Have we reached “peak tech” for security’s sake? The trend towards simplification in 2024

John Swanson, Global Security Portfolio Lead, Uvance

In 2024, a new attitude towards technology complexity will become mainstream. In searching for greater security against cyber threats, we predict that simplification will become the new compass point for CISOs.

A difficult transition

Cybersecurity threats, made worse by the rise of AI, are now so extreme that organizations may need to reconsider the risks associated with maintaining complex technology systems. The potential damage from breaches is existential; modern business governance will no longer tolerate the threats to revenue, reputation, and stakeholders’ wellbeing. As a result, organizations must find effective methods of internal education and governance to manage the risks of budget holders independently adding new hardware, software, and datasets into an estate — via SaaS, for example.

This will be a difficult transition. Business stakeholders are accustomed to implementing technology on their own initiatives. But momentum is turning in a new direction. Gartner has captured this with its “minimum effective mindset”. It’s a strategic approach that advocates streamlining cybersecurity to the minimum necessary to achieve better business outputs with the positive by-product of less burnout among professionals.

Multi-cloud is a potential security risk

Cloud is one very obvious way to achieve greater simplicity. Hyperscalers take security very seriously and have the incentives and resources to ensure highly secure environments.

For this and many other reasons, cloud adoption rates remain high, suggesting that the ongoing simplification of IT estates is an unstoppable trend. It brings with it, however, the new challenge of managing security in multi-cloud and hybrid environments. CISOs must ensure the cross-cloud security of any new cloud-native solutions that are onboarded.

Convergence and consolidation are helping

Another trend in CISOs’ favor is the shift towards convergence and consolidation of technologies. Innovations increasingly incorporate functionalities that were previously separate — think smartphones and super-apps. Consolidation simplifies security by reducing the plethora of security technologies in an enterprise (80 is not unheard of) to a much smaller, better-integrated set of technologies (although this is a number that will never be one).

Reducing complexity provides other benefits beyond security. Streamlined technology systems reduce overall cost. With less to manage day-to-day, IT security teams can focus on high-value strategic initiatives. Simplified environments also enable greater agility to adopt innovations that emerge.

Challenges remain

Of course, simplification is not without challenges. Migration to cloud-based systems can be costly upfront. Personnel may require retraining. And business processes may need reconfiguration. Leaders must thoughtfully manage these disruptions during transitions.

The public cloud also raises valid data sovereignty concerns. Some regulated industries may be unable to utilize hyperscale cloud solutions. Companies handling sensitive customer data may prefer on-premises systems. Multicloud solutions mitigate risks but do not fully eliminate them.

Action points for CISOs seeking simplification

IT leaders should conduct thorough assessments to determine ideal environments for their needs. In some cases, legacy modernization may better balance security and cost. But for most organizations, cloud migration combined with simplification will be the most prudent path forward.

Adopting packaged solutions for needs like ERP or CRM is preferable to highly customized software. Leaders should scrutinize integrations between systems and retire unnecessary touchpoints. And teams should be prudent in adopting new hardware, software, and data sources. Each addition increases complexity and risk.

Focusing budgets on streamlining business processes and aligning personnel around simplified technology systems will pay dividends. Yes, it will limit some flexibility and customization. However, it enables organizations to thrive in a climate where security risks have reached untenable levels.

Towards a new paradigm

Security remains one of the highest priorities in enterprise IT/OT. And that's not going to be changing in the near term. However, the lack of progress toward zero-trust security —to take a single example of an approach that might improve matters — suggests that most organizations are struggling to make meaningful progress. Gartner estimates that fewer than 1% of companies have measurable Zero-trust program in place. Without rapid improvement, simplification is the only viable solution.

The events of 2023, from high-profile breaches to AI dangers and opportunities, were a wake-up call. The distributed work revolution accelerated technology complexity. As we enter 2024, technology leaders will move towards the "less is more" stance advocated by Gartner. The companies that realize this and simplify their estates will be best positioned for the future.

To find out more, visit: https://www.fujitsu.com/global/themes/security/

John Swanson
Global Security Portfolio Lead, Uvance

John has fulfilled many Information Security leadership roles across Public and Private sectors including security programme and capability leadership, consultancy (advisory and delivery), Security Operations Centres and Security Pre-sales functions.

He is responsible for developing Fujitsu's compelling Cyber security go to market propositions, which also underpin Fujitsu's wider Applications, Hybrid IT, Digital Workplace and Industry Sector aligned propositions. John focuses on the business aspects of Information Security and how Fujitsu can help clients enhance the strategic and operational maturity of the information security capabilities within their organizations.