End-to-End Security Architecture for Cloud Workloads

Suman Banerjee, CTO, StratusWorX & Professor of Computer Sciences, Univ. of Wisconsin-Madison
Alex Tate, Executive Vice President, Field Operations, StratusWorX

Introduction

Businesses choose to migrate data and applications to the cloud for the benefits of on-demand resource scaling and cost savings. StratusWorX, with its virtual, cloud-hosted workspaces, provides disruptively new opportunities that save time, effort, and cost. However, some may feel concerned about the security of their remote resources, mission critical services, and sensitive data when they move such services to the cloud. Can the cloud really be secure? The surprising answer is that, if implemented correctly, cloud applications offer significant security advantages in addition to the other benefits. The security benefits stem from the greater potential for monitoring and software control afforded by centralization. We, first, explain this intuitively.

If we consider a business enterprise, with devices distributed across multiple disparate locations, each running its individual operating systems and software applications, each individual device, network, and site needs to be separately secured. If software versions, firewall rules, and applied security patches are not consistent across all devices, adversaries can penetrate the infrastructure. More specifically, the attack surface in this distributed and diverse infrastructure is quite large and an attacker simply needs to just find a single weak link in it to compromise security.

Now, contrast that with the opportunities of StratusWorX's cloud-hosted workspace, where all user devices reside in a fairly homogeneous environment in a few data centers across the world. This reduces the attack surface significantly. Further, the business enterprise using StratusWorX Cloud Workspace can utilize consistent security policies, that can be easily applied across the entire infrastructure, minimizing the amount of security misconfigurations that creep in due to human errors in the process. Thus, at a conceptual level, StratusWorX is already better positioned to provide greater security to any business enterprise through its cloud-hosted infrastructure than if the business used the on-premises incumbent.

While the cloud computing infrastructure is amenable to greater security, several challenges need to be addressed to make this a reality. As cautious adopters of cloud computing are aware, there are numerous threats lurking on the Internet against cloud-hosted services. In this white paper, we focus on a few of the most urgent threats that may make a business owner or network administrator wary about moving to cloud computing, all of which are effectively tackled by the StratusWorX solutions. They include:

- Unauthorized access to user or administrator accounts, whether through social engineering, password brute forcing, or software vulnerability
- Data exfiltration through improperly secured databases
- Running outdated and vulnerable software that allows remote code execution or privilege elevation
- Unreliability, loss of service, or unrecoverable data

The StratusWorX solution is designed to overcome these challenges. This white paper explains how we leverage the unique capabilities of cloud computing to overcome these security threats.

StratusWorX Virtual, Cloud-hosted Workspace

StratusWorX's core innovation lies in the creation of individualized and highly customized virtual desktop environment in the cloud, replete with native software applications, which appear to end users as if they are running locally on any personal device – desktop, laptop, tablet, and even a phone. It eliminates the need for SMBs and their employees to own and manage highly provisioned and expensive computers (desktops or laptops) or servers for daily IT activities.

While the concept appears simple, there are significant challenges with making the user experience of some complex cloud-hosted applications similar to the experience of running them on local desktops. In particular, some software applications have highly dynamic visualizations and user experience is quite sensitive to perceived responsiveness, such as modeling software tools (SolidWorks, AnSys, AutoCAD) used by architecture and manufacturing firms, or video and image editing software tools (Adobe Premiere Pro, Autodesk Maya) used by marketers and media agencies. In many such examples, high jitter and delay in rendering desktop screens from the cloud-hosted virtual machine (VM) to the local display, can make such applications almost unusable. StratusWorX has developed a software infrastructure, to address this performance gap of highly interactive applications (often requiring complex computations) using techniques such as differential encoding, compression, intelligent streaming decisions between the cloud-hosted virtual desktops and end user displays in personal devices, and smart virtual machine placement.

A core innovation of StratusWorX is Zero-Touch, Zero-Delay™ provisioning of this infrastructure, whereby a non-IT person can provision or decommission all of its users' cloud-hosted workspaces including their applications and work environments in a matter of minutes. In particular, StratusWorX simplifies the technology acquisition process for small and medium businesses with its "Single Pane of Glass" approach which consists of fully integrated cloud, infrastructure, applications, storage, security, and backup package accessible through any device with a web browser. Our platform helps customers to run any application in the public cloud, on-premises, or combined at a lower cost. It is trusted by multi-billion-dollar tier-one enterprises, small and medium businesses and carriers for both internal and customer-facing solutions.

StratusWorX has also introduced numerous other innovations in the creation of this holistic solution. Core among them is the end-to-end security architecture and mechanisms that provide improved security properties for end-user devices as well as the infrastructure of the enterprises. This white paper focuses on overall end-to-end architecture which is a key component of the service offerings.

StratusWorX Security Shield

The StratusWorX Security Shield leverages multiple battle-hardened technologies as well as in-house tools that we are actively developing to guard our customers, and our own services, against threats from all angles. We have specialized toolkits for detecting malware, blocking malicious websites, halting DDoS attacks and botnet behavior, preventing attacks on management and administrative consoles due to insecure authentication, and protecting cloud services from hijacking attacks. Additionally, we take a proactive approach to monitoring systems and logs to thwart novel threats as they occur. All these capabilities make cloud security one of our key service offerings for small and large businesses alike.

Security infrastructure and users have many components which include:

a. Application security
b. Continuous monitoring of systems and activities
c. Securing the network
d. Information Security
e. Resilience
f. Regulatory Compliance

Some of our more innovative components are in our design of specific techniques, such as the virtual clean room – an extreme form of security usable in high risk settings, use of virtual functions in network security, and design of a continuous authentication for our system. We describe these components in turn.

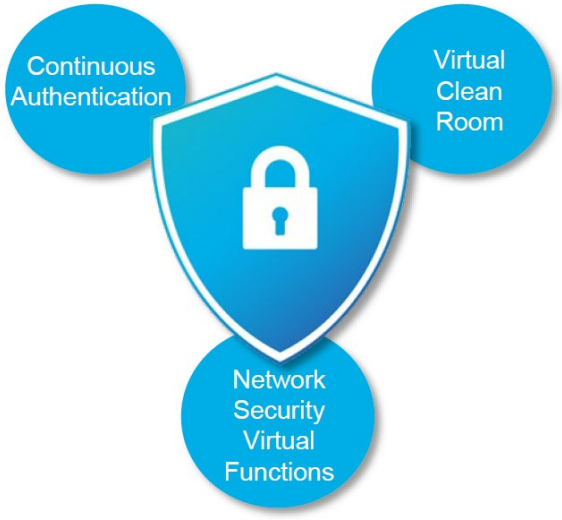


FIGURE 1: SOME OF THE PILLARS OF INNOVATION IN THE STRATUSWORX SECURITY SHIELD.

A) Application Security

Traditional corporate networks rely on careful management of desktops distributed throughout the enterprise campus. Keeping physical equipment secure and up to date is costly and time consuming. Furthermore, attempts to continue managing hardware securing company intellectual property in the face of a bring-your-own-device (BYOD) regime amplify the complications. StratusWorX leverages the strengths of cloud computing to offer a tractable solution to businesses. Centralized virtual machine instances are easy to manage and automate. Through an automated software infrastructure, the latest patches for different applications are identified and routinely applied to all user accounts, thereby minimizing their vulnerabilities. In addition, we have introduced an innovation in form of “disposable” or “ephemeral desktops” that are employed when applications or websites are deemed less secure with a risk to potentially infect the user’s account or other infrastructure.

Use of Ephemeral Virtual Desktops

An ephemeral virtual desktop is a virtual desktop instantiated in the cloud environment which is short-lived. It is launched on demand from a user’s desktop to run one or more specific applications, especially if these applications are considered risky or vulnerable to external threats. If certain applications being used by a user or an organization using StratusWorX falls below designated security requirements, they are not allowed to be run in the user’s virtual workspace directly. Instead, they are launched in these ephemeral desktops to which the user has full access. The actions are contained within this ephemeral desktop. The user interacts with this ephemeral desktop using a visual interface, over remote desktop protocols. No actual software of the ephemeral desktop ever runs in the user’s workspace. Once the activities of the user are complete, the results are retained and the desktop itself is destroyed. This limits the potential damage such vulnerable applications can cause to the organization’s infrastructure.

Using this combination of techniques, StratusWorX enables businesses to control the software and network traffic allowed in a secure network environment. We use industry-recognized, third-party tools as well as in-house tools to scan customer virtual machines for vulnerabilities and security issues and promptly report to the appropriate team for remediation. Any potential security issues are tracked until they have been resolved.

Ephemeral desktops protect user content from vulnerable applications or websites while allowing full access to such content.

Secure User Authentication

StratusWorX centralizes security management and locks down the desktop with ultra-secure, single sign-on and continuous authentication. Password fatigue leads to users creating insecure passwords, and corporate policies of password expiration tend to exacerbate the problem. Users wish for a better way to handle authentication, and helpdesks waste countless hours recovering lost passwords.

StratusWorX is at the forefront of innovations in user authentication. In addition to improvements through multi-factor authentication (MFA) and single sign-on (SSO), StratusWorX is pioneering work in a solution called continuous authentication. Continuous authentication monitors aspects of user behavior throughout their interaction with a system, so beyond the initial authentication challenge. This includes the user click activity, keystroke velocity, files opened, mouse and cursor activities, and websites visited. All of these data streams are processed through machine learning algorithms to detect account compromise in real time.

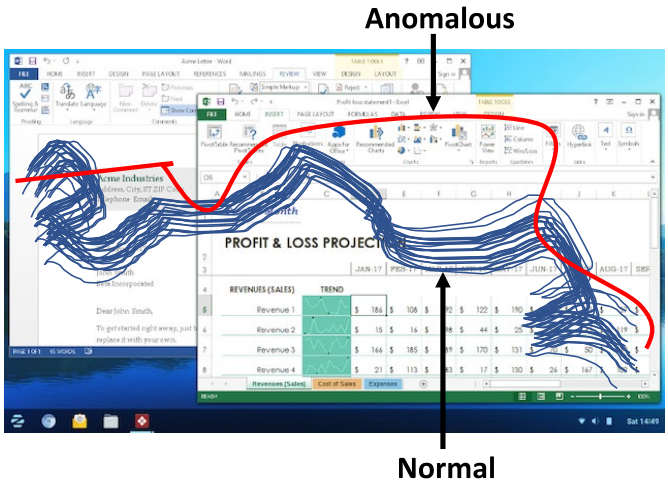


FIGURE 2: CONTINUOUS USER AUTHENTICATION BY EXAMINING MULTI-DIMENSIONAL ATTRIBUTES OF USERS.

Whatever the cause, from a compromised password to a screen left open during a work break, continuous authentication provides a constant layer of defense. The remedial action taken when a potential compromise has been detected is configurable by the customer. Possible actions are locking the session or requiring intervention from a dedicated security team.

In addition to the above elements protecting our environment, we leverage a higher standard of password protection when our hosted Active Directory is leveraged. StratusWorx protects against the current database of known hacked passwords which currently totals over 555,000,000 entries. This ensures our users are choosing passwords that have not been reported to be known exploits.

In addition, we can add custom entries to this listing on a per-request basis to allow for customers/users to request that certain passwords are not allowed with their hosted deployment.

Web Safety

Users require access to the web for information and collaborative software. This is unavoidable but poses a unique challenge for securing a user's cloud desktop, as malicious websites are a common vector for malware. Recognizing this, StratusWorX has built in a multi-layered approach to web security. As part of our strategy, we use a state-of-the-art DNS-based system that protects users against a wide range of malicious and inappropriate content including ransomware, phishing, and vulnerability exploits. It works at the DNS layer, so it does not rely on inspection of HTTPS traffic, thus keeping legitimate traffic secure. Additionally, classification and configurable filters make it easy for businesses to pick and choose the types of content to allow or deny depending on their needs.

Data Security

Businesses require assurances that their valuable intellectual property and sensitive customer data are stored securely at all times, so we provide the tools necessary to control and manage disk encryption for data at rest in storage or on virtual machines. This provides assurance against outside tampering and makes it easy for customers to comply with industry regulations. We make it easy for customers to create and control their own keys for encryption.

Additionally, StratusWorX goes above and beyond the standard techniques for malware and ransomware scanning by additionally monitoring file system integrity. We validate the integrity of operating system files by comparing the, against a known baseline to quickly identify changes that may indicate an attack.

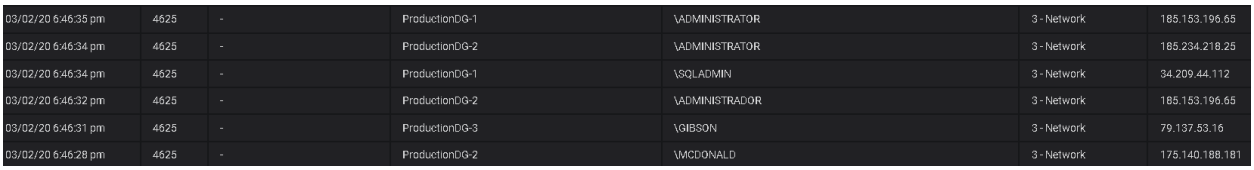
B) Continuous Monitoring

StratusWorX employs a comprehensive security information and event management (SIEM) system that draws on the wealth of data from multiple sources that are available in the cloud environment. Data sources include user activity streams, network traffic, and virtual machine system logs. StratusWorX systems with configuration hooks and rules can produce real time alerts and take automatic proactive actions, for example, to block suspicious login attempts, thwart port scanning, and put a stop to DDoS attacks. We continue to innovate in this space by applying novel machine learning approaches. One such technique is our continuous user authentication technology.

The following is a screen capture of our monitoring solution for the StratusWorx environment. This environment combines feeds from Security Center, Log Analytics and Agent-based information. Monitoring these environments would normally require multiple tabs and independent knowledge of each aspect. StratusWorX has consolidated these views for ease of management by StratusWorx staff, partners and customers. StratusWorX has built the monitoring with RBAC (Role Based Access Control) to ensure that only pertinent data is accessible to partners and customers that have been extended monitoring privileges. StratusWorX monitors a myriad of parameters to create a cohesive security picture. Monitored parameters include brute force attempts, successful logins, malicious network traffic, anti-malware alerts, and critical updates

that are missing. StratusWorX generates several terabytes of security logs daily and can tailor the security environment according to customer and partner specifications also.

The following screenshot is an example of failed login attempts via RDP to a cloud environment. Leveraging Active Directory (AD) logs polled by the StratusWorX Security Center, we can see which server the attacker attempted to log into as well as the account utilized. StratusWorX logs the remote IP address and region of the originating attack in a separate database as a prelude to the drill down into the detailed list of attacks.



Continuous User Authentication

Continuous user authentication is a state-of-the-art technique developed by the StratusWorX team for ensuring fail-safe user authentication beyond the initial multi-factor challenge. It is based on user-behavior profiling and machine-learning techniques that perform a risk assessment in real-time and can immediately respond to suspicious activity such as unusual file-access patterns. Continuous authentication provides a unique second layer of defense against not only compromised account credentials, but also man-in-the-middle attacks and account hijacking from forgetting to lock the computer screen. We enable the business to configure the threshold for response and the actions to take, which can range from locking the user's session to requiring review by the security team.

Continuous user authentication raises the bar for workspace compromise, as users are continuously being validated for their identity, unlike traditional methods that rely on one-time entry of passwords, including those that use multi-factor authentication, at the beginning of each session.

C) Securing the Network

StratusWorX uses aggressive firewall settings and other techniques to secure the boundaries of customer cloud desktops and lock down inbound traffic to virtual machines. Many cases of large-scale data leaks are the result of misconfiguration and unintentionally open databases. We guard our customers' valuable data by instituting a *default deny* policy. Additionally, our virtual clean room technology works through a single, highly scrutinized entry and exit point in the customer network, which is the SSL-protected remote desktop session for the client.

StratusWorX has created a company culture that emphasizes security in everything we do. Part of creating a security-oriented culture is instituting formal processes for system configuration changes. As an example, any change to firewall configuration is documented and put through a review process with our security team. We also routinely audit firewall settings and other security measures at least twice per year. These review processes in addition to others ensure we avoid the kinds of mistakes that would leave our customers open to attack.

This screen below is of a typical Layer 3 Network Security Group. We allow 80/443 for redirection to the Gateway and only 3389 internally on the VNET so RDP is not open to the Internet. The same methodology applies to SSH, WinRM and Grafana with the added step of only allowing specific IP addresses or ranges. We also remove unnecessary public IP addresses from the Domain Controller, workspaces and other infrastructure to reduce the attack footprint. A secondary TOGGLE 3389 exists to allow support IP ranges and addresses to remote into the environment. These are built by default within our environment to ensure we have a security-first approach to securing our user environment from a Layer 3 and Protocol standpoint.

ALLOW_VNET_RDP	3389	Any	VirtualNetwork	VirtualNetwork	Allow
TOGGLE_RDP_IP_ONLY	3389	Any	[redacted]	Any	Allow
DENY_RDP_INTERNET	3389	Any	Internet	Any	Deny
ALLOW_GRAFANA	9090	Any	[redacted]	Any	Allow
TOGGLE_SSH_IP_ONLY	22	Any	[redacted]	VirtualNetwork	Allow
DENY_SSH_INTERNET	22	Any	Internet	VirtualNetwork	Deny
ALLOW_GW_PORTAL	80,443	Any	Any	172.20.5.6	Allow
Allow_WINRM	5985,5986	Any	[redacted]	172.20.5.4	Allow

Virtual Clean Room

The ideal in terms of computer security, the clean room, is a computing environment air-gapped from the public Internet. Access can be controlled by physical barriers, and data leaks can only be the result of deliberate action.

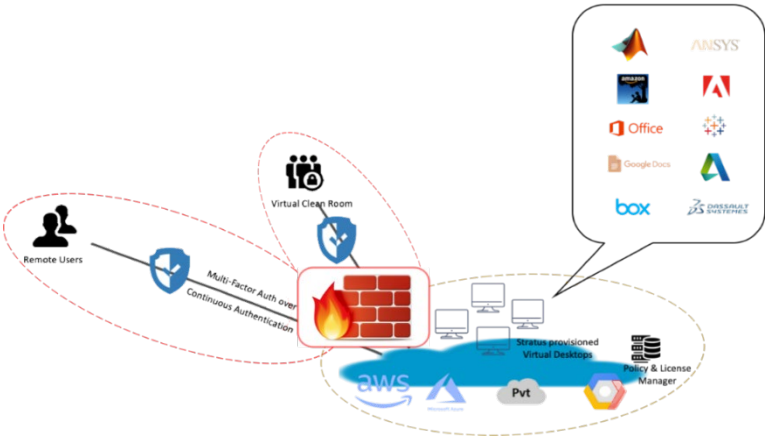


FIGURE 3: THE VIRTUAL CLEAN ROOM AND OVERALL APPROACH TO SECURING THE NETWORK.

Strict security comes at the cost of worker productivity. In the typical work environment, information needs to be shared freely between team members, and a wide variety of online productivity and collaboration tools need to be readily accessible. Drawing upon the clean room idea for inspiration, StratusWorX introduced the concept of a virtual clean room.

In the virtual clean room, the desktop environment is a carefully and automatically managed virtual machine. StratusWorX empowers businesses to specify rules and policies that control the software that runs on the desktop environment as well as where and how business artifacts are to be stored. StratusWorX ensures that connections in and out of the desktop are secured in order to provide an environment with similar security controls as a clean room but with lower cost and inconvenience. We can do this on a large scale because of the many tools and processes that we have put into place as described in the StratusWorX end-to-end security architecture.

A large US-based StratusWorX customer trusts our virtual clean room environment for administering an optical backbone that carries classified federal government data.

D) Information Security

Many larger StratusWorX customers struggle to keep up with personnel changes and all the system privilege changes associated with those. This problem is exacerbated by the many systems requiring user-privilege updates across a panoply of websites, databases, and internal systems. Typically, this results in sticky privileges. Privileges are added when needed, but not reliably dropped. StratusWorX addresses the problem of sticky privileges by centralizing an active directory system and all user privileges across managed applications and services. We simplify user permissions through an easy-to-use role-based access control system. By lowering the overhead of managing user privileges, we see fewer mistakes.

We understand that our customers worry not only about external threats, but also about their exposure to cloud service providers. Acknowledging the situation, we follow best practices to

safeguard our customers' data and maintain their trust. Among our internal policies, we apply strict restrictions on employee access to customer resources after provisioning has been completed, and we empower our customers to generate and control their own encryption keys, thus making it impossible for StratusWorX employees to access their most sensitive data. While our support team still needs access to customer resources from time to time in order to do their job, each access is gated by customer consent both as a matter of policy and by technical controls.

E) Resilience

There is an inherent risk of catastrophic failure and disruption when businesses move their internal data and services to a single cloud provider. The StratusWorX hybrid cloud solution provides a unique level of resiliency by seamlessly replicating data and services across public cloud providers as well as potentially on-premises hardware. With only a single cloud provider, it is possible to achieve geographic replication and reasonable safeguards against hardware failure and network disruptions. StratusWorX makes it easy to guard against provider-level disruption, which many of our customers appreciate for their mission-critical services and data.

FIGURE 4: A MULTI-LAYERED APPROACH TO RESILIENCE AGAINST FAILURES.

To accomplish resilience in different forms, StratusWorX employs various layers of replication, both of user content and data, as well as their virtual machines. We offer at least three levels of redundant replication – (i) the Local Redundant Storage (LRS) where replication is limited to a single data center, (ii) Zone Redundant Storage (ZRS) where replication is limited to multiple data centers with placement within a single political administrative boundary but as widely spread out as possible, and (iii) Geographic Redundant Storage (GRS), where replication is worldwide to accomplish maximum resilience to failures.

These forms of replication allow for a user's workspace and content to be recovered even across catastrophic failures, such as a data center impacted by a natural disaster. The design choices of where and how much to replicate depend on two metrics. The first metric is the Recovery Time Objective (RTO) – the amount of time needed before a failed user workspace is restored, perhaps in a different location. The second metric is the Recover Point Objective (RPO) – the maximum time limit to the last consistent checkpointed state of the user workspace from the point of failure. The selection of the level of replication and the nature of replication depends on requirements of these two metrics that are carefully streamlined in the StratusWorX system.

F) Regulatory Compliance

Our customers operate in highly regulated fields such as finance and healthcare and thus have various regulatory requirements that extend to their cloud service provider.

Imagine a scenario where a multi-national banking company (MNBC) is not allowed to provide a certain service on the public cloud due to data-privacy laws of country A. This will force MNBC to host the service on its own premises in country A. Alternately, MNBC may choose to keep customer data on-premises for regulatory compliance with country A's laws but use the public cloud for hosting the applications that process (not store) the customer data in the public cloud for cost reasons. Now assume that the data-privacy laws of country B allow hosting of similar services in the public cloud, thus, allowing MNBC to offload hosting of the service in the public cloud. Given the reach and spread of modern-day enterprises, it is easy to imagine that the above requirements will become the norm (if not already so) for services.

Some present-day vendors, such as VMware, Amazon and Microsoft, offer hardware and software combinations that enterprises can buy and deploy in their on-premises data centers and couple them with public data centers for complementary deployment of IT workloads on a hybrid cloud. Additionally, some cloud providers offer packaged solutions such as Amazon Outpost and Azure Stack. However, none of these solutions provide true interoperability and seamless operation of workloads across different vendors. The StratusWorX Hybrid Cloud solution enables our customers to pick and choose the locations of their public and private cloud deployments to give complete control and seamless flexibility. This gives our customers complete control over the jurisdictions where data resides, making it easy for them to keep up with regulations while remaining agile in their technical solutions.

Conclusion

Our customers are always under pressure to do more with less by increasing efficiency through automation and reducing physical infrastructure costs and over-subscription of licensed software. With our Zero Touch, Zero Delay™ continuously secure Cloud Workspace solution, we help organizations achieve their goals without becoming lax on security. As detailed in this white paper, security is a primary design consideration in all StratusWorX technical solutions. Security mindfulness is also baked into our work culture, through organizational policies and training materials for new hires, and it is a core focus of our research teams.