you need to start adopting and integrating into your DevOps framework, practices such as static code analysis, dynamic security testing, and real-time analysis and protection of running applications. For example, in a Continuous Integration scenario, you would kick off a security scan as soon as code is checked in.

### Security Compliance and Automated Remediation

The security state of an IT asset is part of its configuration. Yet, for most IT teams, security compliance and configuration management are two distinct activities, done by two distinct teams, most likely with two sets of similar discovery tools and configuration databases. Over and above the obvious duplication, data is typically not shared between the teams. So when IT Security finds a vulnerable component, they have only a partial view of its configuration, and they are unsure of the impact that their remediation will have, beyond just fixing the security issue.

In this state of affairs, remediation cannot possibly be automated, and ends up being a slow, manual, expensive, and error-prone process.

You can address this by doing two things:

1. Integrating your security and configuration management databases to provide a single, complete view of the configuration state of IT components
2. Adding the ability to automate remediation tasks and flows so that they can be launched when needed

These will make compliance scanning and remediation more accurate, faster, and more efficient.

### Security Asset Lifecycle Management

Prevention is often better than a cure. Being able to detect and automatically remediate vulnerabilities can become even easier if you prevent vulnerabilities from entering your environment in the first place. You introduce vulnerabilities when you make changes in the environment (e.g. deploying new assets). Most of the changes in your environment are a result of deliberate action by your IT staff. But how often is the question "what does this mean from a security standpoint?" being raised. How often is IT security represented, for instance, in Change Advisory Board meetings?

When new assets are being deployed, you need to first determine their risk profile. Is it production or test? Is it externally accessible? Is it mission-critical? What technologies does it use?

Integrating IT security operations with your release and change management processes will allow you to answer these questions and better assess the risk profile of the assets being deployed. It will give you the opportunity to take preventive action so that you don't have to apply a cure later.

### Augmented Cyber Operations

The NOC and the SOC do very similar things: they monitor the environment, detect issues, and fix them. In theory, perfect candidates for collaboration. Yet, the reality is that in many enterprises, these are two distinct functional silos. Consider the following scenario:

An application service account is hijacked and used to access and exfiltrate your customer database. As a result, CPU and memory utilization spike, and users call the help desk complaining about the slow application. Then the following happens—all at the same time:

- The IT Operations team opens a bridge call, and domain experts are trying to troubleshoot the problem
- IT Security may be looking into the fact that someone is accessing the database from a never-before-seen location
- Network Operations— in a third operational silo—has detected traffic spikes as gigabytes of data are leaving your company

The result is overlapping efforts, wasted cycles, and excessive time for remediation of a crippling business problem.

Augmented Cyber Operation is about bringing these functions closer together by enabling data exchange between your security monitoring and IT monitoring platforms and event consoles. This integration allows you to query and correlate data between the two sources. Using the example above, you could now see whether CPU and memory spikes correlate to suspicious access to your database, or vice versa. You could put two-and-two together and ensure that remediation is fast and to the point.

### Security analytics

Security attacks are becoming more sophisticated and more "personal"—they are engineered to attack a specific company for specific purposes. Rather than being a full-blown frontal assault at a point in time, this mode of attack is characterized by stealth and longer (often months) periods of time. An attacker might infiltrate your network, but not knowing exactly where the "good" targets are, they stay "under the radar," probing and observing, until they find what they need.

This type of "slow moving" attack is hard to detect using standard IT security operations activities, and many enterprises now have dedicated "hunt teams" to look for telltale signs of suspicious activities and impending threats. But the volumes of data—log files, security scans, audit trails, and more—that these teams need to sift through are very large, making it essentially a Big Data problem.

You need a Big Data platform that can not only deal with data collection and storage, but also provide the advanced analytics necessary to detect patters and turn these volumes of data into useful information. This will allow you to quickly find these telltale signs and prevent an attack from ever taking place.

## Why HPE Software Services?

Hewlett Packard Enterprise has one of the market leading and most comprehensive suites of software solutions for IT Security, Operations Management and Application Delivery Management.

We bring together these solutions and our unmatched expertise to provide you with a proactive approach to security that integrates security and IT operations into a cohesive protection capability for your digital enterprise.

We offer a full range of innovative professional services, practical customer experience, and deep knowledge of HPE and partner technology.

Partnering with HPE Software Services gives you access to:

- IT Security, IT Applications and IT Operations experts with industry-leading knowledge, experience, and best practices developed across all geographies
- Consistent global delivery of world-class professional services
- End-to-end holistic solutions that integrate business processes, people, and technology

## For more information

Contact your HPE representative or email HPE Software Services in your region:

HPE Software gives you the power to gain connected intelligence for the new style of enterprise IT—anytime, anywhere, quickly and securely.

Learn more at

**HPE Converged Security**

**HPE Software Services**

**Sign up for updates**

★ Rate this document

Hewlett Packard Enterprise

4AA5-2780ENW, March 2016, Rev. 1