The Hidden Threat of Shadow IT in Modern Enterprises

September 2024

Carlos Alves

IT departments are typically unaware of the existence of applications & devices being used by individual employees or entire business units, hence the term “shadow IT.

Emerging Cyber Risk

In the digital age, companies are more connected and reliant on technology than ever before. While this brings enormous benefits, it also introduces new vulnerabilities, some of which remain critically under-addressed. One such growing risk is the proliferation of *Shadow IT*—the use of unauthorized devices, applications, and services by employees within an organization. Although often dismissed as a minor issue, Shadow IT presents a significant, and often overlooked, cybersecurity threat.

What is Shadow IT?

Shadow IT refers to the use of technology (software, hardware, or cloud services) within a company without the knowledge or approval of the IT or CISO divisions. These tools are frequently adopted by employees seeking faster or more convenient ways to do their work, bypassing cumbersome approval processes. Examples include using personal cloud storage for sensitive files, third-party messaging apps, or even unsanctioned project management tools.

Why is Shadow IT a Growing Cyber Risk? Here are some reasons.

Lack of Visibility and Control:
When employees use unapproved applications, security teams lose oversight, making it impossible to enforce security protocols or ensure that sensitive data is adequately protected. Without visibility, these tools can easily become backdoors for cybercriminals.

Increased Attack Surface:
Each unauthorized device or application increases the attack surface. If these tools are not patched regularly or lack the appropriate security measures, they become easy targets for malware, ransomware, or data breaches.

Regulatory and Compliance Violations:
Many industries have strict compliance requirements around data handling, especially when it comes to personally identifiable information (PII). Shadow IT can easily violate these regulations, exposing the company to legal penalties and fines, not to mention reputational damage.

Data Leakage and Loss:
Sensitive data stored on personal devices or external cloud services is often outside the control of the IT team. This can lead to accidental or intentional data leaks, particularly if the external services do not provide robust security protections like encryption or two-factor authentication.

So, why aren't the majority of the companies reacting to this?

Despite these risks, many companies continue to underestimate Shadow IT, reason being;

- **It’s Hard to Measure:** Most organizations struggle to quantify the extent of Shadow IT use because, by definition, it operates outside formal channels.
- **Business Pressure for Speed:** Employees adopt these tools to get their work done faster. Organizations are often reluctant to crack down too hard, fearing it could slow down productivity.
- **Lack of Awareness:** Leadership may not fully understand the security implications of Shadow IT, especially if breaches or incidents have not yet occurred.

Addressing the Threat…

To mitigate the risk of Shadow IT, companies MUST take a proactive approach, in order to:

1. **Improve Visibility:** Invest in tools that monitor network traffic to detect unauthorized applications and devices.
2. **Educate Employees:** Regularly train staff on the risks of Shadow IT and the importance of adhering to approved processes.
3. **Create a Secure Culture of Flexibility:** Encourage employees to collaborate with IT when they need new tools. Offer fast-tracked approval processes for new technology requests to reduce the temptation of using unsanctioned apps.

4. **Update Policies:** Ensure company policies are clear about the use of unauthorized tools and implement enforcement measures for violations.

Ignoring Shadow IT is no longer an option. As the technology landscape becomes more complex, companies must tackle this emerging risk head-on, or they risk becoming easy prey for increasingly sophisticated cyberattacks.