Ovum
TMT intelligence | informa

A Buydown for Risk: Why Data Security is a Must

Core and edge security are important, but protecting data itself must be the bedrock

Publication Date: 03/01/19

Rik Turner

Summary

Catalyst

Enterprises face a plethora of different types of risk nowadays, including business, operational, market, and systemic risks. The advent of the World Wide Web and the evolution of connectivity generally, and e-business in particular, have brought with them an ever-present threat of cyberattacks, and cyber-risk has joined the range of risks to be factored into the cost of doing business.

With cyberattacks now inevitable and data breaches highly likely, it is logical that companies should evaluate their investment in security by their ability to reduce risk. In analyzing investment trends, however, Ovum detects a curious imbalance in the allocation of funds.

Investments in the many forms of end-point and network security, hereafter referred to generically as edge security, continue to grow apace. Identity management technology, which Ovum calls core security, grows more slowly, but is still a well-established, multibillion-dollar business. A third area of activity, namely data security, is by comparison relatively neglected. This white paper will argue that protecting the data itself must be the central pillar of enterprise risk mitigation and the base on which edge and core security should rest.

Ovum view

Enterprises are increasingly aware of the need to protect their systems and users from cyberattack. This is a good thing, as it indicates a growing awareness of security risks, no doubt underpinned by the never-ending stream of headlines about companies, many of them household names, and the major data breaches they have suffered (in recent times, the likes of Facebook, Google+, Equifax, British Airways, Deloitte, DHS, and eBay, to name but a few).

This scenario has, inevitably, pushed many companies to double down on investments in technology to keep threat actors and malicious code out of their environment, as well as to stand guard on data leaving it, in order to block any unauthorized outbound traffic. This focus on edge security is perfectly understandable, as is their continued spend on technologies related to the management of identities, whether those of their employees, business partners, or customers (what Ovum calls core security). There is even talk, as companies increasingly enable their employees to work from anywhere, of the notion that "identity is the new perimeter" in IT security.

Both edge and core are eminently deserving of enterprise investment and attention. However, securing the data itself, both via obfuscation techniques and by deploying database security (i.e. database activity monitoring, plus analysis of database log events), is essential to underpin both and, as such, must be front and center of enterprise strategy for managing risk. As threat actors continue to find ways through the corporate edge and to hijack the accounts of legitimate users (particularly those with the greatest access privileges), protecting a company's sensitive data assets, and ensuring that authorized data activity is appropriate, are the cornerstones of mitigating enterprise risk.

Time and again we see well-built edge defenses breached and bamboozled, and even companies with mature systems for managing privileged access have been duped by account hijacks. Only by investing in the security of the actual data can companies hope to reduce the risks to the business.

Obfuscation renders stolen data useless, while database security enables the detection and blocking of attempts by attackers to access data, even if they are posing as legitimate users.

Key findings

- Edge and core have higher profiles than data.
- Both edge and core security have shortcomings.
- Data security is better at risk mitigation.

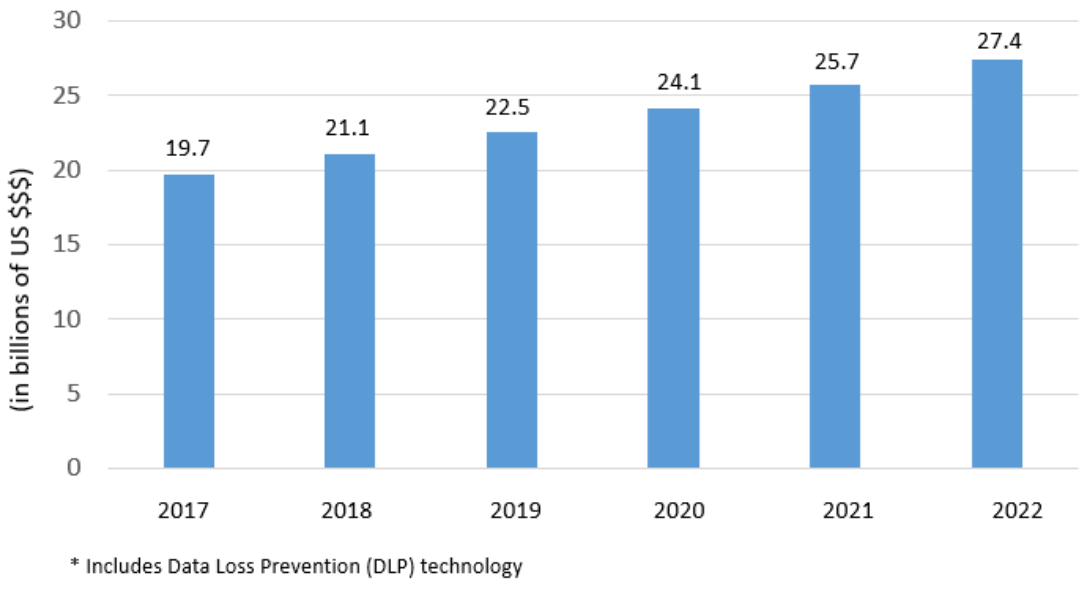
Edge and core have higher profiles than data

Data breaches raise the profile of edge security

Edge security comprises all the multiple technologies designed to sit on the real or notional edge of a corporate network to keep bad people and code out (firewalls, anti-malware, intrusion detection/prevention, and so on), as well as valuable data in (i.e., data loss prevention, or DLP).

This type of security currently has a high profile, with both enterprises and the general public, thanks at least in part to the never-ending succession of data breaches hitting the headlines. Indeed, it has caught the public imagination to such an extent that it now has a more "thrilling" name: rather than information or IT security, it is increasingly referred to as cybersecurity. It is also a major focus of tech spending.

Figure 1: Edge security market forecast*



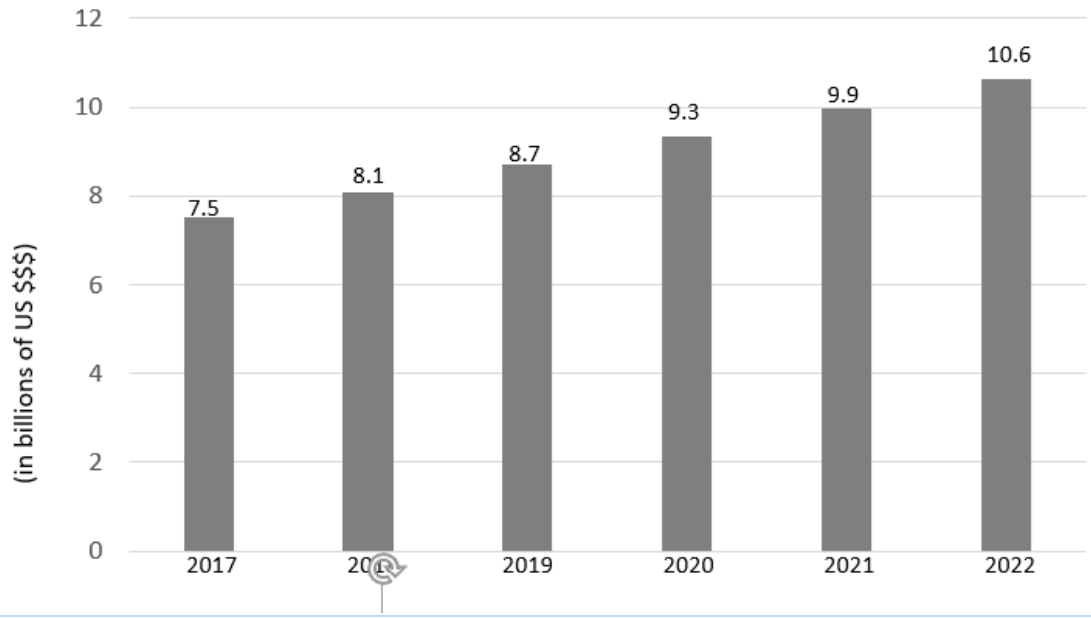
Source: Ovum *Software Market Forecasts: Security, 2017–22*

Identity is a sine qua non of a functioning enterprise

A second category is core security, which is another way of referring to identity management technologies (identity and access management, or IAM; privileged access management, or PAM; and even customer identity and access management, or CIAM).

This is a veritable mainstay of IT operations, since no major enterprise can operate without exercising control over what its employees can and cannot access when they come onto its network. Furthermore, IAM has been "democratized" in recent years by the advent of identity-as-a-service, or IDaaS, whereby an IAM platform resides in the cloud and is delivered as a service rather than as expensive on-premises software, making it available to smaller companies.

Figure 2: Core security market forecast



Source: Ovum *Software Market Forecasts: Security, 2017–22*

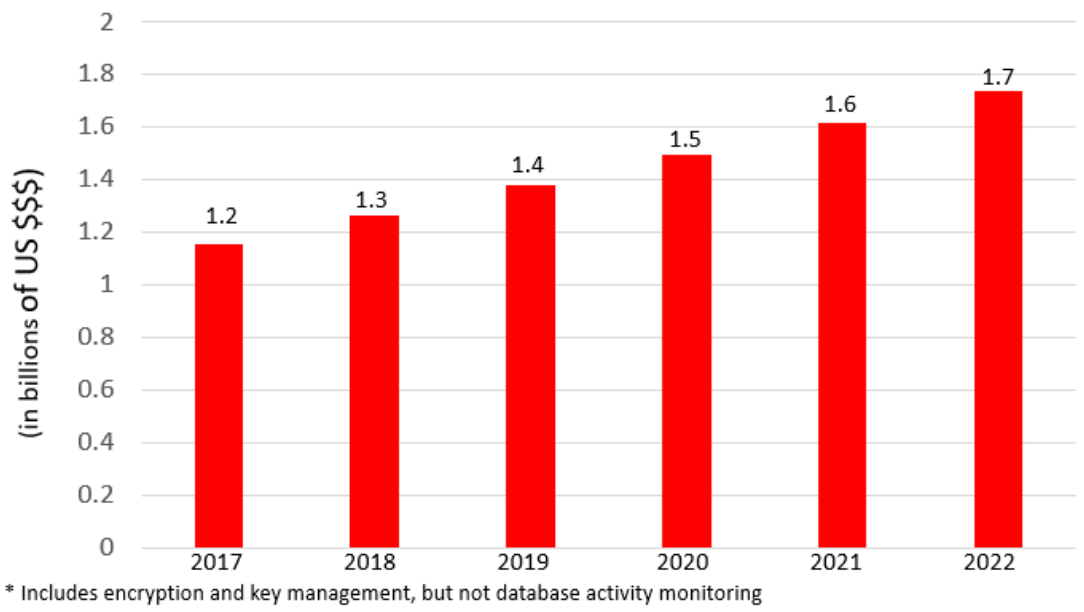
Meanwhile, the privileged-access segment of the market has grown in importance as hackers have, for obvious reasons, taken to targeting the credentials of users with access to all areas.

Data security is less of a focus for enterprise spending

The third area of security involves protecting the data, whether by obfuscating it to render it useless to anyone gaining unauthorized access, or by protecting the database in which it is held. In contrast to edge and core, data security is often a rather overlooked part of the defender's armory.

Encryption has a reputation for being complex, particularly the key management that is essential to its success. Tokenization is often delivered as a service for companies that need to demonstrate PCI compliance, but is seldom seen outside that use case. Database security as defined above, meanwhile, is barely on the radar for many organizations.

Figure 3: Data security market forecast*



Source: Ovum *Software Market Forecasts: Security, 2017–22*

It is Ovum's contention, however, that data security of all types must be at the heart of any enterprise's defenses if it is to manage and mitigate risk.

Both edge and core security have shortcomings

Edge security is fallible

Despite hefty investments in edge security, enterprises continue to be breached, as new attack methodologies are developed at an ever-increasing rate. Furthermore, the evolution of the dark web, where exploit kits can be acquired for pennies on the dollar, makes it even easier to mount attacks in the current environment.

Indeed, the very proliferation of edge security tools, generating hundreds and even thousands of alerts daily, represents an increased security risk in its own right. We know, for instance, that FireEye sandboxes had flagged the anomalous behavior that was part of the huge Target breach in 2013, but the company's security team was too overloaded to notice.

… and it only looks at inbound traffic

The escalating threat landscape and evolving attack methodologies mean that, sooner or later, an attacker will find their way into a corporate infrastructure, and once they are inside, perimeter security is powerless to address the attack. Furthermore, perimeter-security approaches fail to catch insider threats, which include malicious users, careless users, and compromised users (in scenarios such as account hijack).

With cloud migration, data now resides in hybrid environments, both on premises and in the cloud. Edge security does not provide visibility into who is accessing what data, especially, as is the case in cloud, when a database can be spun up dynamically by anyone.

So great are the problems raised by the threat of data overload and alert fatigue that the industry is now investing heavily in the branch of artificial intelligence (AI) known as machine learning to try to improve matters. The hope is that by training algorithms to match patterns, breach detection rates can be improved and incident response accelerated. Indeed, there is talk in some quarters of going beyond this automated detection approach to harnessing AI for actual prediction.

Edge is also blind to insider threats

Finally, the issue of authorized and unauthorized data access is beyond the scope of edge security. As such, that part of corporate security infrastructure is of virtually no use in protecting against insider threats, whether from disgruntled employees or compromised accounts.

Core security can be noisy

The key challenge for core security is how to determine whether a legitimate data activity is appropriate. Just like edge security, IAM and PAM can generate huge amounts of alerts, which overwhelm security analysts. Without the context of data activities, they can end up generating more noise than actionable security insights.

… and it has its own vulnerabilities

Core security also has its security issues. The very rise of PAM is indicative of the fact that regular IAM has proven to be too weak, so that the credentials of privileged users within an organization were perceived to require extra protection. Yet even the more robust approach of PAM can struggle to address the challenge posed by well-funded, patient attackers who trawl social media for information about developers, sysadmins, or C-level executives, which can then be used to help gain access to their user credentials.

Thus, if an observant hacker finds the name of a sysadmin's puppy on Facebook, or discovers that in their spare time they are huge fans of World of Warcraft, this can narrow the search for their passwords, or help develop a suitably compelling spear phishing email. Indeed, the evolution of social networking sites, and its resulting impact on notions of what information should remain private, has significantly compounded the problem of protecting credentials.

Data security is better at risk mitigation

Breaches are now when, not if

It has become something of a truism that, in the current state of cybersecurity, being breached has become a question of when, not if, for most enterprises. As a result, edge security vendors have shifted their focus from prevention to detection and response, which initially means mitigation, then remediation. This change, while it represents an acceptance of the new reality, is also an admission of defeat.

As a consequence of this disheartening scenario, enterprises now include cyber as one of the many types of risk that they must manage, alongside but distinct from commercial, financial, systematic, or market-wide risk. It can be thought of as a subset of operational risk, though for the purposes of insurers, for instance, cyber-risk is a separate and standalone category.

Data security reduces risk more effectively than core or edge

In the digital age more than ever before, data constitutes the crown jewels of every enterprise, and it is precisely what cybercriminals are after when they penetrate a corporate infrastructure. In this context, data security is a vital ingredient in any enterprise risk-management strategy, with investments in data security correlate directly to risk mitigation.

Investments in breach reduction are a necessary part of cybersecurity spending, while maintaining an up-to-date infrastructure for identity is a key part of digital transformation. Edge and core security are both extremely important. However, the return on investment in data security, in terms of both improved security posture and risk reduction, is both more immediate and unparalleled in its efficacy.

Data breaches represent direct costs, in terms of the time and resources spent communicating with customers, possible monetary settlements of lawsuits, and – depending on the sector – fines paid to authorities. In addition, there are the indirect costs of lost business and customers, the so-called reputation hit (with a knock-on effect on a public company's share price) and, of course, loss of market share.

Compliance is a further driver for data security

Compliance requirements, most notably the European Union’s General Data Protection Regulation that came into force in May 2018, have brought increased attention to data privacy and the need not only for more controls on data movement, residency, and access, but also for better security practices.

The increasing overlap of compliance and security as it relates to data is key to why data security reduces risk more effectively than security provisions for the edge or the core. Database security is a key component within data security, so let us now turn to specifically to that area of technology.

Database security has operational benefits

Database security can have significant operational benefits. It can, for instance, uncover unknown, rogue, and even simply disused databases within an organization's infrastructure, making it possible for them to be shut down, thereby reducing the corporate attack surface.

It also identifies all the places where a company's most sensitive data resides, helping focus the mind of corporate defenders on where they need to concentrate their efforts. To quote the old IT security aphorism, "You can't protect what you can't see." Using database security, companies can gain visibility into who is accessing data, when it is being accessed, and how it is being used. Companies can also pinpoint critical threats to critical data by applying machine learning and security analytics, which also allows security teams to better address the problems raised by event overload and alert fatigue.

Aside from the obvious contribution this makes to mitigating risks to confidentiality and integrity and reducing the threat of external and internal data theft, the increased visibility can identify gaps in the

company's IAM process, such as excessive rights or the existence of dormant accounts, thereby helping to fix IAM. As such, it can also be seen as enhancing the operation of core security (i.e., identity services), in that it provides a clear picture of who is doing what, when, and how.

And, of course, the effective use of database security has a key role to play in helping companies comply with the multiple data privacy and security regulations now in place or about to be introduced around the globe.

Recommendations for enterprises

Think data security first

In formulating security policy, begin by focusing on risk. Data security can reduce risk in a more effective manner than either core or edge security and, as such, should be prioritized when you are defining your security posture. Once you have got data security right, then you can decide what to do in core and edge.

Data security is a key differentiator in the data-driven world

If done right, data security can enable an organization’s business growth without constraining the flow of data.

Security goes beyond edge and core

There is no doubt that continued investment in edge security, from both a network and end-point perspective, is a worthwhile endeavor, and indeed, new forms of protection are continually emerging to enhance this area of security. Equally, the way you deliver identity services, particularly to employees and business partners/contractors, can now benefit from the ubiquity and facility of cloud computing. However, in order to reduce risk, securing your critical data should be your first priority, with edge and core security serving as additional layers to be wrapped around data security. Keep abreast of the evolution of data security technologies, with regard to both emerging data obfuscation techniques and the ability to monitor who is accessing the information in a database, as well as what is being accessed, when, and where from.

Appendix

Author

Rik Turner, Principal Analyst, Infrastructure Solutions

rik.turner@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

CONTACT US

ovum.informa.com

askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing

Boston

Chicago

Dubai

Hong Kong

Hyderabad

Johannesburg

London

Melbourne

New York

Paris

San Francisco

Sao Paulo

Shanghai

Singapore

Sydney

Tokyo