StratusCore Inc. Customer Security

Version 2.22   February 2017

Table of Contents

Introduction

Enterprises in many sectors of the economy have been moving their computing to the public cloud for several years. Media and Entertainment (M&E) companies are similarly making the shift to cloud-based content creation, enticed by benefits ranging from reduced cost and complexity to easy definition and enforcement of software and storage standards. However, many M&E enterprises are embracing the cloud specifically for enhanced management and security of digital assets. StratusCore's suite of cloud-based content creation tools is bringing this dream to reality. **This paper, *Stratuscore Customer Security*, explores the security threats that Media and Entertainment companies face. It then weighs the various organizational obstacles to realizing cost-effective security. Ultimately, *management must elect to employ the security features* present in any security architecture to realize their benefits.** The paper includes a brief overview of the high-priority actions and habits that productions must adopt to enjoy the protections that cyber-smart and asset-wise M&E professionals must have. We conclude with an examination of the security strategy and mechanisms that protect users of StratusCore's suite.

StratusCore designed a strong multi-tier security model into its cloud-based content development suite from the ground up. StratusCore's Chief Architect, David D'Andrea, is a security scientist with decades of experience working on systems designed to satisfy the most rigorous federal and military IT requirements. Today Mr. D'Andrea also serves as a Hewlett-Packard Enterprise Company Master Technologist, specializing in federal and military high-security computing challenges.

The extensive end-user security features in StratusCore's *cloud-based content creation platform* are mirrored in StratusCore's *internal operations architecture and procedures*. Readers interested in the security designed into StratusCore's own IT systems are encouraged to consult ***StratusCore Internal Security,*** the companion to this white paper. StratusCore's IT approach offers a solid model that Media and Entertainment industry companies can adopt for their own in-house IT security.

The Security Challenges Facing the Media & Entertainment Industry

In the Media and Entertainment industry—like nearly every industry—organizations of every size face cyberthreats. The risks are most severe for large organizations: research shows they face more than two times the risk of security breaches than smaller companies. Bigger organizations generate, collect, and store a wealth of intellectual property and other high value information such as digital assets and sensitive personal information. This data makes them prime targets for both internal and external cybercriminals.

Remarkably (or, perhaps not surprisingly), Media and Entertainment companies seem to be targeted as much or more often than the norm. Attackers are drawn to the extreme value of their digital assets, to further political goals, to the high visibility of their products, and many other reasons. Two prominent recent attacks are Sony PlayStation Network (2011) and Sony Studios (2014). Those data breaches resulted in combined losses of $186 million. Beyond the financial impact, Sony also lost intellectual property, trade secrets, corporate email, and personal information. The culprits made these available to the public via the Internet. As with nearly all breaches, the brand damage, corporate embarrassment and erosion of customer trust was truly devastating. Recovery can add dramatically to the expense of attacks.

While Sony's misfortunes are legendary in the industry, the reality on the ground is getting worse. In an annual survey of media executives performed by Price Waterhouse, the fraction of M&E executives reporting employee theft of digital content prior to a major launch was up 18% over 2015. Vendor theft of content prior to a major launch window rose nearly as much. *Theft of critical media by external parties (e.g., hackers) prior to a key launch rose 55%, with nearly half of the 319 respondents to the Price Waterhouse survey referencing incidents.*[1] Although survey participants hailed from companies of all sizes, an astonishing sixty-one percent reported *more than* 10 security incidents in the prior year. In sum, while awareness is up (a good thing), attacks are up more.

These types of security breaches happen thousands of times a day. Malicious entities around the world, including companies and even nation states, are engaging hackers to help them conduct corporate espionage and other types of "intelligence gathering." Hacking is an industry. And as companies transition away from traditional infrastructure models, producers, artists, and content owners need protection that goes well beyond the firewall and antivirus software. Security is no longer only about safeguarding workstations; it's now also about protecting role-based users.

How in the World Did They Get in Here?

We Didn't Get Real About the Threat

The first explanation for successful attacks is basic: someone didn't take the threat seriously. Worrisome stories about hackers and internet-based attacks are like a drumbeat: new accounts of security debacles keep coming up. Yet most of us still assume that we're safe. Despite abundant evidence that the hackers are enjoying regular success, our natural inclination is to do nothing. *Why are we doing nothing?*

[1] Zumberge , Marianne,"**Cyber Attacks on the Rise in Media Biz Since Sony Hack: Survey (Exclusive)", Variety Magazine, 5 Nov. 2015. Web. 27 Jan. 2017.**

Ignorance of changes in the IT landscape is the principal reason. Many of us probably still conceive of “security” as a firewall and antivirus software. We imagine that if those are in place, we’ve beaten 95% of the threats—and all we must do personally is watch for sketchy emails. But a defense built solely on firewall and antivirus technology was inadequate in the era of workstations on an internet-connected LAN. Fast-forward to today: these two components, while still useful, are utterly insufficient on their own to assure a reasonable level of protection.

For example, growing use of social media by M&E industry freelancers creates one of the primary vectors by which threat groups gain access to content production systems. The traditional assumption that threats come only from outside the firewall is no longer valid. Advanced attacks access information from inside the network through infected guest, producers, artists, and content owner access.

Once an organization’s network is compromised, it can take weeks, months, or longer for a persistent threat to be detected in the network. Some threats are so sophisticated that they may sit doing nothing for weeks, like sleepers, before they get to work. Meanwhile, the targeted organization continues to create valuable data and the risk of significant operational damage escalates rapidly.

A second factor contributing to our willingness to ignore cyberattacks and cybertheft is money. IT defenses are costly—and productions run on a tight budget. It’s easy to forget the much larger cost of a successful intrusion. Result: security budgets are underfunded (or there is no such budget at all). This, in turn, leads to violations.

A third factor in our collective failure to address security is training. Even if technology necessary to assure security is present, productions often don’t have the time (the other critical budget) to devote to security education. Result: production assistants don’t get the IT instruction they need. When PAs aren’t properly resourced, what happens next is predictable: everything falls apart.

Case-in-Point #1: The Assistant Line Producer’s Mistake. *The new assistant hadn’t joined the production staff with intent to steal the trailers, or anything, for that matter. However, Ron, the assistant line producer managing him, seemed determined to make it effortless. Everyone working on the show had access to all the production files, regardless of roles. It didn’t matter if someone was working on digital costume art or coloration or rendering the lighting. Even the “kids” adding the credits had permissions to everything. What’s more, Ron had removed individual logon credentials from the wireless access point in the main production office. Instead, there was a single global password used by everyone. Ron apparently did this to appease the horde of freelancers who, like himself, who were all connecting their personal phones, iPads, and music players. Getting on the network with a hard-to-trace device, and downloading the trailers, was thus a snap. Basically, total anonymity, logs with nearly useless information—it’d be nearly impossible* *to identify him as the perp. His niece would be ecstatic to see clues to the next episodes before anyone else at school…*

In sum, our failure to take security seriously is perhaps the #1 contributor to digital catastrophe.

We Got Real About the Threat, But Real Security is Real Difficult

What about enterprises that do invest in security? Are they safe? Not always. **The second explanation for successful attacks is that protecting the network, data, and the workforce from cyberthreats has never been more difficult for organizations.** IT security teams face both a constantly evolving threat and steadily changing network landscape. These are the top reasons security is hard:

- Evolving threat: hackers are always exploring for new ways to “get in.” Hacking is highly lucrative. In contrast to perceptions, attackers are often highly disciplined organizations with groups of skilled specialists. They study and deploy a huge range of cyberthreats. Consequently, the hacker industry has innovated social engineering intrusions, physical/digital keystroke logging, email scams, and day-zero Trojans, malware, and ransomware, among other categories of attacks.

  These experts constantly explore for and develop new attack vectors. Thus, the attacks for which information technology teams must prepare are often unknown. Their task can be compared to searching through a haystack—for something they’ve never seen before.

- Shifting networks: Enterprise networks are increasingly fluid. This is especially true in digital content creation. Reflecting changes in organization structures, changes in projects and work groups, and shifting office layouts, network configurations are constantly in motion. Unfortunately, each time a change occurs in the work environment, and networks must adapt, the risk of an error that creates a vulnerability goes up sharply.

We Got Real About the Threat, and Even Invested in Real Technology…But Our Productions Never Got the Memo

The third major reason that cyber attackers succeed is that middle and lower-level managers—and end-users—don’t use available security technology.

You read that correctly: *a huge percentage of IT security debacles results from organizations simply not using what they have*. Groups opt out of cyber security for a variety of reasons. However, they typically boil down to just two:

- Senior management doesn’t take ownership for driving digital security through the entire organization
- Lower management intentionally punts to avoid logistical burdens

Often senior management will conscientiously study cyber threats, make careful decisions about risk management, and allocate substantial resources to acquiring suitable tools to control risk. Unfortunately, failure occurs when top management stops at that point and neglects to drive cultural change through all groups contributing to the production. Real security demands a security culture, a culture of respect and vigilance for the extraordinary enterprise value of most digital assets. Without it, the organization-wide adoption of secure processes and procedures never takes hold. IT security is uneven. Many holes exist in the protective mechanisms and practices that *together* (and only together) form the fabric required for real security.

Perhaps just as often, lower management decides independently to "run things their own way." Outcome: new or established IT procedures wind up ignored or discarded.

Case-in-Point #2: The Artist's Mistake. *Francesca assumed that the production had a firewall and strong anti-virus protections, so she clicked on the link in the email offering free trial versions of popular 3D creation software. As expected, the link led to a retail web site. However, web site took a long time to load and looked cheap, like the software reseller was rinky-dink. She didn't recognize the name of the vendor. So, Francesca closed the browser window and moved on with her work. Unfortunately, this artist's simple act of responding to an inviting email resulted in the theft of all the files in her entire pre-viz group. Malware at the web site installed a "Zero-Day" Trojan on Francesca's laptop. This new exploit, unknown to the software defenses on the network, entered her IT environment undetected. Because the Trojan code that was installed remained, lurking, on the network, much of the final production was also lost months later.*

The M&E sector is well represented in this group. For example, many content-creation production professionals develop their own unique methods for bringing projects to fruition on time and under budget. Often, they are rightfully proud of their trademark innovations and work styles, and adhere to them year after year. Unfortunately, this may leave the door to disaster wide open. For example, many Production Assistants may resist implementing modern IT security because it means having to train the digital artists on a production. *Over and over.* With the numbers of freelance digital artists working on each show steadily climbing, and the artists on a production constantly rotating as specialists come and go, the burden of training all those contributors has grown exponentially. Juggling all that training has become highly unappealing—or simply unmanageable with existing resources.

M&E organizations can also fail cybersecurity challenges when IT teams must develop more robust security policies within rigid business constraints. For example, an information technology department may be forced to use an existing IT architecture.

Another example: the department may have limited resources to scale network security to remote and branch studio offices, which typically have little or no IT support on site.

Absent a security culture, digital content creation (DCC) enterprises experience uncontrolled use of network and internet access by producers, artists, and content owners. This opens doors not only to cyberthreats but also to compliance and data security risk.

Case-in-Point #3: The Content Owner. *Raul had just seen the third edit of the night scenes at the screening room. Central to the plot, they were good but not quite on…. Ah ha! It suddenly hit him: he would ship the 90 seconds or so of night images to a friend from film school days who was a genius with after-dark CG lighting effects. Within a few hours, Raul had a bag of terabyte drives headed for L.A. Unfortunately, data is most at risk when it is in motion. Although he didn't know it, moving the discs was going to cost his company dearly. The data arrived 10 hours late "due to LA traffic." In that time, the data was copied. Raul took the time to use encryption, so the thieves who saw the shipment couldn't access the content. However, Raul made the mistake of using symmetric encryption (both the sender and the receiver use the same keys). This didn't matter at first. But the thieves who handled the delivery obtained Raul's name, and his friend's name and email address. The rest was soon history. The baddies developed targeted "spear-phishing" threats that soon accessed his friend's studio, and then his own studio. Equipped with the key, criminals were instantly able to crack encrypted files of the near-final film stored on the network at Raul's production company. Copies were available on the streets of Shanghai two weeks before the general cinema release date in the U.S.*

Common Threat Vectors and Protection Strategies

Let's explore some of the vulnerabilities most commonly used by attackers. Table 1 names some common threat vectors, i.e. pathways that attackers can use successfully to gain access. These are shown in the first column. The second column describes vulnerabilities that can be exploited when the threat vectors exist.

The third column of Table 1 describes the benefits of common security technologies and how they block the threat vectors.

Table 1
Critical Threat Vectors and Avoidance Strategies

Threat Vector	Vulnerabilities If Ignored	Security Technology
Absent or incomplete role-based assignment of access permissions and authorities	Assigning *identical rights and permissions* to all users is a mistake: access to resources is thus shared to many people unnecessarily–needlessly increasing security risks. Lack of role-based access also increases the difficulty of identifying culprits.	*Role-based assignment of access rights and permissions* allows production managers to match user access to file directories, storage, and network services to each user's authority level, job requirements, etc.
Lack of Single Sign-On (SSO) Security (i.e., all users have same sign-on credentials)	If all users have identical sign-on credentials, there is no opportunity to detect the identity of culprits if an attack is detected. Also, network managers are challenged when a user departs (or is let go): there is no way to de-authorize a user without changing everyone's credentials.	Single Sign-On (SSO) security assigns each user unique sign-on credentials. One of the main benefits using SSO is one set of credentials can be used with multiple applications. If the user is terminated (or simply finishes her work on the project), only one account needs to be disabled, not multiple. In addition, the network can uniquely log his/her activities. Works best with multi-factor authentication supporting non-repudiation.
Extended logon sessions (no session timeouts)	User sessions that continue for hours, even during periods of inactivity, leave the production vulnerable to easy theft. Equally challenging: any theft may be blamed on a user who in many cases is not the culprit. Result: loss of Intellectual Property plus false suspicions and distrust.	Automatic session time-outs, after a period of inactivity, protect against "drive-by" theft of digital assets, say, by short-term contractors who are quick with a USB drive. A particularly cost-effective security feature, session time-outs can seem burdensome. However, if paired with VLAN technology enabling users to access all *appropriate* work resources with one sign-on, the hassle can be minimized.
Unsecure and unauthorized public Wi-Fi	Managers of production offices and sound stages may be tempted to remove Wi-Fi access controls, especially when working with a fluid work force. This immediately opens the network to intrusions by anyone using any device.	Strong security for wireless access points (including unique logon credentials for each user and multi-factor authentication) dramatically reduces opportunities for theft
Unregulated satellite studio offices	At smaller post-production offices lacking informal IT staff and regulations, physical security of IT assets may be easily circumvented, resulting in	A well-regulated confederation of post-production vendors will maintain tight, consistent physical control of information systems (ranging from media drives to servers); and tight

	intrusions. Weak network security can also lead to malware attacks. As media files are transferred back and forth, viruses and Trojans may move throughout a production's entire vendor community, from contributing VFX houses and RMSPs to distribution facilities.	access control to networks and resources. Such standards are difficult to create, and enforce, but the benefit is strong security.
Single-factor authentication	In a single-factor authentication system, loss of logon credentials can go unnoticed (or be denied), opening the door to intrusions. These may recur many times before detection, magnifying damage	Multi-factor authentication typically requires users to both know information (e.g., a password) and have physical possession of a device (e.g., a digital key generator). Prevents unauthorized access if one set of credentials is lost or stolen.
Lack of non-repudiation of each users' unique identity	Without non-repudiation, an attacker with a stolen password can both gain access and elude detection. Similarly, a malicious user can deny making attacks by claiming that someone stole her/his password.	A system with non-repudiation knows with conviction that a user's identity has been accurately represented. At minimum, requires that users present two types of credentials (dual-factor authentication).

The M&E sector is particularly prone to many of the threat vectors in Table 1. For example, many productions have work forces that are highly mobile: staffers are freelancers, their identities change nearly constantly, and they are often always in motion (shifting from one location to another on the production). Result: the temptation to deactivate or defeat almost every one of the technologies capable of blocking key threat vectors is very high. (The overhead of training every contractor in your security systems can *seem* excessive.) Another example: the wide swings in the human resources and equipment demanded by a production over its development cycle mean that the network and authorized personnel both change constantly. Result: in a conventional network environment, maintaining IT security requires intensive attention to detail.

How to Optimize Your Organization's Security-Productivity-Cost Triad

Now consider your own production enterprise. You might be a major studio, a full-line rich media service provider, a visual effects (VFX) house, or any of several other essential contributors on the sound-stage-to-post-production-to-distribution continuum. Regardless of your size and role, today's organization needs to harness the power of both local and cloud-based services and solutions without undermining agility or security. That's a given. But as any enterprise expands its use of the Internet and network access, it increases its exposure to risks. These tangible threats can affect brand, operations, data, and more.

So how can you provide your staff with easy access to tools, files, and internet resources in a flexible, *secure* architecture that doesn't break the bank—or the spirit of your people as they focus on their creative process?

StratusCore's Comprehensive Approach

To address security challenges faced by M&E executives and managers effectively, StratusCore provides a potent, pervasive solution that can:

- Address current security demands. The StratusCore environment delivers strong protection against today's threats. Critically, it addresses how modern users access information.
- Adapt to meet the changing threat landscape. StratusCore's architecture protects against new forms of threats. It addresses anything that bypasses edge network defenses.
- Meets the constraints and needs of producers, artists, and content owners. The logical and physical design of StratusCore's environment, including its security features, fits within any production's current infrastructure. It scales gracefully as the production grows.

Securing every device, every user, and every bit of data that crosses the organization network requires an adaptive, cloud-aware architectural approach. StratusCore's network-based security architecture is that approach. *StratusCore's security philosophy is based on the Company's own infrastructure and operations platform.* (Readers with an interest in learning more about StratusCore's own platform are encouraged to study ***StratusCore Internal Security.*** This white paper is available from the company through your account manager or by emailing info@stratuscore.com.)

StratusCore's solution combines public-cloud-based elements with StratusCore's own private cloud. This "hybrid cloud" approach delivers the best attributes of both the public cloud and private data centers managed for high security. These benefits include:

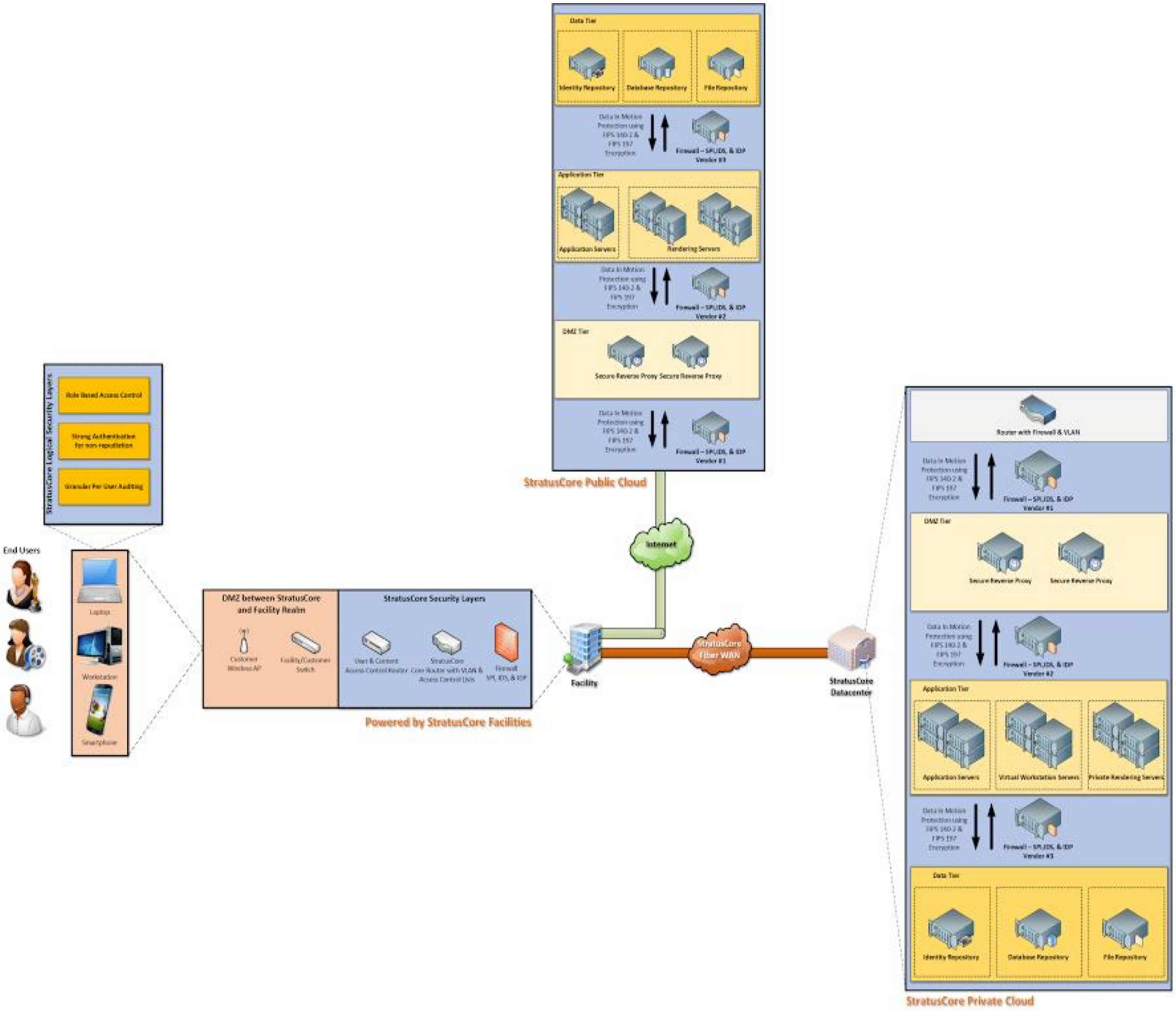
- The cloud enables easy sharing across the multiplicity of companies involved in any production.
- Cloud-based development of content dramatically improves collaboration between contractors, and speeds workflows.
- Use of a common tool set (i.e., a standard set of DCC software applications) reduces or eliminates software conflicts and version-control challenges. Selecting software from StratusCore's cloud-based app store also eliminates use of improperly licensed content creation software.
- With virtually unlimited storage and compute resources, cloud-based content creation makes it easy to add to private data center capacity during peak loads.

- Access to render and virtual workstation services hosted in StratusCore's private datacenters provides additional assurance of security. This benefit is particularly appealing for late-stage post work.

Figure 1 offers a diagram of StratusCore's hybrid cloud architecture. Several important elements merit mention:

- On the right, the diagram shows the logical and physical elements of StratusCore's private datacenters. These facilities employ a tiered security model.
    - The datacenter is protected by a firewall and VLAN. (These are visible in the top of the block depicting the datacenter.) Right below in the diagram, a second firewall provides further protection. Threats attempting to reach the first tier must overcome these defenses. Tier One comprises reverse proxy servers. These hide the identity of the servers inside Tier Two (the application layer) from would-be attackers. In the application layer, Workstation and Rendering servers (and other applications) process customer content. The content itself is stored in the third, and most-protected tier of the datacenter, behind an additional firewall.
- StratusCore's private datacenters are connected by StratusCore's WAN to *Powered by StratusCore Facilities* ™, also known as **PBSFs**. These are sites serviced by StratusCore's secure 10Gb fiber backbone. Artists and production professionals working at PBSFs, whether sound stages, co-work facilities, or production offices, can move content quickly and securely. Contributors can collaborate using StratusCore's workflow application or workflow solutions offered by StratusCore's software partners. StratusCore's private, self-contained "in-mail" ensures project communications can occur without exposing system infrastructure to the public internet.
- Above the *Powered by StratusCore Facilities*, the top-middle of the diagram shows a StratusCore datacenter hosted in the public cloud. StratusCore's architecture is cloud-agnostic. It can be deployed on demand on any of several public-cloud vendors StratusCore supports today.
- The far left of Figure 1 shows both StratusCore's edge network elements and end-user systems. Within each PBSF, StratusCore's network terminates with a firewall; and a router enabling VLANs and precise access controls. These features allow productions to control user access to network features with high precision.

Figure 1
StratusCore's Hybrid Cloud Architecture – Security Features


StratusCore Logical Security Layers
Role Based Access Control
Strong Authentication for non-repudiation
Granular Per User Auditing
End Users
Laptop
Workstation
Smartphone
DMZ between StratusCore and Facility Realm
Customer Wireless AP
Facility/Customer Switch
StratusCore Security Layers
User & Content Access Control Router
StratusCore Core Router with VLAN & Access Control Lists
Firewall SPI, IDS, & IDP
Powered by StratusCore Facilities
Facility
Internet
StratusCore Fiber WAN
StratusCore Datacenter
Data Tier
Identity Repository
Database Repository
File Repository
Data In Motion Protection using FIPS 140-2 & FIPS 197 Encryption
Firewall – SPI, IDS, & IDP Vendor #3
Application Tier
Application Servers
Rendering Servers
Firewall – SPI, IDS, & IDP Vendor #2
DMZ Tier
Secure Reverse Proxy
Secure Reverse Proxy
Firewall – SPI, IDS, & IDP Vendor #1
StratusCore Public Cloud
Router with Firewall & VLAN
Virtual Workstation Servers
Private Rendering Servers
StratusCore Private Cloud

Tier Security Controls

- VLANS
- Separated server containers
- Access Control Lists
- Strong Authentication using FIPS 201 (Smart cards)
- Role Based Access Control
- Data At Rest Encryption using FIPS 140-2 & 197
- Data In Motion Encryption – Intra-application communication using FIPS 140-2 & 197
- Secure data destruction using DoD 5520.22-m
- OS, Data, and Application logging/auditing

Applicable Regulations

StratusCore aligns to the following regulations:

- Computer Fraud and Abuse Act [PL 99-474, 18 USC 1030]
- E-Authentication Guidance for Federal Agencies [OMB M-04-04]
- Federal Information Security Management Act (FISMA) of 2002 [Title III, PL 107-347]
- Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy [OMB M-01-05]
- Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection [HSPD-7]
- Internal Control Systems [OMB Circular A-123]
- Management of Federal Information Resources [OMB Circular A-130]
- Management's Responsibility for Internal Control [OMB Circular A-123, Revised 12/21/2004]
- Protection of Sensitive Agency Information [OMB M-06-16]
- Security of Federal Automated Information Systems [OMB Circular A-130, Appendix III]

Applicable Standards and Guidance

StratusCore aligns to the following standards and guidance as prescribed by FedRAMP:

- A NIST Definition of Cloud Computing [NIST SP 800-145]
- Computer Security Incident Handling Guide [NIST SP 800—61, Revision 1]
- Contingency Planning Guide for Federal Information Systems [NIST SP 800-34, Revision 1]
- Engineering Principles for Information Technology Security (A Baseline for Achieving Security) [NIST SP 800-27, Revision A]
- Guide for Assessing the Security Controls in Federal Information Systems [NIST SP 800-53A]
- Guide for Developing Security Plans for Federal Information Systems [NIST SP 800-18, Revision 1]
- Guide for Developing the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach [NIST SP 800-37, Revision 1]
- Guide for Mapping Types of Information and Information Systems to Security Categories [NISP SP 800-60, Revision 1]
- Guide for Security Focused Configuration Management of Information Systems [NIST SP 800-128]
- Information Security Continuous Monitoring for Federal Information Systems and Organizations [NIST SP 800-137]
- Managing Information Security Risk [NIST SP 800-39]
- Minimum Security Requirements for Federal Information and Information Systems [FIPS Publication 200]
- Personal Identity Verification (PIV) of Federal Employees and Contractors [FIPS Publication 201-1]
- Recommended Security Controls for Federal Information Systems [NIST SP 800-53, Revision 4]
- Risk Management Guide for Information Technology Systems [NIST SP 800-30, Revision 1]
- Security Considerations in the System Development Life Cycle [NIST SP 800-64, Revision 2]
- Security Requirements for Cryptographic Modules [FIPS Publication 140-2]
- Advanced Encryption Standard[FIPS Publication 197]
- Standards for Security Categorization of Federal Information and Information Systems [FIPS Publication 199]
- Technical Guide to Information Security Testing and Assessment [NIST SP 800-115]

StratusCore Logical and Physical Security Model

The components of StratusCore's hybrid-cloud delivery platform and customer-premises networks fit together in a comprehensive solution that help defend against, discover, and remediate threats originating from the Internet. This architecture also helps organizations better manage the security risks of borderless networks, so employees and contractors can globally access the network with their device of choice and use the applications and information they need to do their jobs.

Figure 2
StratusCore Security Foundations

	Security Model			
Goals	**Encryption**	**Content**	**Network**	**Access**
Protection	Provide transparent encryption of user's data	Protect users everywhere, all the time	Security policies, procedures, and implementation protect data content	Deliver access protection and identity-based non-repudiation
Control	Provide uniform protection of content	Support control of all web, private mail, storage, and virtual workstation traffic for all users	Offer exceptional visibility and control of the network and service access	Simplify complex identity & access controls entitlements assignments
Flexibility	Require no additional user training or action	Integrate transparently with existing security and network infrastructure	Provide agile, open, and scalable services	Secure access to sensitive content
	Security Features			
Support for Industry Standards, Best Practices	**Symmetric and asymmetric encryption**	**Network & Web Security** **Private Mail Security**	**Firewall** **Intrusion Detection System** **Intrusion Prevention System**	**Identity and Access Management** **Malware protection**

Figure 2 offers insights into StratusCore's customer security investment. Our security model is defined and constantly reevaluated with four goals in mind: protection; control; flexibility; and support for industry standards and best practices. We apply these goals to the four foundational elements of StratusCore's security model: encryption, content, access, and network design.

- **Content Encryption**: Data in motion and rest are symmetrically and asymmetrically encrypted using Federal standards (FIPS 197 & 140-2). After customer use of storage facilities (public or private) is complete, all customer data is rendered unrecoverable, even with forensics. StratusCore securely deletes files using Department of Defense's 5520.22-m wipe standard.

- **Content Security**: Strong authentication, authorization and auditing protect StratusCore's transport, web-based render services, storage, and virtual workstation service. StratusCore's built-in private email service, with multiple security features, further protects producers, artists, and content owners.

- **Network Security**: StratusCore's platform includes firewalls, direct-fiber, intrusion & detection prevention systems, standard Federal security policies, and regulated network access control.

- **Secure Access:** Identity and access management is universal. Access is safeguarded through role-based entitlements.

The Result: StratusCore's Customer Security Implementation

Our security provides complete control over how producers, artists, and content producers access StratusCore resources, including SaaS applications and services.

Network security: StratusCore's cloud security *keeps threats off the StratusCore network*. It helps customers of all sizes more effectively control and secure usage of the system by both contractors and employees. Our cloud security provides both inbound and outbound protection and extends security to all roaming users with an authorized StratusID account.

StratusCore's *cloud security is reinforced by behavior-based analysis* to provide exceptional threat defense from zero-day-based malware, ransomware, and Trojans. All inbound and outbound traffic is scanned in real time for both new and previously identified threats. Every piece of HTTP and HTTPS web content accessed is analyzed by security and context-aware scanning engines.

Application and asset security: StratusCore's access security also *provides increased control of assets* for productions employing our software as a service (SaaS) applications. Role-based access control limits the growth of risks created by the proliferation of applications. Precise control can be applied at a granular security level to any service. Welcome by-products of tight security include insights into resource use and increased protection from cloud data loss.

Conclusion

StratusCore understands how to secure services, whether on our fiber network, in the cloud, or running over the open Internet. We also understand and deliver on the security requirements of Media and Entertainment professionals who are trying to complete content creation projects on a tight budget, under difficult time constraints, with the help of a handful or a battery of contributors. By leveraging a multitier combination of products, technologies, services, and design expertise, StratusCore enables the most efficient, scalable, cost-effective, and secure networking and computing environment in the industry.