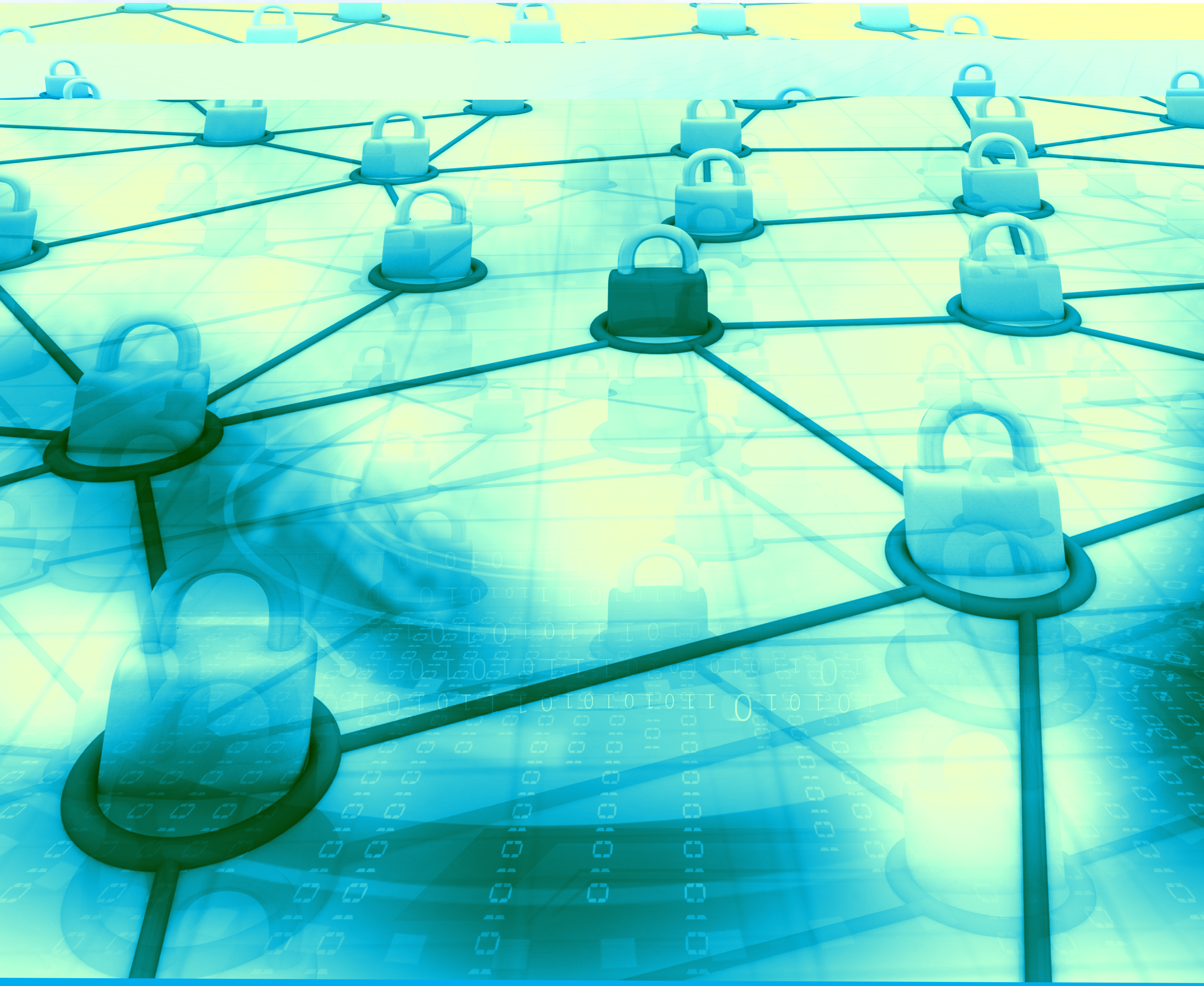


Securing Your Business

Security@SAP

June 2016

Letter from Bill McDermott

Dear customers,

Information security is a journey without a destination. The security threat in the enterprise is relentless and multiplying, and the attackers are getting more sophisticated. Around the world, there is tremendous concern around information security. It is top-of-mind for every CEO I meet.

This SAP Security Point of View briefing outlines key security trends, shares how your peers are thinking about security, and provides an overview of SAP's security strategy and portfolio.

Our mission is to keep you focused on running your business and managing your customer relationships, knowing that your data is safe with SAP. We commit to continuously innovate in this critical topic to keep you secure - both in the cloud and on-premise.

Run Simple. Run Secure.

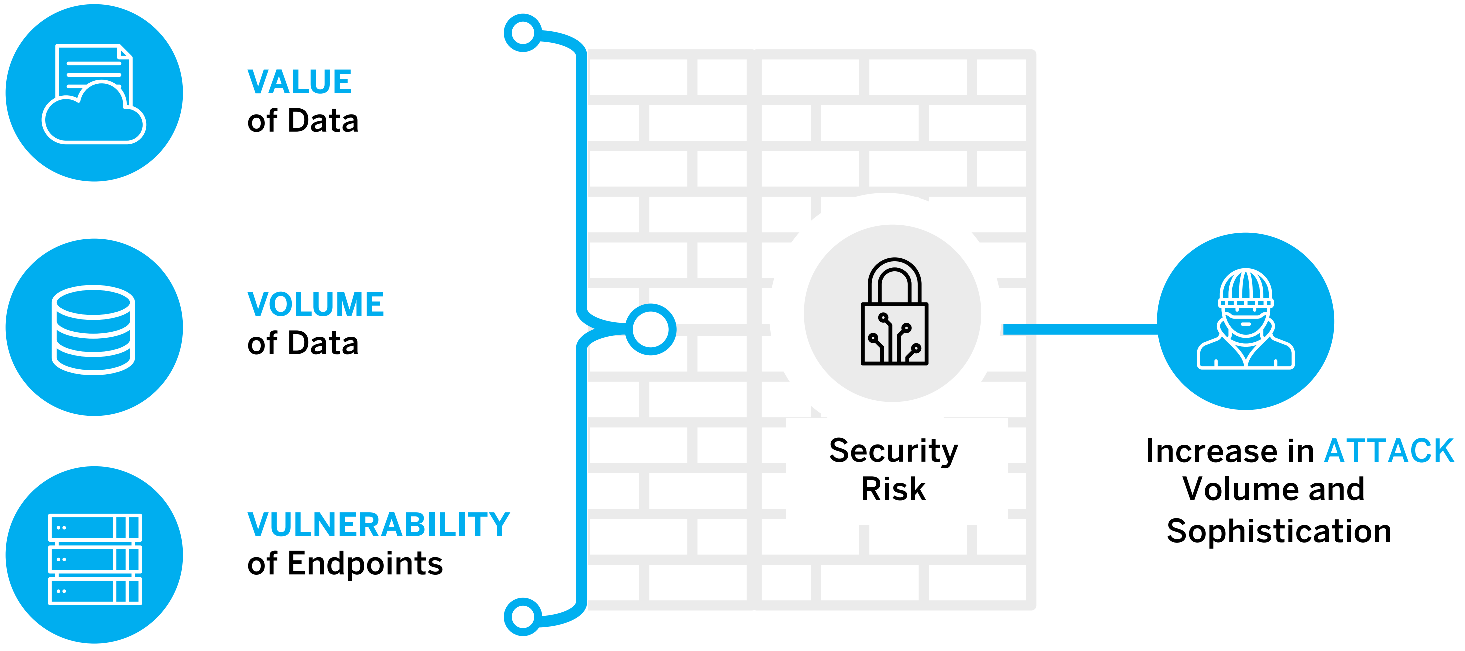
Bill McDermott
CEO, SAP SE

Security Risk in the Digital Economy

Defining Your Security Risk

Digital disruption is real and is here to stay. Companies all around the world are re-imagining their businesses with the customers at the center. Smart machines are getting smarter. Connectivity at the individual and machine level is measured in billions. Communication within organizations and by individuals is generating an almost unmeasurable amount of information.

While these advancements offer great potential value and can deliver breakthrough innovation for businesses, they also come at the cost of heightened security risks. The complexities of the digital economy combined with the emerging "hacker industry" are significantly increasing the threat to organizations.



VALUE of Data

VOLUME of Data

VULNERABILITY of Endpoints

Security Risk

Increase in ATTACK Volume and Sophistication

Companies can think of the security risks to their business as being a product of 4 key components related to one of a company's most important assets - its data. First, the value of the data - both in terms of the value able to be extracted and the value a potential hacker could exploit. Second, the volume of data being stored - companies are collecting and storing more data than ever before. Third, the vulnerability of endpoints and other systems exposed to the outside world - data no longer remains locked inside a data center; instead it increasingly proliferates outside of the four-walls of business. Lastly, the sheer number of and the sophistication of attacks facing businesses are at an all-time high with the "commercialization of hacking".

Changing Nature of Your Security Risk

$2.8 trillion
GDP increase from online data flows

Dramatic Increase in Value of Data: The world is becoming smarter with the digital economy, and this is influencing companies in dramatic ways. Companies are creating new business models, embedding software in products, and focusing on business outcomes. This shift will exponentially increase the value of data – and in turn, makes a breach of the same data more damaging than ever before. McKinsey & Co. reported a $2.8 trillion GDP increase from data flows as more and more trade and commerce shifts to online business models.

521.000 PB
of data storage capacity to be shipped by 2020

Exponential Volume of Data: The pace of data creation is exploding. With the advent of mobile, consumers are now creating as much as 70% of new data. Data creation will further accelerate as the Internet of Things (IoT) becomes more prevalent. Big data is becoming ever pervasive, with IDC predicting over 521,000 PB total enterprise storage capacity to be shipped by 2020. As the volume of data rises, so does the size of the attack surface for any potential hacker targeting enterprise data.

21 billion
new devices connected by 2020

Increasing Vulnerability of Endpoints: While data was once stored safely inside the four-walls of enterprises - it is now being stored, accessed, and modified on mobile devices, in the cloud, and by the devices across the Internet of Things (IoT). IoT alone will dramatically increase the number of devices that can be compromised by a cyberattack with Gartner estimating 20.8 billion IoT devices connected by 2020. This will cause valuable data to be stored across hybrid infrastructures - on-premise, in the cloud, and on endpoints - further increasing security risk.

65 percent of companies surveyed experienced more Advanced Persistent Threats (APT)/ targeted attacks

Greater Proliferation of Attackers: With the ever-increasing risk of corporate spying and digital theft, cybersecurity must be addressed at the corporate-level as organizations execute their digital strategy. Attackers are becoming more sophisticated and persistent - in 2015, 65% of companies experienced more Advanced Persistent Threats (APT)/targeted attacks.[1] As cyberattacks become "commercialized", the realized value of successfully breaching a company's data will continue to attract more sophisticated and more numerous attackers. The number of records compromised is staggering: an average of 1.9 million records was breached every day in 2015.[2]

Customer Perspectives on Security

Shifts in Approach to Security and Spending

A survey of over 700 IT security professionals sponsored by SAP and conducted by IDC found that as security risks mount, organizations are shifting from a reactive, threat-oriented view on security towards taking a proactive, predictive approach.[3] SANS Institute recently reported that while median IT budgets are remaining constant, companies saw a 3-5% up-tick in the percentage of it going towards security between FY2014 and FY2016.[4]

BUSINESSES are taking a more proactive, predictive approach to security

TODAY

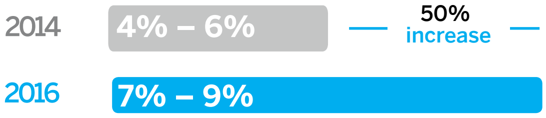
52%

2-YEARS FROM NOW

60%

businesses rating themselves as more proactive than reactive in their approach

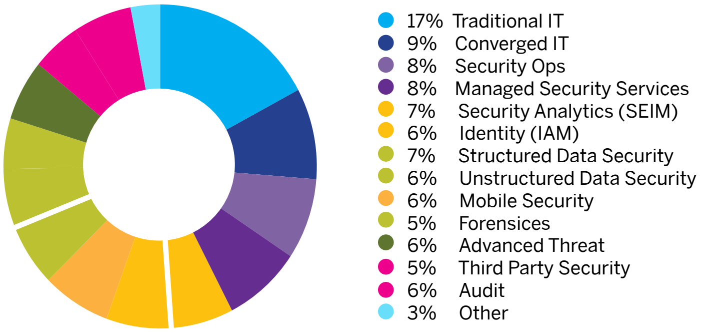
SECURITY spend as a percentage of overall IT spend increased between FY2014 and FY2016



security spend as % of overall IT spend

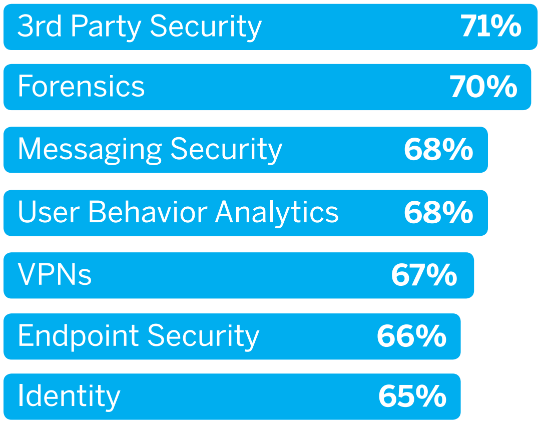
Similarly, security spend today is concentrated in traditional and converged IT infrastructure security. And while respondents expect that two years from now the greatest increase in spending will go into continuing to expand traditional IT infrastructure security, they are also more heavily investing in Managed Security Services (MSS) and Advanced Threat Protection. To this end, there is wide consensus among companies that the cost of maintaining their own security will continue to rise. This is why many businesses are turning to third-parties to manage part of their security.

Companies today are investing in security technologies...



% of overall security spend into each security category

... And increasingly outsourcing parts of their security infrastructure



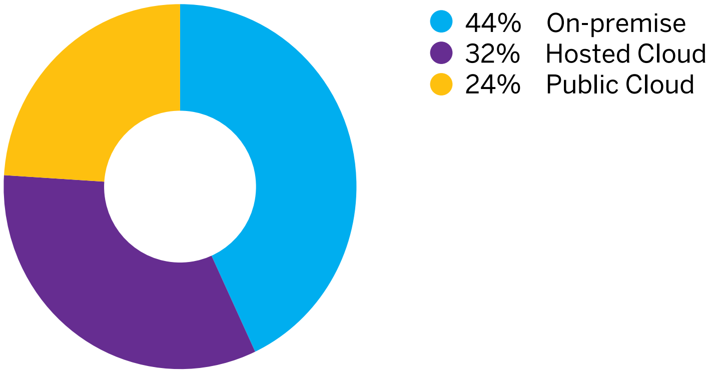
% of respondents outsourcing each part of their security

Cybersecurity Trends

In the era of Advanced Persistent Threats (APT) - such as Stuxnet and the Duqu worm, many traditional security-protection techniques can potentially be bypassed, and malicious exploits can reside undetected in critical systems for years. Recent debate over government data access programs has created more mistrust within this changing threat landscape and reinforced the need for secure information systems.

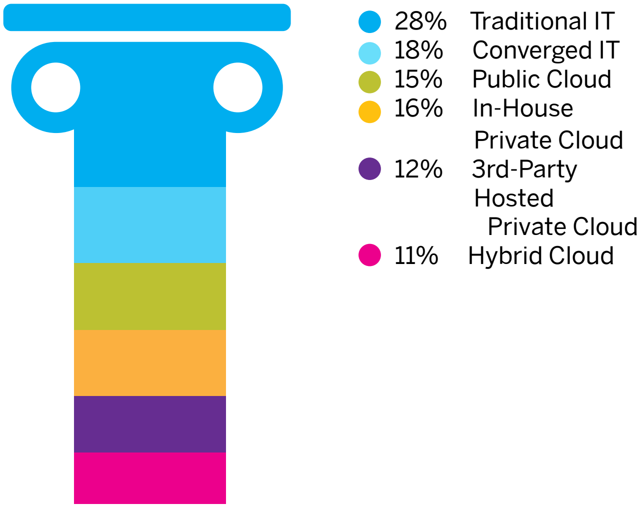
The increasing interconnectivity of companies and businesses across the globe leads to an unprecedented exposure of IT systems to the Internet, making it highly attractive to hackers. As companies continue to build new applications and deploy them in their on-premise and cloud environments, there is a strong need to secure applications across this hybrid infrastructure. Our survey of IT professionals found that 44% of applications in use by companies are still on-premise solutions compared to 56% being in the cloud, a percentage that will only grow as businesses continue to adopt cloud applications and services. IT infrastructure showed a similar trend with 46% being traditional or converged infrastructure compared to 54% being some form of cloud (e.g., public, in-house private, third-party hosted, or hybrid cloud).

Applications continue to move to the cloud...



% of overall applications in use in each category

... With infrastructure undergoing a similar transformation.



% of overall infrastructure in each category

Publicly available data on massive breaches and attacks shows that even large companies and institutions must prepare for the real threat of being attacked by both individual hackers and organizations looking to steal information or cause damage. When IT security professionals were asked about their highest areas of concern, more than half of them were extremely or very concerned about security breaches, increasing sophistication of malware threats, complexity of IT security, and the proliferation of endpoints to be protected.

"What keeps you up at night?" (Respondents ranking 'extremely or very concerned' with issue)

Sophistication of Malware Threats

65%

External Security Breaches

63%

Complexity of IT Security

59%

Internal Security Breaches

58%

Endpoints to be protected

57%

2015 IN REVIEW: DATA BREACHES

Data Records Lost or Stolen in 2015

7 0 7, 5 0 9, 8 1 5

1,938,383

Records lost or stolen **Every day**

80,766

Records **Every Hour**

1,346

Records **Every Minute**

22

Records **Every Second**

Next-generation Security

To respond to these new and ever more persistent threats, emerging technologies and approaches are being deployed across the enterprise. Companies can no longer rely on just firewalls and barricading their perimeter; they must also look to use 360-degree correlation analytics across network, endpoints, applications, and data to better address threats. The increasing availability of connectors / APIs to access data allows organizations to aggregate data from more sources, enabling these correlations.

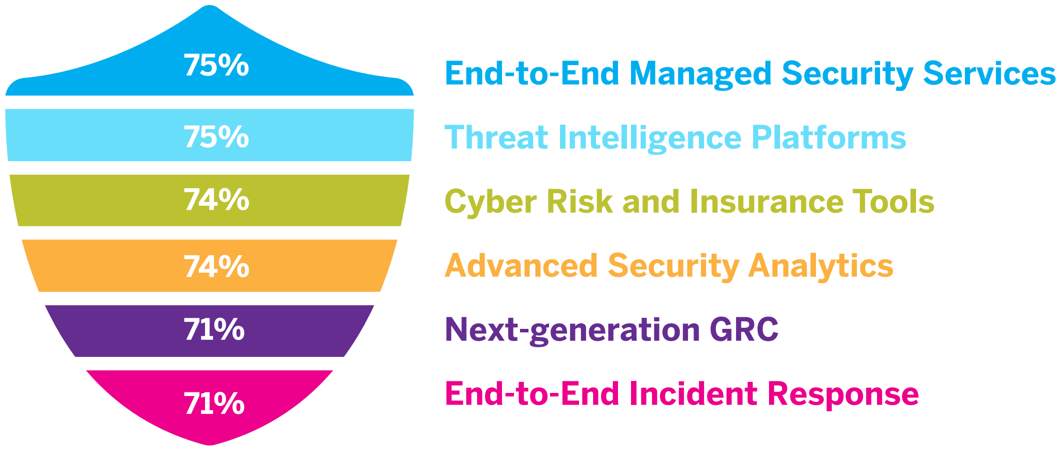
Similarly, advancements in machine learning and deep learning can power cybersecurity analytics and provide an unprecedented level of detection and sophisticated response to a cyberattack. A natural progression is occurring from threat detection to reaction, enabled by integration with security process automation and governance, risk, and compliance (GRC) vendors. In addition, next-generation context and application-aware firewalls are emerging, enhancing both protection and performance of business applications. These are also being complemented by real-time incident response and forensics to accelerate detection, limiting breach impact.

When asked about future security product offerings, 74% of respondents surveyed stated that they were extremely or very interested in more advanced security analytics capable of aggregating technical events into a single platform to speed decision making. Similarly, 71% were extremely or very interested in next-generation GRC offerings capable of leveraging existing process automation data and incorporating "soft" security skills to take pressure off of security operations teams.

CYBERSECURITY INNOVATIONS

- **360-degree correlation** analytics across network, endpoints, applications, and data
- **Real-time incident response** and forensics to accelerate detection limiting threat impact
- **Next-generation context** and application-aware firewalls to enhance both protection and performance
- **Deep learning powered** cybersecurity analytics able to respond to threats in an adaptive manner

Businesses are excited about next-generation security technologies...



% of respondents extremely or very interested

SAP's Strategy to Secure Your Business

SAP has a very long history of helping customers with their mission-critical business applications and analytics. The breadth of our customers is significant - from non-profits to governments, healthcare to manufacturing, pharmaceuticals to utilities. Over 300,000 customers depend on SAP.

From an attacker's standpoint, SAP is one of the most valuable applications to gain access to. This means that SAP must ensure its software is not only secure but also incorporates all aspects of Security Theory. SAP is in a unique and key position to drive what the enterprise software industry has lacked for over 20 years: the ability to finally incorporate security into applications delivering the ultimate protection of content and transactions.

> SAP is in the business of securing our customers' businesses.
>
> **Justin Somaini,**
> **Chief Security Officer**

SAP Security Vision

A world-class vision built on five ideals to secure your business:

Defendable Application

Identify and prevent attacks from within the application

Zero-Knowledge

Ability to store data in the cloud and protect it from outside control

Zero-Vulnerability

Minimize vulnerability to ensure maximum protection

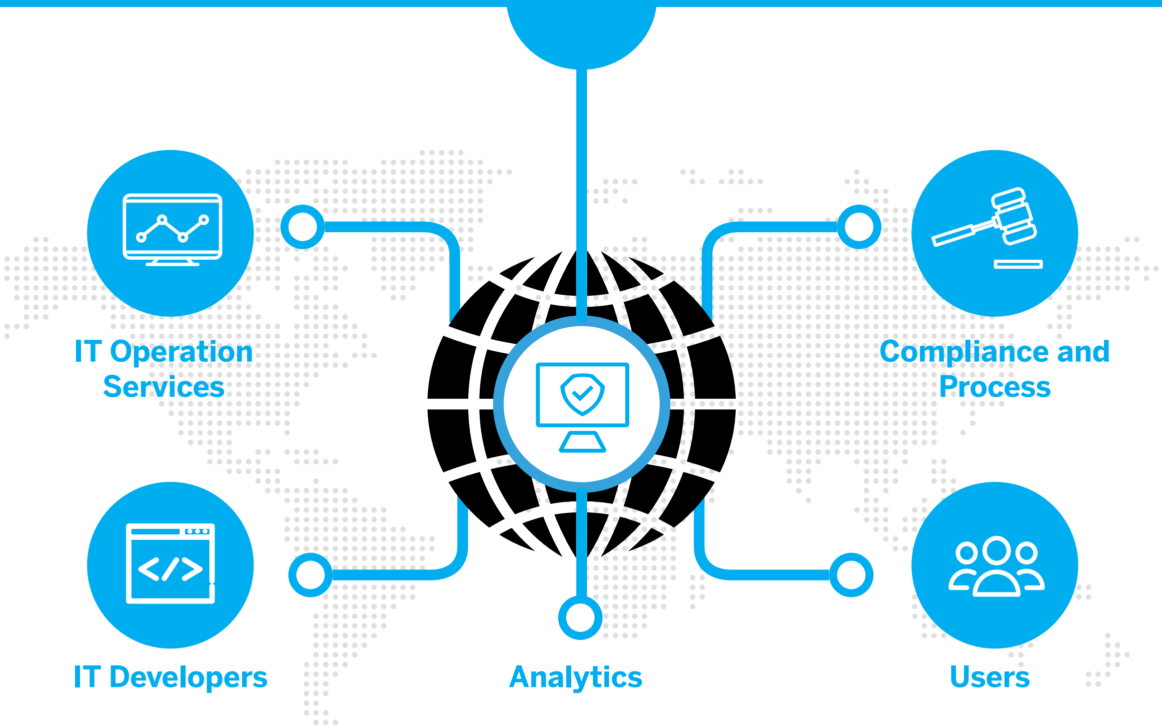
Security by Default

Building security into products right from the start

Transparency

Full and pro-active transparency for the customer

SAP offers a comprehensive portfolio of security products, all of which have been proven with customers and internally at SAP as well...



Enterprise Threat Detection

A security breach that exposes critical data has the potential to seriously damage a company's business, personnel, assets, and brand reputation. It is important to monitor all system activities for unexpected and suspicious incidents to prevent possible attacks, detect incidents, and react before damage can be done. SAP **Enterprise Threat Detection** enables organizations to detect and analyze potential threats to identify critical attacks as they are happening, so that appropriate countermeasures can be applied in a timely manner to prevent serious harm to SAP's customers' business.

Governance, Risk, and Compliance

SAP solutions for **governance, risk, and compliance (GRC)** enable customers to automate the processes associated with managing access to business applications. These include analyzing and remediating access risk, certification, and audit required for compliance and security. The solutions offer a collaborative process for business users to manage roles centrally. SAP extends our offerings using **NextLabs** to take access authorization management to the next level with dynamic attribute based access control (ABAC), to improve enterprise data security & compliance. The **SAP Regulation Management application by Greenlight**, cyber governance edition provides visibility into business risk based on cyber threats by managing security compliance regulations and mapping them to controls.

Identity Management Portfolio

The **SAP Single Sign-On** and **SAP Cloud Identity** application and service enables employees to log in to all applications from their initial authentication. The key is to reduce the risks and potentially high administrative costs associated with multiple authentication processes. Employees do not need to remember passwords for each application they access. In addition, frequent calls to the help desk to reset forgotten passwords and to unlock systems become a thing of the past.

The **SAP Identity Management** component helps enterprises to manage user access to applications securely and efficiently. The software provides a central mechanism for provisioning users in accordance with their current business roles. It also supports related processes, such as password management, self-service, and an approval workflow.

Code Scanner Portfolio

Custom source code risk can be reduced by improving the security of custom applications based on ABAP and by preventing potential attacks by developing secure code with solutions and guidelines. These guidelines for analyzing code vulnerability can help companies inspect all ABAP-based custom code. **SAP NetWeaver AS, add-on for code vulnerability analysis**, is an integrated tool for efficiently scanning and testing source code written in ABAP, which increases security and compliance and reduces risk and costs.

Your software is everywhere – in house, on the Web, in the cloud, and on thousands of mobile devices. It gives the users the information they need for fast and solid decisions. Making these highly accessible applications also highly secure is key to preventing threats to your IT landscape. **SAP® Fortify software by HP** helps you find and fix software vulnerabilities pro-actively on the Web, on premise, in development or in QA to reduce the risk and costs while rolling out secure applications.

Mobile Security Portfolio

The **SAP Mobile Secure portfolio** is an enterprise mobility management (EMM) software-as-a service (SaaS) offering that makes it simple to securely manage mobile devices, apps, and content. From a single, integrated solution, enterprises are able to address mobile security and application management needs for both their employees and their extended ecosystem.

Digital Business Services

The **SAP Digital Business Services (DBS)** organization processes security incidents securely and reliably for SAP customers and partners through on-site as well as remote support services. The security team maintains information security by following clearly defined measures including required authorizations and secure and encrypted remote support connection.

Specialized services and resources help our customers to efficiently build and run SAP software securely. These include the following:

- The **security monitoring center at SAP** is a dedicated IT security team that operates 24x7 to detect and analyze attacks.
- The **secure operations map at SAP** is a reference model to identify and structure all areas for the secure operation of SAP software landscapes.
- The **SAP EarlyWatch® Alert** service monitors operation- and security-critical aspects of SAP systems.
- The **SAP Security Optimization** service provides recommendations to help resolve potential security issues.
- **SAP Solution Manager** enables system recommendations in the change management work center.
- The **global security hub,** comprising SAP's internal security team, helps ensure global availability of security services to SAP customers.
- **SAP MaxAttention™** is the optional strategic support engagement offering from SAP for continued and effective business operations.

Stay Connected.

We are securing the future together!

Visit us here: go.sap.com

Sources/Footnotes:

[1] Ponemon Institute, 2015 State of the Endpoint Report, Jan 2015
[2] Gemalto, Breach Level Index (BLI), 2015
[3] IDC Future of Security Survey – Preliminary Results, sponsored by SAP, May 2016
[4] SANS Institute, IT security Spending Trends, Feb 2016