smartsheet

A Smartsheet Report:

4 Critical Principles of Enterprise

By Peter Oehlert
Senior Director of Information Security, Smartsheet

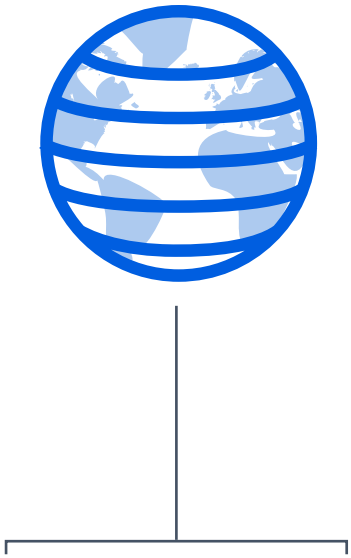
The threat landscape faced by the enterprise is rapidly changing. At a time when bad actors are becoming increasingly creative, persistent, and patient, businesses are facing the imperative to evolve in new ways that expose them to new or different kinds of risk. Organizations must move more quickly if they want to remain competitive. To succeed, they must also be more connected to external stakeholders — vendors, customers, partners, and an increasingly dispersed workforce — often via the cloud. More business is conducted outside the walls of the enterprise, with connections back into business-critical systems.

For enterprise security professionals, the universe of worry is expanding. Besides defending against increasingly sophisticated external attacks, we also need to know who our users are, and tightly control what they do and don't have access to. We need to secure the transfer of information between users and systems. When data is spread across more locations, in the cloud and on-premise, it exponentially increases the scope of what must be protected across our systems, as well as those of our vendors and partners, and even down to the personal devices of our employees.

Effective enterprise security isn't easy, but it's never been more crucial. According to Verizon's 2019 Data Breach Investigations Report, in 2018, there were 53,308 security incidents resulting in 2,216 data breaches in 65 countries. Almost three-quarters (73%) of cyberattacks were perpetrated by outsiders; over a quarter (28%) involved insiders. Monitoring and detection is critical; according to the report, 68% of breaches took months or longer to discover.

Most enterprises are taking this challenge seriously: According to ISACA's 2018 State of Cybersecurity research, 64% of enterprises were expected to increase their cybersecurity budget in 2018 — up from 50% in 2017.

I've spent almost two decades helping some of the largest technology and financial service companies in the world — including Microsoft, Google, Facebook, and Smartsheet — to engineer systems and develop processes to keep their data and their customers' data safe from harm in an increasingly complex threat environment. From working as an engineer on cutting-edge security technology and analysis, to leading large security teams dedicated to managing risk, I've considered threats to enterprises from many perspectives. Based on my experience, here are four critical principles of enterprise security.



When data is spread across more locations, in the cloud and on-premise, it exponentially increases the scope of what must be protected across our systems, as well as those of our vendors and partners, and even down to the personal devices of our employees.

Principle #1: Least Privilege

A fundamental principle that underpins much of enterprise security across all kinds of different dimensions, least privilege is the practice of giving every user exactly as much access as they need and no more. And while most organizations recognize least privilege as critical — and have well-documented policies and procedures — they're often imperfectly enforced because of the complexity that arises from precise access control. In all kinds of enterprises, users of all kinds — both internal and external — have significantly more access than they should.

A problem for years, least privilege has been getting more complex with the pervasiveness of "bring your own device" (BYOD). Employees now have access to critical data on their personal devices. How do you safeguard against others who have or can gain access to those personal devices?

Enterprises must harden their approach to least privilege. Though managing access on an individual basis isn't scalable for organizations, doing so is critical to minimize threats and contain breaches. Whether it's a rogue insider or external bad actor, and whether an incident is pertaining to a single compromised device or large data source, providing actual least privilege significantly limits an enterprise's exposure. A new approach is needed, because central IT-managed permissions aren't scalable. In the absence of stringent least privilege, a company's security can be compromised after a bad actor identifies the first weak point in the system. The preferred security approach, least privilege, makes attackers do as much work as possible, with each compromise providing as little as possible return, requiring them to compromise the next step and the next after that.

Applications increasingly offer granular administrative controls to help enterprises prioritize least privilege, but even that can be too complex to manage. Often software, such as Microsoft Windows, comes with default permissions which are rarely, if ever, updated because it is too difficult. Keeping access current across a growing, fast-moving enterprise is a daunting challenge.

Enterprises must harden their approach to least privilege ... Whether it's a rogue insider or external bad actor, and whether an incident is pertaining to a single compromised device or large data source, providing actual least privilege significantly limits an enterprise's exposure.

User Accountability

At Smartsheet, we've added a layer of accountability at the user level that helps our users. Our application gives enterprises transparency into and control over who is accessing data, so that every participant in the enterprise manages least privilege — without help from IT to configure and manage it. The granularity of our user-friendly share controls adds a layer of protection to the system, and gives control to those who are best suited to determine who really needs access.

This granularity is available to Smartsheet users at the sheet level, where individual projects are often managed, and at the workspace level, often involving groups or divisions. Members of a team can share access to a body of work, but an external vendor can see only one sheet — or even only one row. We've taken that a step further with our premium add-on capability, Dynamic View, which allows users to share only

certain subsets of rows or columns of a sheet. Despite providing several layers of granular user access control, we adhere to our philosophy of simplicity: In our application, users have access to powerful controls, which are simple to understand and to use to control access.

And removing access is just as important, which is why Smartsheet controls make it just as simple to revoke access.

To help enterprises monitor least-privilege policies at scale, Smartsheet recently released APIs for event reporting. This new functionality enables a global view of how permissions are assigned across an organization and how data is being used inside Smartsheet.

Machine-level Privilege

At Smartsheet, least privilege extends well beyond our app; it's a fundamental precept of our infrastructure. Unlike many SaaS (software as a service) companies, we apply least privilege down to our individual machines and services. Our network is highly segmented in our production environment; our machines don't have access to talk to other machines unless strictly necessary. Though complex, we apply least privilege in multiple layers.

It's critical for enterprises who want to walk the line between rapid growth, agility, and scaling for secure admin control to choose technology partners that do not compromise on least privilege. Insist on granular control at every level, and on technology that empowers individual users to understand and participate in least privilege.

It's critical for enterprises who want to walk the line between rapid growth, agility, and scaling for secure admin control to choose technology partners that do not compromise on least privilege. Insist on granular control at every level.

Principle #2: Manage Security at Scale

Keeping up with the pace of scale at today's enterprises can be incredibly challenging for security teams, because greater scale means more employee arrivals and departures, more sharing of data across and outside of the enterprise, and increased aggregated risk. Managing this risk involves managing a rising tide of both data security and employee access. Enterprise security leaders increasingly need tools to help them do both.

In a rapidly growing enterprise, securely provisioning and de-provisioning employees becomes a major challenge. Companies that have tens or even hundreds of different systems and applications need a way to enable provisioning of access to multiple new employees — and rescind access from employees changing roles or departing — in an efficient, scalable way. The time is long past when enterprise IT could manage these processes manually.

Rapidly scaling organizations should consider cloud technologies that enable automated provisioning and error-free sharing. Additionally, these technologies should give enterprises a breadth view of every action taken by users.

Automated Provisioning

A SCIM, or System for Cross-domain Identity Management, is an open standard that was created to allow for automated user provisioning. It communicates user identity data between identity providers (such as companies with multiple individual users) and service providers requiring user identity information (such as enterprise SaaS apps). Cloud-based applications that provide a SCIM integration enable enterprises to take advantage of this automation, streamlining their provisioning process. In summer 2019, Smartsheet will release a SCIM integration, enabling enterprises to add or remove employees using Azure Active Directory and automatically provision or de-provision Smartsheet at the same time. Using features within automated provisioning, administrators have better control over how users are granted or denied access to information within their instance of Smartsheet.

We're also focused on helping organizations harden the security around collaborating, so we've created new functionality called Smartsheet Directory Service, to be released later in 2019. The Directory Service integrates with enterprises' internal directories, enabling users to more securely share data by reducing error-prone manual email entry. This lets Smartsheet and your directory do all the hard work. When employees join, they are enabled in Smartsheet. When they move around the organization, their access to data in Smartsheet is automatically updated based on group membership changes in the enterprise directory, and when they depart, they are automatically deprovisioned.

Rapidly scaling organizations should consider cloud technologies that enable automated provisioning and error-free sharing. Additionally, these technologies should give enterprises a breadth view of every action taken by users. With Smartsheet event reporting, organizations can essentially view a stream of all Smartsheet-related events across the business, from the creation of new sheets, reports, and dashboards, to sharing and even viewing of information. Smartsheet makes this data available to security and IT teams, giving them the power to monitor actions and assess risk according to their security requirements.

At Smartsheet, data uploaded or submitted to our app belongs to our customers, and is treated as such, period.

Principle #3: Data Protection

It's critical that IT and business leaders seek out technology partners that build for both foundational security and robust data access controls within the platform. This means looking for a fully encrypted and secure app with necessary product capabilities to give an organization the controls needed to keep data secure. It also means considering how data can or will be used by companies that offer services.

Make sure partner providers work with top-tier hosting or cloud partners to ensure that data is safe at rest. Look for multi-site data redundancy at facilities that are AICPA SOC 1 examined. And check for data monitoring that includes the strongest authentication protocols and continuous surveillance, including 24 x 7 production environment management.

Encryption serves as the strongest line of defense in a multilayered data security strategy. Smartsheet uses NIST approved encryption to protect data in transit and at rest in our data centers. This means that data that is sent to our application is protected as it travels over the internet and stored securely with our hosting and cloud partners.

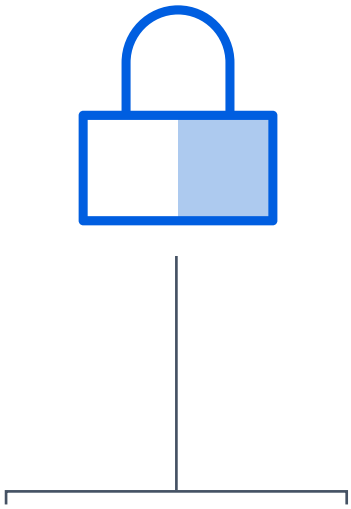
At Smartsheet, data uploaded or submitted to our app belongs to our customers, and is treated as such, period. We don't touch it, except as required by applicable law; as requested by customers in writing; as allowed by a customer via the service's access controls; and as necessary to provide services and prevent or address technical problems with services, or violations of our user agreement. The way we've built our application and our architecture reflect this philosophy.

Principle #4: Audit and Monitor for Security

In 2012, Robert S. Mueller, then director of the FBI, said, "I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again." Effective enterprise security should be based on the assumption that every business is going to be attacked at some point.

Effective enterprise security requires a holistic approach: continually auditing to make sure security systems and processes are functioning the way they should be, while also monitoring internal activities and external threats. At Smartsheet, we go beyond that to consider everything from who our employees are to every step of our software supply chain, from the creation of our application to its eventual deployment on our customers' desktops and mobile devices.

It's not enough to build a firewall; security leaders must constantly monitor, keeping an eye out for new threats, and be prepared to deal with adversaries as they emerge. Not all external threats will be known; detecting unknown threats requires behavior and anomaly detection — figuring out what good traffic looks like so that the system can flag bad traffic. Effective auditing should also include penetration testing, using both internal teams and external providers to mimic attacks, and try to penetrate networks and applications.



Effective enterprise security should be based on the assumption that every business is going to be attacked at some point.

Securing the Enterprise for the Road Ahead

Keeping up with the pace and velocity of security threats to the enterprise is an exercise in constant vigilance. Having policies in place that effectively address each of these four key principles is critical for any enterprise — and also for the vendors and technology partners with which they do business. At Smartsheet, we dedicate significant resources to assessing and responding to this rapidly changing threat landscape, with capabilities and controls that empower our customers to transform the way they work within an end-to-end secure environment.

At Smartsheet, we build for security through and through.
Learn more at smartsheet.com/trust.

About the Author

Peter Oehlert is senior director of information security at Smartsheet, where he leads the overall security teams and security engineering team to protect Smartsheet customer data and the application. He has more than 25 years in technology working as a developer, security engineer, and leader. Prior to Smartsheet, Peter lead the Product Security team at Facebook and ran iSEC Partner's office in New York, where he assisted the largest technology and financial service companies in the world in improving their security posture.

As part of Microsoft's core security team during the time of the Trustworthy Computing memo, Peter was a member of a small team responsible for changing the entire company's outlook on and awareness of security. He helped draft parts of Microsoft's SDL and produced some of the earliest recognized work — and holds a patent — in the nascent area of identifying security vulnerabilities through fuzzing. He has written a variety of static and dynamic analysis tools to improve security analysis and often speaks on the topic of security and security leadership at enterprises, industry gatherings, and conferences.

About Smartsheet

Smartsheet (NYSE:SMAR) is a leading cloud-based platform for work execution, enabling teams and organizations to plan, capture, manage, automate, and report on work at scale, resulting in more efficient processes and better business outcomes. Smartsheet is committed to continuously delivering a secure and extensible platform that meets the complex needs of today's largest enterprises. More than 75% of the companies in the Fortune 500 rely on Smartsheet to implement, manage, and automate processes across a broad array of departments and use cases. To learn more about Smartsheet, visit http://www.smartsheet.com.