

Gartner's Top 10 Security Predictions 2016

How to prepare for these new and known threats to enterprise security over the next two to four years.

June 15, 2016

Contributor: Kasey Panetta

(<https://web.archive.org/web/20160619165354/http://blogs.gartner.com/smarterwithgartner/author/kpanetta/>)

Today's security professionals battle threats from outside the organization as well as those from their own employees. But what about threats that they already know exist? The next few years will see a variety of attacks as well as progress in the technologies and processes that prevent them. At the 2016 Gartner Security & Risk Summit (<https://web.archive.org/web/20160619165354/http://www.gartner.com/events/na/security>), Earl Perkins (<https://web.archive.org/web/20160619165354/http://www.gartner.com/analyst/25748/Earl-Perkins>), research vice president at Gartner, presented the top Strategic Planning Assumptions (SPAs) for security in the next two to four years.

- 1 Through 2020, 99% of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year.**

Recommended Action: Companies should focus on fixing the vulnerabilities they know exist. While these vulnerabilities are easy to ignore, they're also easier and more inexpensive to fix than to mitigate.

- 2 By 2020, a third of successful attacks experienced by enterprises will be on their shadow IT resources.**

Recommended Action: Business units deal with the reality of the enterprise and will engage with any tool that helps them do the job. Companies should find a way to track shadow IT, and create a culture of acceptance and protection versus detection and punishment.

- 3 By 2018, the need to prevent data breaches from public clouds will drive 20% of organizations to develop data security governance programs.**

Recommended Action: Develop an enterprise-wide data security governance (DSG) program. Identify data security policy gaps, develop a roadmap to address the issues and seek cyberinsurance when appropriate.

- 4 By 2020, 40% of enterprises engaged in DevOps will secure developed applications by adopting application security self-testing, self-diagnosing and self-protection technologies.**

Recommended Action: Adopt Runtime application self protection (RASP) for DevOps. Evaluate less mature vendors and providers for potential security options.

- 5 By 2020, 80% of new deals for cloud-based CASB will be packaged with network firewall, secure web gateway (SWG) and web application firewall (WAF) platforms.**

Recommended Action: While concerns exist about customer migration to the cloud and bundling purchases, companies should assess the application deployment roadmap and decide whether investment is justified.

- 6 By 2018, enterprises that leverage native mobile containment rather than third-party options will rise from 20% to 60%.**

Recommended Action: Experiment and become familiar with native containment solutions. Keep in mind that enterprises with average security requirements should plan to move gradually to native containment.

- 7 By 2019, 40% of IDaaS implementations will replace on-premises IAM implementations, up from 10% today.**

Recommended Action: Enough limitations have disappeared on Identity as a Service (IDaaS) that companies should start experimenting on small-scale projects. While a clash of regulations could derail the increased implementation, companies should work to recognize the current limitations and benefits.

- 8 By 2019, use of passwords and tokens in medium-risk use cases will drop 55%, due to the introduction of recognition technologies.**

Recommended Action: Passwords are too entrenched in business practices to disappear completely, but companies should look for products that focus on development of an

environment of continuous trust with good user experience. Begin by identifying use cases, and press vendors for biometric and analytic capabilities.

9 Through 2018, over 50% of IoT device manufacturers will not be able to address threats from weak authentication practices.

Recommended Action: By changing the enterprise architecture, IoT introduces new threats. Early IoT security failures might force the industry towards authentication standards, but companies should identify authentication risks, establish identity assurance requirements, and employ metrics.

10 By 2020, more than 25% of identified enterprise attacks will involve IoT, though IoT will account for only 10% of IT security budgets.

Recommended Action: As IoT continues to grow, vendors will favor usability over security and IT security practitioners remain unsure of the correct amount of acceptable risk. Companies should assign business ownership of IoT security, focus on vulnerable or unpatchable IoT devices, and increase IoT-focused budget.

Read the Special Report: Cybersecurity at the Speed of Digital Business

(https://web.archive.org/web/20160619165354/https://www.gartner.com/doc/3332117?srclid=1-6963644879&cm_sp=gi_-_cysec_-_srpage)

Watch the webinar: The New Risks of Digital Business

(https://web.archive.org/web/20160619165354/http://www.gartner.com/webinar/3222617?srclid=1-6731481769&cm_sp=WBNR_-_SWG_-_SecurityRiskCampaign?cm_sp=swg_-_cta_-_webinar).

Learn more about IT security trends at the Gartner Security and Risk Management Summits 2016 taking place in National Harbor, Maryland

(https://web.archive.org/web/20160619165354/http://www.gartner.com/events/na/security?cm_mmc=swg_-_event_-_securityNA), Tokyo

(https://web.archive.org/web/20160619165354/http://gartner-em.jp/srm2016/?cm_mmc=swg_-_event_-_securityjapan), Sao Paulo

(https://web.archive.org/web/20160619165354/http://www.gartner.com/events/pt/la/security?cm_mmc=swg_-_event_-_securitybrazil), Sydney

(https://web.archive.org/web/20160619165354/http://www.gartner.com/events/apac/security?cm_mmc=swg_-_event_-_securityaustralia), Mumbai

(https://web.archive.org/web/20160619165354/http://www.gartner.com/events/apac/security-india?cm_sp=swg_-_event_-_securityindia) and London

(https://web.archive.org/web/20160619165354/http://www.gartner.com/events/emea/security?cm_mmc=swg_-_event_-_securityemea). Follow news and updates from the events on Twitter at #GartnerSEC

(<https://web.archive.org/web/20160619165354/https://twitter.com/search?q=%23GartnerSEC&src=typd>).

© 2016 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.