alkira

WHITEPAPER

Shadowless IT

Eliminating the Threat from Shadow IT in the Cloud Era

Shadow IT – spending on IT that happens without the knowledge or control of the IT department – presents several challenges: uncontrolled cost, governance problems and exposure to organisational risk. Shadow IT also has an upside. It can result in solutions to business problems that IT departments take too long to solve.

Shadow IT has been enabled by the cloud and the proliferation of software-as-a-service applications. Enterprises are ambivalent about shadow IT, which may undermine governance and control, but enables innovation. They are also pragmatic: the cloud genie is out of the bottle and is not going back.

IT leaders recognise that business-led application development is desirable and inevitable - **83%** in a recent survey believe business users will be more involved in software development in future and **92%** think that with the right controls in place users could be entrusted with low-code tools. Gartner believes these tools could account for **65%** of enterprise application development by 2024.

With so much activity escaping the gravitational pull of the IT department “How do we eliminate shadow IT?” may be the wrong question. CIOs should be asking instead how they can foster creativity and agility while managing the security risks associated with shadow IT.

Above all, in an environment of steadily rising security threats and increasing risks of financial and reputational damage, CIOs should be extremely alarmed at the prospect of unsanctioned network activity. Whatever is not visible on the network is a source of potential harm.

Why Shadow IT?

- As product development shifted to the cloud, product engineers have become the de facto responsible parties for setting up cloud networks and security. Their focus is on product development not infrastructure enablement, to which they often pay minimal attention
- The controls and constraints on the IT department, in the interests of governance and compliance, prevent it from being responsive or agile
- Applications developed by IT don’t meet users’ expectations or needs
- Business users are constantly looking for new ways to analyse information
- They’re also looking to exploit the ever-increasing power of personal end-user devices
- Cloud and SaaS make it easier than ever to access applications

Even where IT is running like a well-oiled machine, it can't compete with the attractions of shadow IT. The IT department is constrained by competing priorities, testing cycles, corporate procurement, security and governance policies, and availability of skills, training and support. The shadow IT alternative will almost always be quicker and easier to obtain.

How long is the shadow?

The average company uses 1083 cloud services, only 108 of which are known and 975 are unknown

Gartner estimates that **35%** of IT spending is in departmental or discretionary budgets outside the control of the IT department

Frost & Sullivan reports that **80%** of staff admit to circumventing IT processes

Cisco estimates that **80%** of the software used by end users is not cleared by IT (that figure rises to **83%** for IT staff themselves)

of CIOs admit to being bypassed by line of business sometimes. **31%** say they are routinely cut out of purchasing decisions

Upsides

1. **Employees create their own solutions –** overcoming delay in getting what they need from IT and creating higher employee engagement

2. **Better alignment with business need** – nothing gets lost in translation

3. **Improved productivity –** solutions can remove obstacles to people doing their jobs

4. **Reduces the burden on the IT department –** giving people access to white-listed pre-approved solutions or licensing them to develop their own, can save work and leave IT to get on with core business

Downsides

Unknown and uncontrolled cost is a perennial headache. Other issues include:

1. **Procurement –** the organisation may not be able to take advantage of negotiated discounts

2. **Waste –** alternative services mean the organisation may not get planned returns on investment in IT. Unsanctioned purchases may be abandoned after one or two uses

3. **Productivity –** purported gains from shadow IT may be offset by time wasted by business users setting up new systems without formal training. Proliferating collaboration tools – such as the 57 different file-sharing applications used by the typical enterprise (McAfee) – may reduce not enhance collaboration

4. **Data integrity –** as corporate data is manipulated in different systems there may be multiple versions of the truth

5. **Business logic –** even if the data is reliable, unproven analytic tools in the hands of inexpert users may result in unreliable logic shaping business decisions

6. **Regulatory compliance -** uncontrolled data flows jeopardise compliance with data protection laws and regulations governing financial services, healthcare and other industries

Further headaches for the IT department include:

- **Asset management –** unauthorised software makes it difficult to check if licensing terms are being met, creating legal risks

- **Support –** already overstretched departments may struggle to support shadow IT users, particularly as IT may only be called in at the point of crisis

- **Lifecycle management –** shadow IT is less likely to be documented creating problems down the line with maintenance and upgrades

- **Back-ups –** poor disaster recovery is a weakness of many cloud-based applications

- **Testing –** untested applications could compromise the entire IT infrastructure. Networking and security requirements may be ignored by DevOps and “citizen developers” in line of business in the interests of quick results

- **Configuration management –** shadow IT systems are unlikely to be included in configuration management databases (CMDB) that define the relationships between different systems, which may result in compatibility issues.

Security

Gartner estimates that one third of successful attacks made on enterprises breach shadow IT resources. Experian Data Breach Resolution claims that 80% of breaches result from employee negligence and that negligence thrives in the shadows where unsanctioned applications and devices are a major source of vulnerabilities and root causes are hard to identify.

- Fewer than 10% of cloud services meet data security or privacy requirements. The average enterprise suffers 20 cloud-related security incidents a month (McAfee)
- Nearly half (47.5%) of cloud-based apps reviewed by Netskope scored “poor” in that company’s Cloud Confidence Index and only a fifth (22%) rated “good” or “excellent”
- The cloud is responsible for delivery of 61% of malware
- 36% of phishing campaigns go after cloud app credentials

Alkira – removing the networking barrier

Cloud networking is complex. Long after enterprise applications are ready to go, the network and security teams are working out how they can be deployed with the performance and protection they need.

Business users and DevOps have taken the line of least resistance with SaaS applications or with resources spun up in the cloud without the involvement of network and security teams.

Uncontrolled proliferation makes it almost impossible for security and networking teams to track what is connected to the enterprise network. New virtual resources (VNets and VPCs) are appearing all the time, creating a snowflake environment where everything is different and IP address conflicts are around every corner. Connecting and securing this mess is a major challenge.

Reducing the time to provision highly secure cloud networks using Alkira Cloud Services Exchange® (CSX) removes another of the major factors that drives IT into the shadows.

The Alkira platform provides end to end visibility of all the resources on the network. It enables micro segmentation, advanced routing and zero trust security, and ensures that all application traffic whether it originates in the enterprise data center or in an Internet hosted SaaS application is firewalled in the cloud without performance-draining backhauling to the data center.

Visibility is key

Managing shadow IT typically relies on one of two approaches: bringing in consultants or intensified policing by the IT department. Both approaches are expensive and typically involve

months of work on cultural issues, business process reviews and communications.

Auditing and asset management tools are useful, but add to the array of tools already in use and identify problems only after they occur. Enterprise infrastructure is too critical and the threat level too high to continue taking a piecemeal and retrospective approach to monitoring and control.

Visibility has become exponentially harder in the cloud era because there are so many cloud and cloud provider concepts to get to grips with to understand the entire network and security around it.

IT needs a complete picture of:

1. Existing virtual networks in use and new ones being created
2. The various resources deployed inside and outside these networks
3. Connectivity to and from the virtual networks and associated resources
4. Where resources are exposed to unsanctioned access
5. Utilization of these resources

Alkira gives enterprise IT teams (network, security and devops) visibility into their cloud deployments from a network connectivity, security, and utilization perspective. Besides giving administrators greater visibility of their existing cloud deployment, it informs them of shadow IT scenarios as they happen, enabling IT to get ahead of the problem.

Here are some of the shadow IT use cases successfully mitigated by the Alkira solution:

Unauthorized addition of cloud workloads resulting in sprawl and subsequent cost

Misconfigured overlapping IP address ranges resulting in routing issues

Unsecured ingress and/ or egress Internet access resulting in security risks

Unused configured resources resulting in unnecessary expense

Unauthorized configuration changes resulting in policy non-compliance

Summary

CIOs acknowledge that it is neither possible nor desirable to control everything. They see the benefits of greater user involvement in making and buying applications. They appreciate the need for greater business agility and how this could be enabled by ceding some of the authority traditionally reserved by the IT department.

Many recognise that with appropriate rules in place, the right tools and adequate training, the business imperatives and maverick tendencies that led to shadow IT can be formalised and legitimised, and the worst of the threats it poses neutralised.

They also see how such a permissive regime could benefit their own departments, giving them greater oversight of IT activity in the rest of the organisation and leaving them free to focus on core systems.

But while the CIO may have to let go of some areas of procurement and development, other aspects of the IT function are non-negotiable. No one should be able to connect anything to the network that goes unnoticed.

The right networking and security infrastructure can provide the enterprise guard rails to allow shadow IT activity to be brought out of the shadows without compromising business innovation and agility.

2001, Gateway Place,
Suite 610W, San Jose,
CA 95110

+1 855-925-5472

www.alkira.com