Client security: Shifting paradigms to prepare for a cloud-only future

Microsoft Core Services Engineering (CSE, formerly Microsoft IT) has been working to fulfill the company’s commitment to be a cloud-first organization. Roughly 90 percent of our IT resources are now hosted in the cloud, and we’re looking ahead toward a future where all devices that connect to those resources will be cloud-connected. Moving vital business assets to the cloud, where they are accessed by cloud-connected client devices, requires a new security paradigm—one that gives us more control over information while keeping pace with the changing security landscape.

As part of our digital transformation, we have been moving from a traditional hybrid infrastructure toward a modern management environment that uses cloud identities and services. Modern management is helping us streamline how we support our mobile workforce and keep work and customer data secure. As we look to the future, we are aligning our current initiatives and planning future investments to help us overcome the potential risks and challenges of securing vital business assets in a device-agnostic, cloud-only organization.

The following diagram illustrates some of the elements in traditional, modern, and future IT (more than five years away) security.

Finding the correct balance between worker productivity and the need to control and protect sensitive information is one of our main challenges. Modern management has introduced operational efficiencies and is increasing worker productivity by providing access to work data anytime, anywhere, and from any managed device. We can support a mobile workforce and bring-your-own-device (BYOD) scenarios, and we are placing more emphasis on cross-platform support for our corporate apps.

By moving to an environment that consists of cloud-connected clients, we are shifting our focus from securing information at a client level to protecting data in the intelligent cloud and controlling access at the app level. We will have to accommodate an increasing number of devices that we manage, and the proliferation of Internet of Things (IoT) devices that make up the intelligent edge of cloud-enabled devices makes client management more challenging.
Moving data protection from the client to the cloud

For over 20 years, we built client-based security mechanisms that provided more than adequate protection within the “castle” walls of our network and data centers. When we began moving more resources to the cloud, and as employees became more mobile—often using personal devices for work—it became clear that we needed to adjust the way we think about security. Trying to adapt traditional security methodologies to the changing landscape would be costly and would not adequately address risk for all the diverse device manufacturers, standards, and platforms.

Modern management has introduced agentless, client-based security measures, such as antimalware and auditing, that are helping increase device security with centralized security, intelligence, and machine learning services that function in the cloud. They are helping us extend protection to data that resides outside of our infrastructure, in the cloud, and on devices that we manage but do not own.

Table 1 shows how we have begun transitioning some of the traditional client-based security to more centralized and cloud-based protection, considering our goal to address those IT functions in an intelligent edge, intelligent cloud-only environment.

**Table 1. IT security functions in the landscape today and in the future.**

<table>
<thead>
<tr>
<th>IT function</th>
<th>Today</th>
<th>Future</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>We are assessing our information security ecosystem, looking for areas to reduce data sprawl, centralize services, and reduce the number of devices that require disparate security methods to safeguard access.</td>
<td>Decrease complexity by ensuring data resides on centralized, approved cloud platforms with strong, pervasive identification capabilities that allow protection to travel with the data, such as Azure Information Protection.</td>
</tr>
<tr>
<td>Protect</td>
<td>We are using the management functions of numerous protective products across a wide array of platforms and locations. We rely on Windows-centric protection at the client including Windows Defender, Firewall, and BitLocker. <strong>Windows 10</strong> introduced agentless protection technologies including Windows Defender Advanced Threat Protection (ATP), and Windows Information Protection.</td>
<td>Critical data is centralized on cloud platforms, allowing organizations to focus on native capabilities built for the cloud platform. We are looking forward to more centralized solutions that drive intelligence. For example, behavioral analytics can be used to screen user commands to prevent unauthorized or malicious file propagation.</td>
</tr>
<tr>
<td>Detect</td>
<td>Our system requires collection, processing, and storage of many events across a constantly changing ecosystem of devices and applications. Threat Analytics and Windows Defender ATP use centralized cloud services that help us detect issues more quickly.</td>
<td>Focus on automated intelligence to collect and analyze anomalous events from centralized cloud platforms that retain and process critical data, such as Threat Explorer in Office 365 Threat Intelligence.</td>
</tr>
<tr>
<td>Respond</td>
<td>Before Windows Defender ATP, tracing an incident through all the potential systems (users, servers, and cloud) and services that an event may affect could require too many resources. We can now see the scope of impact and have</td>
<td>Focus only on data managed on cloud platforms and the inherent capabilities provided by the cloud platform, with potential for auto-remediation.</td>
</tr>
<tr>
<td><strong>remediation actions that are just a click away.</strong></td>
<td><strong>Recover</strong> Clearing events from user devices, the datacenter, and cloud services results in a sharp decrease in productivity. <strong>Focus on restoration of cloud services only.</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Protecting data with cloud-based, data-centric controls**

Moving toward a cloud-only model can help reduce security investments that focus on the client and network layers because we can use data classification to help ensure that sensitive data never leaves the cloud. Cloud data storage gives us the ability to continuously fingerprint and pattern-match to detect anomalies or unauthorized access. Strong identity controls, business continuity and disaster recovery (BCDR) mechanisms, scalability, availability, ease of use, and manageability make data access and use seamless.

Centralized systems, with cloud-based, data-centric controls, will improve upon traditional mitigation techniques, such as network-based security perimeters and data loss prevention (DLP) services that primarily focus on limiting access to data in transit. Now, we prioritize technologies that do not reside on client machines or require an agent. We are also looking at virtualized applications and services that use platform-provided cloud security services to help bring us closer to a more secure future in the cloud.

Figure 1 illustrates the future IT environment that is built on cloud-based, data-centric controls.

Figure 2. Data-centric security at the cloud layer

Centralizing data and services in the cloud will enable uniform classification and treatment of data. Centralization offers better insight and development opportunities to improve both coverage and effectiveness of access controls and encryption.
Strategic planning for a cloud-only future

We are evolving into a cloud-first company, while also preparing for a cloud-only future. This requires some strategic planning to help us prioritize our activities and investments as we move forward. Some of our focus areas, based on current initiatives and future plans, are:

- Begin moving identities to the cloud.
- Look to cloud-based device management solutions to help streamline device management in the organization.
- Adopt cloud services, including centralized and standardized solutions for forensics, analytics, monitoring, and antimalware.
- Drive internet-only connected offices and clients.
- Use conditional access to help control access to data.

We are also in the process of rationalizing our current and future infrastructure investments. Areas where we are and are not placing emphasis as we plan future investments include:

- We will have a reduced need for network perimeter-based controls on the user-side edge.
- We will no longer require datacenter infrastructure to support client-based connectivity.
- We will be replacing client-based security controls or legacy controls with security services provided at the platform level—for example, Windows Defender ATP.
- We are investing in cloud-based provisioning and controls.

The future of data security

Like other organizations, we must make strategic decisions about current and future investments to build a cloud-centric corporate environment. We are centralizing data repositories in the cloud to help streamline management and analysis functionality. We are reducing our reliance on network services and traditional network perimeter-based security controls, and prioritizing our future investments toward being cloud connected and internet only.

The future of client security is focused around securing data where it resides—in the cloud. Our initial data protection investments in the cloud are already helping to substantially increase enterprise security in client protection. As we continue to streamline cloud security, we can create tighter and more uniform controls. A more unified approach will give us a holistic view of corporate security controls, risks, and exposure. This centralized view will allow us to capitalize on more sophisticated artificial intelligence and machine learning security measures.

For more information

**IT Showcase**

- Creating security controls for IoT devices at Microsoft
  microsoft.com/ITShowcase
- Core Services Engineering tackles security
- Expedition Cloud
- Building cloud apps using the Secure DevOps Kit for Azure