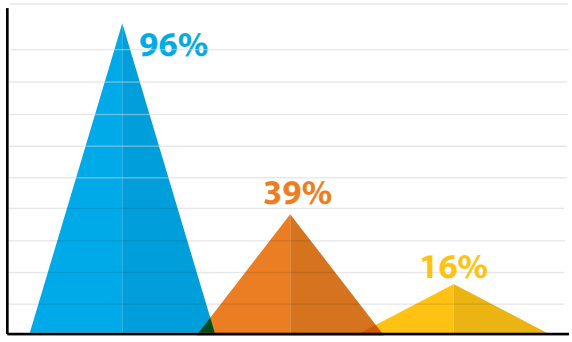
Threat, Violation and Consumerization Impact

Network Complexity, Exposure Diversity and Issue Velocity Challenging Security Management

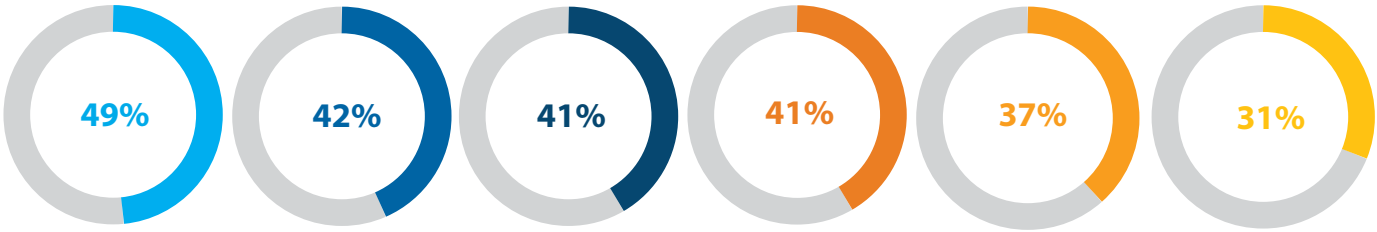
Summary of Research

Significant Security Incidents Experienced in Past 12 Months



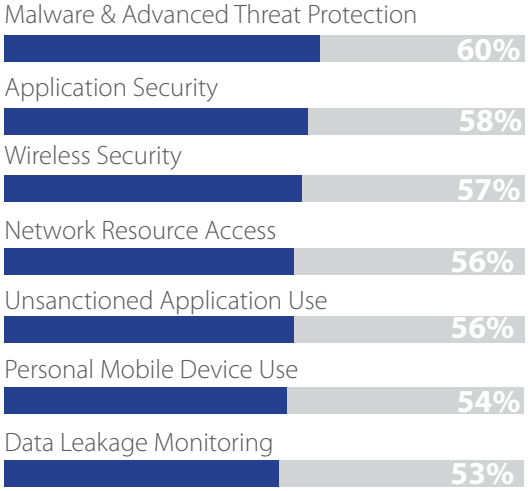
- Experienced on average at least 1 significant security incident
- Experienced on average more than 2 significant security incidents
- Experienced on average more than 5 significant security incidents

Infrastructure Complexity Impacts Security Management – 40% of Companies Find Security Management More Difficult Today Than Two Years Ago

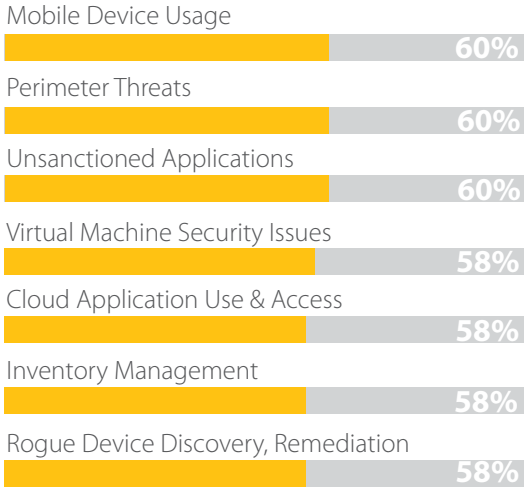


Problem Prevention | Problem Diagnosis | Problem Identification | Problem Remediation | Problem Monitoring | Problem Documentation

Top Seven Areas That Saw Significant Security Violations

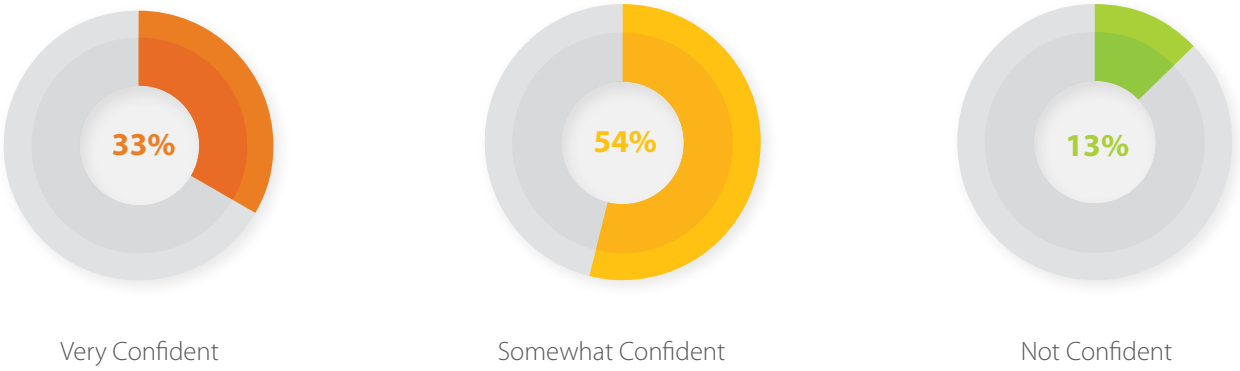


IT Security Management Problems For Which Existing Controls Are Rated Below Average to Poor (0-60%)

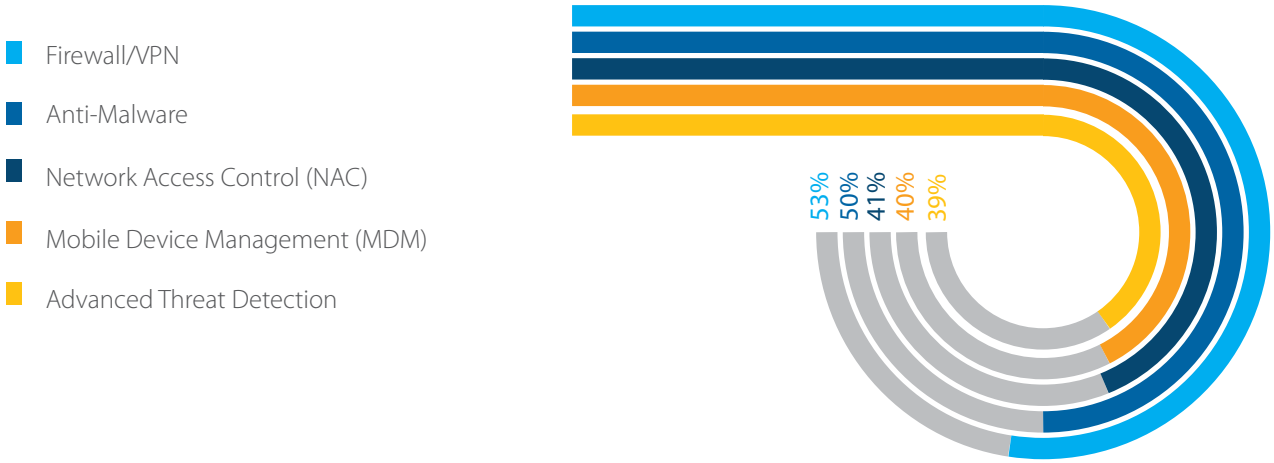


Summary of Research Cont...

Likelihood of Improving Weakest IT Security Management Areas



Top 5 Solutions for Integration Value



Introduction: Infrastructure Complexity and Cyber Threat Velocity Impacting Security Management Capabilities

This IDG Connect survey, sponsored by ForeScout, illustrates the nature and extent of the security threats and defense maturity arrayed against organizations in the finance, manufacturing, healthcare, retail and education sectors in Austria, Germany, Switzerland (DACH region), the UK and the USA. It offers a snapshot of security issues impacting organizations, the processes, tools and controls used to pre-empt and contain violations, exposures and cyber threats, assesses the degree of confidence IT departments have in their efficacy, and identifies areas most likely for future enhancement and investment.

Most organizations within the UK, USA, and the DACH region continue to experience a significant number of security breaches and exhibit a diverse range of exposures, indicating that increases in operational complexity, such as devices, accessibility, mobile, virtualization and cloud, are extenuating gaps in existing security operations. Furthermore, the growth in the number of violations, vulnerabilities, and cyber attack landscape is widely apparent.

The absolute necessity that every organization should undertake is to evaluate the implementation of new monitoring and mitigation mechanisms beyond conventional tools and controls within a defense-in-depth program. It is equally apparent that in many cases effective cyber defenses will require processes conducive to continuous protection which integrates better discovery, prevention and response capacity across the entire IT estate – from end user device and network to the server, application and data.

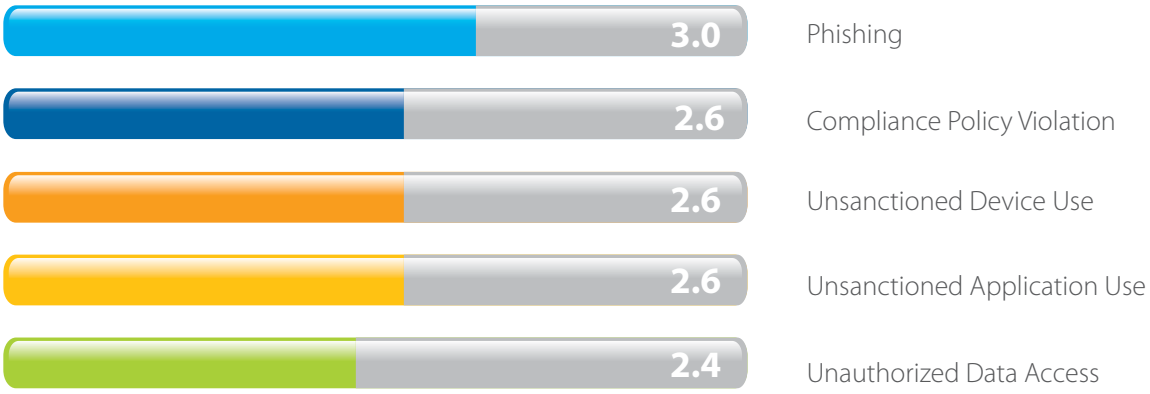
The requirement to sustain effective security management is evidenced by the extent of regulation applied to how security measures are working and how information is protected both on and off-premise. All five verticals surveyed are governed by regional and industry specific data protection, governance and risk management legislation and regulation including the UK Data Protection Act of 1998 and the European Union's Directive 95/45/EC in Europe, the global Payment Card Industry Data Security Standard (PCI DSS) and federal regulations including FISMA, GLBA, NERC, HIPAA/HITECH and DISA STIG in the USA.

Security professionals need not only to know who is accessing their data, when and from where, but where and how data is being stored and protected. That mandate applies not just to the servers, networks, PCs and storage resources within their employers' own on-premise architecture, but also extends to infrastructure belonging to business partners.

That task is further complicated by the current trend of IT consumerization where employees are using personal smartphones, tablets and applications to access corporate networks, applications and data. This places considerable pressure on IT staff tasked with implementing security and data protection measures on a diverse range of systems featuring variable levels of security control – many of which may be outside the direct jurisdiction of the company.

The survey polled 1600 senior IT security and technology purchase decision makers based in the DACH region (Austria, Germany and Switzerland), the UK and the US. The results were collected and analyzed from April to May 2014. Respondents from Europe worked for organizations employing over 500 people, and those from the US for organizations with over 1,000 staff. All were employed in either the finance, manufacturing, education and healthcare sectors, with the addition of the retail industry for organizations polled from the DACH region.

To What Extent Has Your Organization Experienced Significant Security Incidents? (Mean Scores Per Security Incident)



Phishing, Compliance Policy Violations, Unsanctioned Devices and Apps Use, and Unauthorized Data Access Proliferate

Most organizations within the UK, USA, and the DACH region are experiencing an alarming number of security breaches and exhibit a diverse range of exposures, indicating that gaps in existing security operations and defenses are widely apparent. Globally, 96% of organizations experienced at least 1 significant security incident across the ten types surveyed here, 39% saw more than 2, and as many as one in six organizations reported 5 or more security incidents in the same annual period across all ten incident types.

The top five sources of compromise recorded by survey respondents were phishing attacks, compliance policy violations, unsanctioned device use, unsanctioned application use and unauthorised data access, with as much as 25% of organizations across all vertical sectors experiencing five or more instances of phishing specifically in the past 12 months.

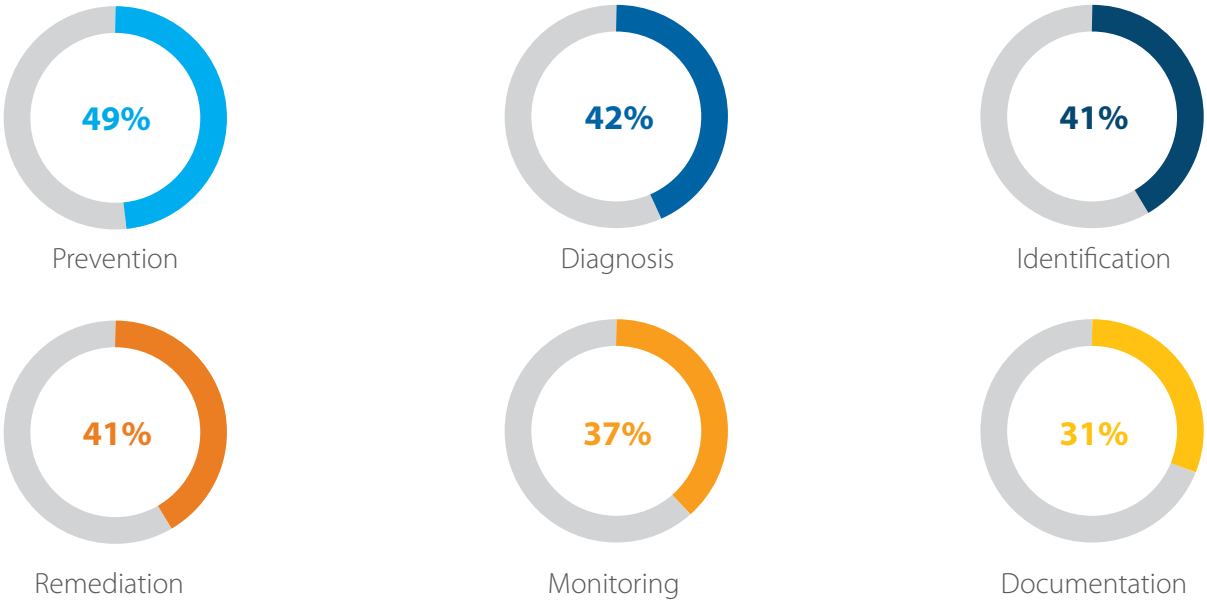
Organizations in the DACH region and to a lesser extent also those in the UK believe themselves to have suffered fewer incidents of these top 5 breaches relative to those in the US. Breaches caused by unsanctioned device and application use, were particular problems for those working in the healthcare industry in Germany, Austria and Switzerland, a vertical which showed consistently below average scores for every other type of security issue other than unknown devices.

Aggregated across all three regions, the finance sector recorded marginally higher numbers of phishing attacks, compliance policy violations, instances of unsanctioned application use and data leakage than the other industries, with manufacturing seeing more breaches caused by unauthorized data access, unknown devices and zero day malware. The healthcare industry appears least affected by both phishing and targeted attacks but slightly more open to unsanctioned device use and data leakage issues.

A majority of respondents indicated a material impact on resources and time originating from man hours spent on identifying, diagnosing, fixing and documenting security incidents within their organizations - resources which could potentially be better deployed elsewhere if the security threat could be more effectively managed and/or automated.

Evidence that security controls to guard against data leakage, targeted attacks, system breaches and zero-day malware have been widely implemented can be seen in the average of 32% of organizations across all vertical sectors and geographies which did not record any incident of significant impact over the previous 12 months. By contrasting this figure with the 4% of respondents across all three regions and verticals which said they did not see any security breaches at all over the same period, we can infer that whilst incidents did occur, they did not cause significant impact, indicating that effective measures to contain them were in place. However, the average of 68% that did suffer incidents of significant impact shows that efficient controls may not be widely implemented, may be too difficult to enforce, or that the volume of incident exceeds the ability to prevent, limit or respond to these issues.

Have Security Violation and Incident Management Become More Challenging in the Last Two Years? (Yes)



Greater Infrastructure and Operational Complexity Expands Security Management Overhead

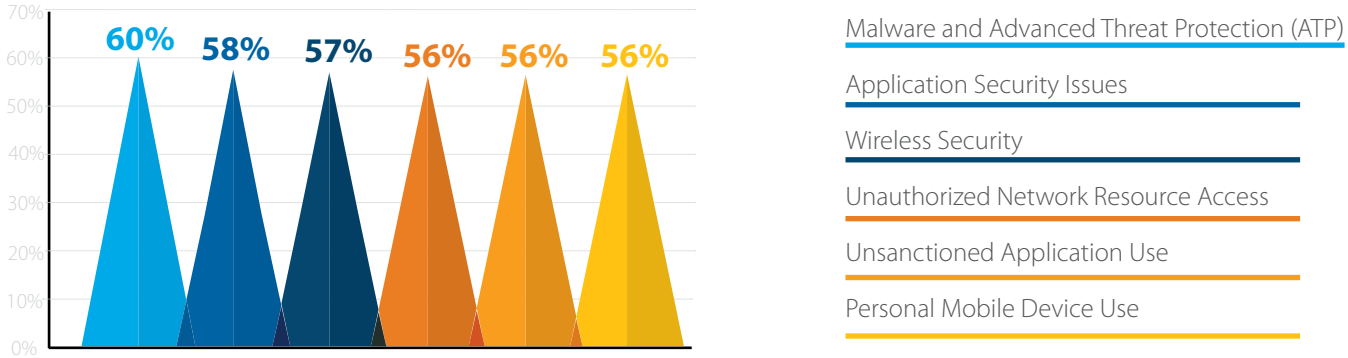
The survey results indicate that the information security management overhead is expanding rather than contracting in most organizations, with significant staff resources allocated to incident response - even within organizations with mature network security, data protection and compliance measures already in place.

Problem prevention is perceived to be more challenging today than two years ago by 49% of all organizations across all five industry sectors with the average brought down by a slightly lower figure in the healthcare sector (45%). Problem diagnosis (42%) and remediation (41%) were also deemed more difficult on aggregate though less so in the manufacturing sector which attributed slightly more significance (42%) to problem identification whilst finance saw problem remediation (48%) as a particular issue.

The findings suggest many organizations will continue to place more emphasis on problem prevention and explore the means to facilitate remediation, even though just under half of respondents indicated either no apparent change to remediation challenges (46%) or that the task was getting easier (14%). Problem monitoring is seen as slightly less challenging by most respondents on aggregate. However, it is possible that the monitoring used in some organizations may not yield the intelligence needed to effectuate any meaningful reduction in identification, diagnosis and remediation.

A Gartner research note "Designing an Adaptive Security Architecture for Protection From Advanced Attacks" published in February 2014 posits that most enterprises are 'overly dependent' on blocking and prevention mechanisms such as firewalls and anti-virus software which are 'decreasingly effective' against advanced attacks, for example. The research company advised information security architects to take a more pro-active rather than reactive approach, assume that their systems are under a state of constant compromise that requires continuous monitoring and remediation, and put greater resources and investment into building out threat detection, response and predictive capabilities rather than pursuing architectural strategies more heavily orientated towards prevention.

Security Violations/Incidents that had a Significant Impact Within the Last 12 months (Ranked as Top Priority)



Malware and Advanced Threats, Application and Wireless Security Issues, and Unauthorised Network Access Are The Most Impactful

The vast and burgeoning plague of malware and advanced persistent threats, which include zero-day and targeted attacks, as well as application and wireless security issues, and unauthorized network access heads the list of significant incidents that organizations have suffered on a global basis over the last year. The risks due to these threats range from service outage to data leakage.

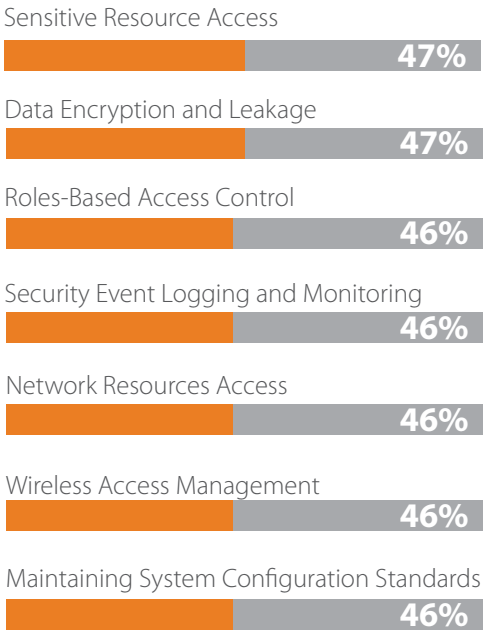
Pricewaterhouse's *Global State of Information Security Report 2014* recorded significant growth in the volume of incidents in 2013. Nearly a quarter of the respondents cited data loss as a result of security incidents, representing a 16% increase over the previous year, and the average cost per incident was $531 (note that 7% of those surveyed reported losses in excess of $10 million dollars). This report also concluded that 18% of those surveyed did not know the frequency of incidents.

Respondents in our survey reported incidents caused by unsanctioned application use/lack of application security, breaches of wireless security /unauthorized network resource access and personal mobile device use as next most significant in terms of impact that these incidents had on the business. This further illustrates the security challenges presented by the growing diversity of network access methods and device usage.

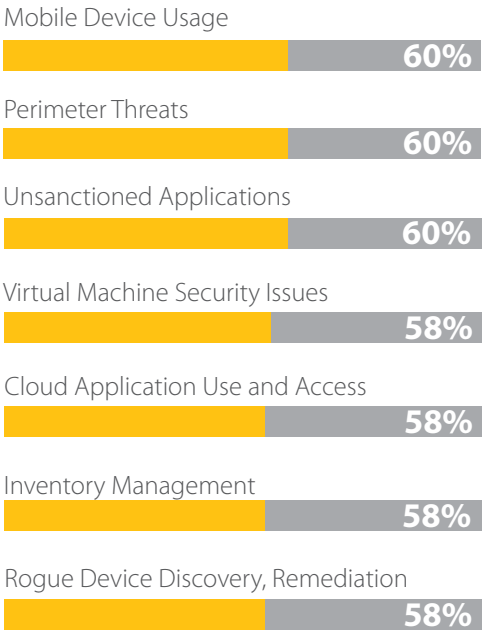
When ranked according to impact on a global basis, the healthcare sector was particularly affected by data leakage monitoring issues (60%) compared to other industries, with education scoring relatively high on four out of the six top threat areas compared to the other sectors. Whilst the financial industry appears to have seen less violations in the area of data leakage monitoring, it recorded slightly higher than average data leakage incidents compared to other industries. This could suggest that existing monitoring solutions may not be as efficient as they could be in detecting this type of vulnerability – a surprising finding given reputation risks and the potential to be fined for breaches of data protection by regulators that insist on detailed and accurate security auditing.

Malware and ATP attacks were rated as top priority by 23% of organizations within the UK, USA, and DACH on aggregate. When it comes to data leakage monitoring, the UK (50%) experienced slightly less violations compared to the US (54%) and DACH (56%) regions. Mobile security issues were ranked third in terms of impact significance for all global sectors except financial services where greater restrictions on device usage are more strongly enforced though companies in this sector still suffered more violations due to issues with endpoint data encryption than those elsewhere.

Mature Effective Policy Definitions, Technical Controls and Mitigation Capabilities



Below Average to Poor Policy Definitions, Technical Controls and Mitigation Capabilities



Comparing IT Security Perceived Capabilities

When asked to rank the efficacy of cyber security policy definitions, technical controls and mitigation capabilities in place within their organizations, an average of 17% of respondents across all three regions and industry sectors rated the controls listed in the above graph at the highest level (81-100%) in any one given control among the 24 referenced in the survey.

Current approaches to data protection, resource access controls, event logging/monitoring and system configuration were perceived to be implemented to a higher degree of maturity. At the other end of the scale, personal mobile device, perimeter threats, unsanctioned application controls and usage, inventory management, and virtual machine security controls were reckoned as most immature.

An interesting result came from system configuration being considered mature whilst endpoint compliance was seen as relatively ineffective despite a direct correlation between both which involves system hygiene and endpoint defense maintenance – a finding which suggests the interconnection between the two is not widely understood.

Perimeter threats and cloud application use and access controls were also given relatively low maturity ratings (between 0-60%) by 60% and 58% of respondents across all geographies and industries. This may indicate that next-generation firewalls are being slowly adopted into security architecture and suggests ongoing management and security challenges presented by cloud-based applications and services for both personal and business which are being accessed from desktop PCs and mobile devices from multiple locations.

Respondents in the healthcare sector across all three regions revealed themselves to be even more immature in personal mobile device security (65%) and endpoint compliance discovery and remediation (62%) compared to the cross industry aggregate (respectively 60% and 57%). The education industry appears to have more issues with virtual machine security (68%) and inventory management (65%) compared to industry aggregate (respectively 58% and 58%). Financial institutions in general had more mature security management capacity in aggregate compared to other industries.

Degree of Low Confidence That Poor Rated Security Processes, Tools and Technical Controls will be Improved in the Next 12 Months (Top 6 Areas Rated Somewhat to Not Confident)?

Perimeter Threats | Network Resource Access | Unsanctioned Application Discovery and Remediation | Mobile Device Use | Wireless Access Management | Active Host-Based Defense

Planned Investment and Upgrade Activities

Many organizations are optimistic about investing in resources which improve security management, control and response capabilities in the future. On average 33% were very confident that their organizations would improve those security measures deemed as being immature or less effective, however, just over half (54%) of respondents were somewhat confident.

However, when it comes to comparing those security measures deemed of poor maturity that would be improved in the next 12 months against the types of significant security incident which respondents reported they had suffered elsewhere in the survey (Tab 4), upgrade or investment plans do not appear aligned.

On aggregate, there were higher levels of confidence that sensitive data discovery and classification and security event logging and monitoring (37% very confident), compliance and audit documentation (36% very confident), identity/roles-based access control, sensitive resource access and host-based system back-up tools (all at 35% very confident levels) would be improved in the next 12 months. Areas of lower confidence for upgrade (cited as either somewhat or not confident) were perimeter threats, network resource access, unsanctioned application discovery and remediation, mobile device use and wireless access management, which may reflect greater challenges perceived in implementing and maintaining respective policies and enforcement tools.

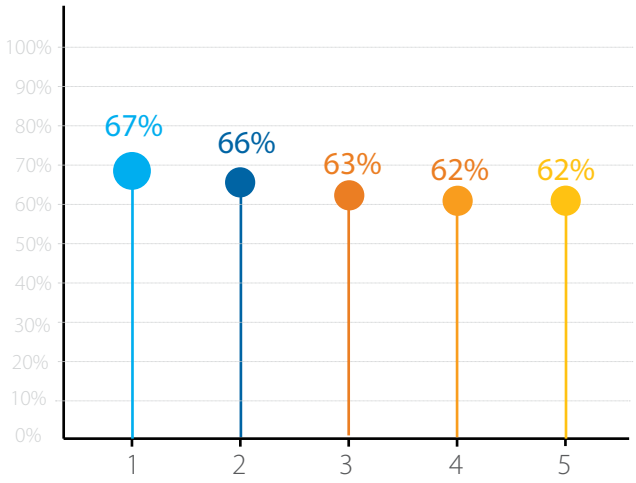
Overall only 20% were very confident that perimeter threats would be better mitigated, despite the fact these could be aligned to combat the growth of zero-day and targeted attacks.

Both geographical and industry differences are again apparent, however. The manufacturing industry demonstrated particularly high levels of certainty that tools to combat perimeter threats would be improved, for example, with an aggregate of 24% very confident across all three regions. But that figure drops to as low as 6% and 8% for the UK and DACH education sectors (where 94% and 92% are either not or only somewhat confident) and rises to as high as 32% in the US healthcare industry (where 68% are not or somewhat confident).

Elsewhere respondents from the finance sector in the DACH region were particularly confident that virtual network management tools would be improved (48% very confident) compared to their counterparts in the US (where only 29% expressed themselves very confident).

Aggregated across all three regions those most confident that security event logging and monitoring tools would be improved came from the financial services industry (45%) with education the least certain in this respect (only 33% were very confident compared to 67% who were either somewhat or not confident). Those in the education and manufacturing sectors were least sure (73% and 71% either not or somewhat confident) that security measures relating to personal mobile device usage would be improved.

Visibility and Control Confidence in Network and Endpoint Security (Top 5 with Least or No Confidence)



1 - Devices Outside of Configuration Standards

2 - Devices Outside of Security Standards

3 - Virtual Machines Outside of Configuration Standards

4 - Devices on the Network

5 - Remote Devices Outside of Security Standards

Remote Devices and Virtual Machines Outside Security Standards Present Most Fears

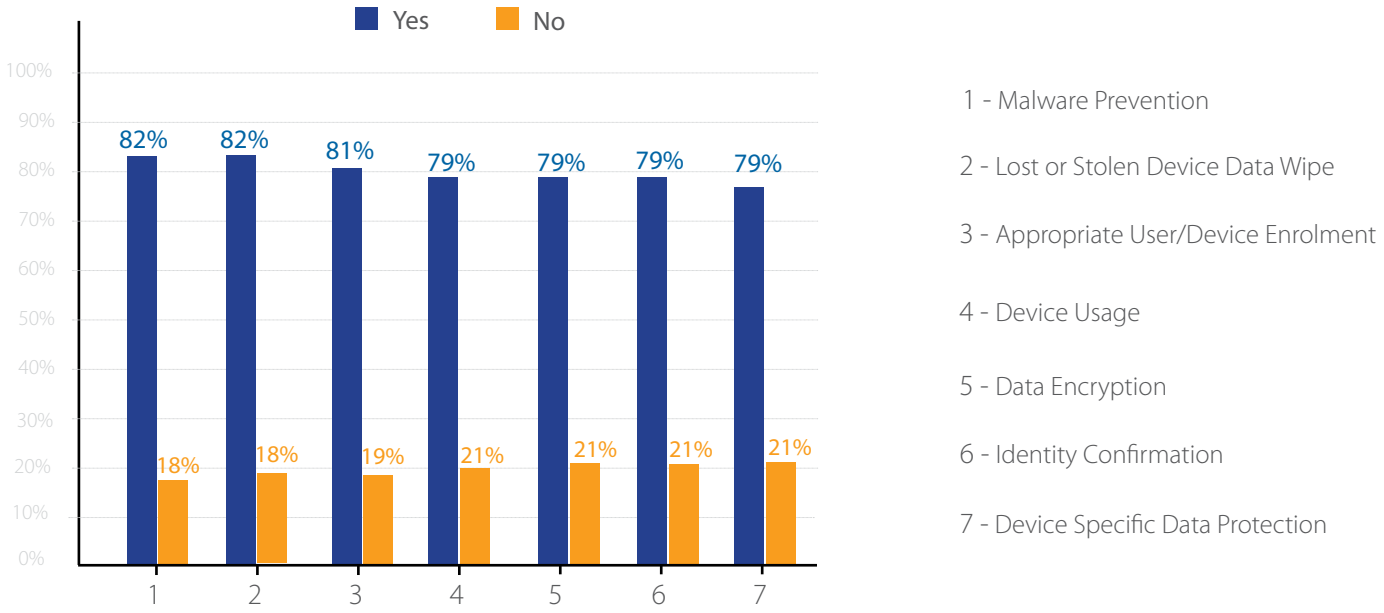
Despite respondents across all three regions being generally optimistic about the levels of visibility and control they currently have into network and endpoint security, the top five areas within which they indicated either lower or no confidence centred on knowing devices on their network, maintaining appropriate defenses on devices, virtual machine configurations, and remote devices not adhering to security policy.

Those in the UK showed significantly less confidence in their ability to control users on internal networks (57% said they were either not, or somewhat confident) compared to their counterparts in the US and DACH regions (both 49% and 48% respectively). And respondents in Europe also appeared slightly less sure of their ability to see and control external users using their networks (62% in DACH and 63% in the UK were either not or somewhat confident) compared to the US which recorded an equivalent figure of 59%.

This indicates that whilst a greater number of organizations are satisfied or overly confident with security provisions governing devices connecting to their networks which belong to their own staff, a sizeable proportion, particularly in the US, fear breaches from within more than most. With many industry frameworks specifying demonstrable endpoint configuration integrity for compliance purposes and network resource access control, anxiety concerning remote devices and virtual machines outside of security standards (rated as not or somewhat confident by 63% and 62% respectively of all industry sectors across all three regions) are well founded and suggest there is noted room for improvement to the device, user and application visibility and control.

This ties with findings recorded elsewhere in the report (page 5) which show compliance policy violation occurring an average of 2.6 times in the last 12 months across all three regions, but more (3.1) in the US than in both the UK (2.5) and Germany, Austria and Switzerland (2.2). On aggregate US respondents were more certain that their organization would invest in roles-based access control measures (38% very confident) than the UK (32% very confident) and DACH (35% very confident). Of those working in the German, Austrian and Swiss finance sector in particular, 61% were either not or only somewhat confident that roles-based access controls would be expanded or updated, compared to just 55% of finance companies in the US and 56% in the UK.

Does BYOD have an Impact in Terms of New or Additional Security Risks?



IT Consumerization Impacting GRC

A large majority of organizations believe that the Bring Your Own Device (BYOD) trend which sees employees expecting to use their own smartphones, tablets and other devices to access company networks and systems has an impact on their existing governance, risk and compliance (GRC) controls.

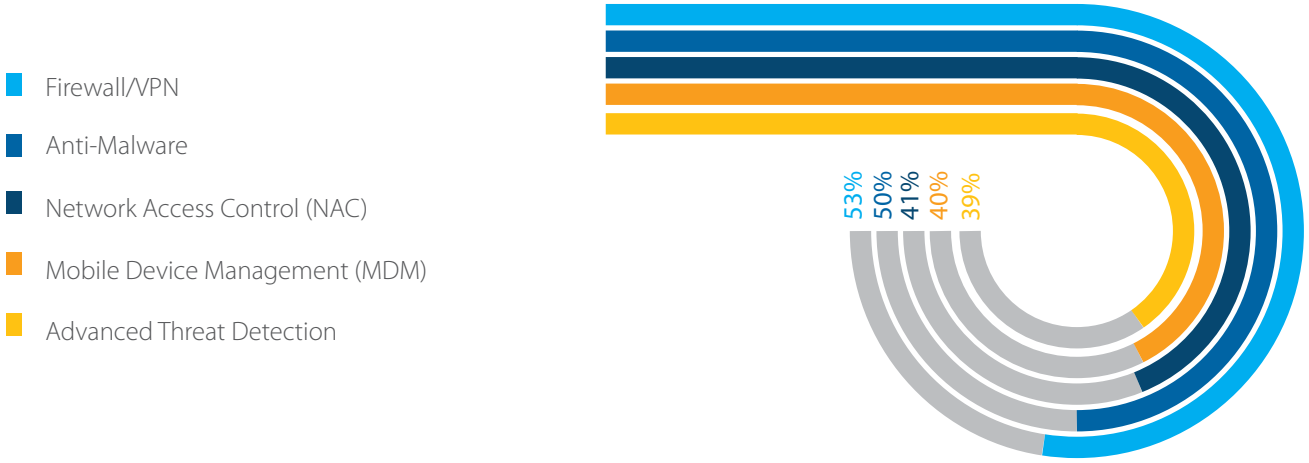
An average of 78% of all respondents cited that any one of the 14 popular BYOD controls referenced would have an impact on GRC. The need to implement malware prevention (82%), lost or stolen device data wipe mechanisms (82%), appropriate user/device enrolment tools (81%), device usage controls (79%) and data encryption (79%) on those devices are perceived to have the most significant GRC implications.

Controls deemed to be least impacted by BYOD were password management, rooted/jailbroken device isolation, software/hardware inventory management, blacklisted application identification and configuration identity. With a lower perceived impact on GRC, these controls could represent a gradual and softer control approach towards enabling BYOD.

Respondents from Europe cited data wiping, device specific data protection and data encryption as having a high impact on GRC with mean scores of 80%, 79% and 78% respectively. The equivalent figures were marginally higher for US respondents (83%, 80% and 81%) however, despite European organizations being perceived as subject to more stringent EU data privacy laws.

The findings echo the conclusions of the Worldwide Data Loss Prevention 2011 – 2015 Forecast published by research analyst firm IDC in June 2012, which posited that the growing use of consumer mobile devices and cloud services in the workspace was challenging established enterprise information security and IT risk management practices. To mitigate the threat, IDC advised organizations to implement strategies built on tiered levels of access, privileges and controls, and to assess security platforms which span network, device, user, application and data management in both on-premise and off-premise cloud architectures.

Perceived Technical Controls Interoperability Benefits



Security Integration to Enhance Visibility, Context and Mitigation

The survey results present an interesting picture of security solution interoperability. When asked to identify which security controls would provide significant benefits in terms of greater visibility, context and automated threat mitigation capabilities if better integrated with other controls, about half of respondents across all three regions highlighted firewalls and VPNs and anti-malware tools, and 40% cited network access control and mobile device management tools.

Gartner, in its *"Predicts 2014: Security Solutions"* research note published in November 2013, highlighted the criticality of context-aware security and security intelligence within future security technologies given the highly effective, targeted and complex nature of new security threats and their impact on IT security professionals. Gartner asserts that by 2016, 85% of security offerings will incorporate and leverage context-aware and or security intelligence feeds into their standard capabilities.

As the market is considering greater tool interoperability and intelligence exchange, the survey indicated a disparity between end user awareness and vendor platform capability to offer such integration. Perhaps surprisingly, vulnerability assessment, security information and event management tools, as well as intrusion detections systems were perceived by respondents to offer fewer benefits from an integration perspective.

Differences by region and vertical sector are again apparent. The integration of advanced threat detection (ATD) tools with other controls were seen as less beneficial in the UK and DACH regions (36% and 35% respectively) than the USA (46%), though perhaps indicating less penetration of this type of solution in Europe.

The integration of Firewall/VPNs (58%), anti-malware (54%) and GRC management (34%) tools were rated as potentially more helpful by the financial services sector when aggregated across all three regions, and also for vulnerability assessment, MDM and ADT in the US specifically. On aggregate, manufacturing rated interoperability value better with ADT, security event management, endpoint protection and patch/configuration management whilst those in the healthcare sector rated the benefits of integrating MDM as most significant (46%).

Frost & Sullivan's "*Continuous Compliance and Next Generation NAC"* report compiled in late 2013 highlighted the benefits of using NAC to leverage the flow of information swapped between firewalls, IPS, MDM, DLP, AV and SIEM tools in order to monitor overall security posture and to enable a more automated, policy-based response to security issues.

In the US, the benefits of NAC integration were rated more (49%) by those working for finance companies seeing potential advantages compared to the other three industries. In Europe, the perceived benefits of NAC integration for manufacturing, healthcare and education sectors were rated higher than that of the finance sector.

Conclusion: Confidence in Cyber Security Undermined by Contradicting Investments

IT security practitioners in all three regions were generally positive about the levels of their policies, technical controls and mitigation implementation, but the findings show contradictions in maturity, efficacy and enhancement. Beyond introducing security risks, any gaps also present an opportunity for organizations to better align investments and resources in order to cope with more advanced exposures and attacks and to better reduce management deficiencies.

In the past 12 months, almost all survey respondents across regions and industries have experienced a significant security incident - 39% experienced more than two and 16% experienced five or more. Phishing attacks, compliance policy violations, unsanctioned device and applications use, and unauthorized data access comprise the top issues. Operational complexity and an increasing threat landscape have impacted security management as more than 40% perceive that problem prevention, diagnosis and remediation are more challenging today than two years ago.

The top five areas to which IT security practitioners attributed lower or no confidence ratings centred on making sure remote, external devices and users, as well as virtual machines, accessing the network can be detected, identified and maintained to appropriate security and configuration standards and policies. This suggests an overall lack of faith in existing network device intelligence and system integrity, two core components of all compliance frameworks and security best practices – areas that should be "beefed up" given prevention and remediation challenges.

While securing mobile and personal devices was a recurrent theme across all geographies and industries, many organizations look set to invest towards better securing of enterprise mobility. Softer controls, such as configuration, inventory and network resources access management, were perceived as having less GRC ramifications than those of malware prevention, data wipe mechanisms, data encryption, and devices usage control. This can imply a more cautious and phased approach to enabling BYOD.

It is assumed that policy management, technical controls and response capabilities will improve in order to reduce the number and magnitude of security incidents that an IT organization will face. On aggregate, more than 30% of respondents had confidence that their organizations would improve those security measures deemed as being immature or less effective in their enterprise, but half (54%) were only "somewhat confident". The precise nature of that investment is critical however. Survey responses indicate some misaligned investment in areas outside of where more significant security incidents were incurred.

Respondents indicated they were most confident in improving sensitive data discovery and classification, security event logging and monitoring, compliance and audit documentation, host-based system back-up, identity/roles-based access control, and sensitive resource access tools over the next 12 months. They demonstrated comparatively less certainty that other areas of defense – such as controls for perimeter threats, network resource access, unsanctioned application discovery and remediation, personal mobile device usage, wireless access management and cloud application use and management – would be upgraded. This intimates either the extent of perceived difficulty to make headway in these areas or some reticence to divert or add investment. For example, only 20% were very confident in addressing perimeter threats, despite the fact that this is among noted controls to thwart zero-day and targeted attacks. This leaves room for security professionals and vendors to reassess their approach.

In its "Designing an Adaptive Security Architecture for Protection from Advanced Attacks" research note, Gartner also warned of the dangers of implementing '12 siloes of disparate information security solutions' and recommended an integrated approach which shares information between different elements.

Our survey findings suggest that IT professionals are still discerning where to apply tool and control integration capabilities. Interoperability can better advance prevention, diagnosis and remediation capabilities, areas with greater perceived security management challenges, and overall can provide an opportunity for policy-based automation – all of which could free up staff time and resources for other tasks within the business.

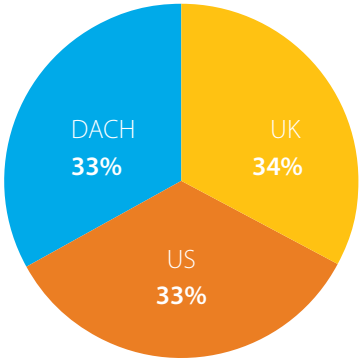
Demographics, Sponsor, Attribution

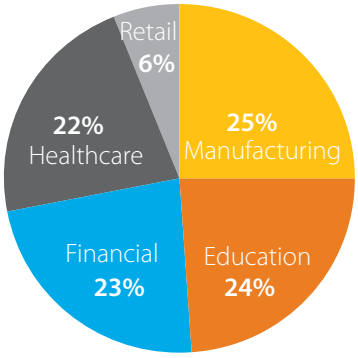
Demograhics

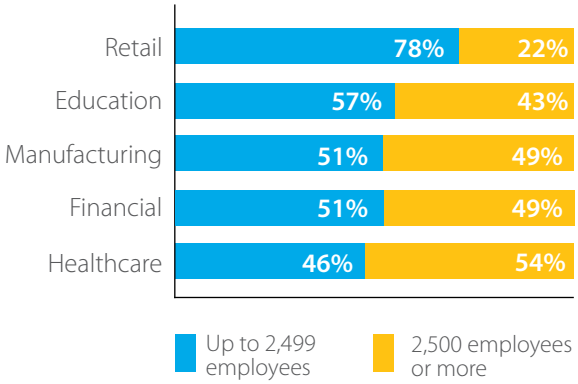
1,596 respondents:

54% Executive – Decision Maker
30% Director – Recommender
16% Practitioner – Influencer

Surveyed conducted and complied May-June, 2014.







Sponsor: ForeScout

ForeScout delivers pervasive network security by allowing organizations to continuously monitor and mitigate security exposures and cyberattacks. The company's CounterACT platform dynamically identifies and assesses network users, endpoints and applications to provide visibility, intelligence and policy-based mitigation of security issues. ForeScout's open ControlFabric technology allows a broad range of IT security products and management systems to share information and automate remediation actions. Because ForeScout's solutions are easy to deploy, unobtrusive, flexible and scalable, they have been chosen by more than 1,500 enterprises and government agencies. Headquartered in Campbell, California, ForeScout offers its solutions through its network of authorized partners worldwide. Learn more at www.forscout.com

Research: IDG Connect

IDG Connect is the demand generation division of International Data Group (IDG), the world's largest technology media company. Established in 2006, it utilises access to 38 million business decision makers' details to unite technology marketers with relevant targets from 137 countries around the world. Committed to engaging a disparate global IT audience with truly localised messaging, IDG Connect also publishes market specific thought leadership papers on behalf of its clients, and produces research for B2B marketers worldwide.

Attribution