Building a secure communication and collaboration strategy with Microsoft Teams

The role of security in furthering achieving businesses objectives

In the past, cybersecurity and privacy were often low on the list of priorities for many organizations. However, as cyberthreats have increased, so have the risks of ignoring those threats. Breaches, compromised data, and cyberattacks can put vulnerable beneficiaries at risk, disrupt nonprofit operations and services, expose you to liability, and tarnish the reputation you have so painstakingly built.

Risk for Small and Large Organizations

Determining the best approach to security becomes more difficult as attacks grow more sophisticated, employees use a wider array of devices and applications, and data flows into and out of your organization through more channels. And don't think small organizations are smaller targets for data breaches: the risk is often higher for small organizations because they have fewer safeguards in place.

Assume Breach

Business leaders must balance these challenges with the need to collaborate, innovate, and further your mission in the most cost-effective way possible. You need a multifaceted security approach that constantly protects all endpoints, detects early signs of a breach, and responds before damage occurs. No matter how strong your defenses are, "preventive measures" are no longer enough. These days, you need to adopt an "assume breach" posture that includes detection and response measures.

Factoring Risk

Risk management is now a requirement for businesses of all sizes. The goal is to minimize the potential impact of increasingly sophisticated attacks by more effectively protecting a growing group of users, devices, applications, data, and infrastructure–with fewer resources.

Today's businesses require agile security frameworks built on holistic strategies embedded into technologies, processes, and training programs. This eBook highlights some of the strategies and best practices that businesses can use to successfully integrate security into the fabric of their operation.

> 'Every hour of the day you need to be prepared, which means you have to **exercise this operational security posture on a continuous basis.'**
>
> *- Satya Nadella, CEO, Microsoft*

Businesses must enable collaboration with integrated security

Cyber Criminals are Agile and Evolving

Cyberthreats have evolved from “smash and grab” attacks that compromise systems with a persistent, long term presence to a much broader range of vulnerability. Attackers now use a variety of vectors and an increasingly advanced array of tools and techniques. These include:

- Stealing credentials
- Installing malware that erases itself to avoid detection
- Modifying internal processes and rerouting network data
- Social engineering scams
- Targeting staff mobile phones and home devices

Organizations are Reacting rather than Planning

To respond to this rapidly evolving threat landscape, organizations are deploying more and more security tools. The challenge is that each of these tools addresses specific issues, but they rarely work together. Many use proprietary dashboards, consoles, and logs that are difficult to integrate, making it nearly impossible to have a comprehensive security view and prioritize threats quickly. This is even more challenging when dealing with both cloud and on-premises resources. As a result, attacks can sometimes go undetected for up to 140 days.[1]

- New modes of work and collaboration and the devices they require elevate an organization’s risk of security breach
- The lack of integration between security products makes it hard for security teams to quickly see and combat threats holistically
- Seek out security products designed to integrate with others

‘The average large organization uses **75 distinct security products.’**[1]

1. Balaji Yelamanchili, Executive Cice President and General Manager of Enterprise Security Business, Symantec, in "Symantec Introduces New Era of Advanced Threat Protection," Press Release, October 27, 2015. < https://www.symantec.com/en/in/about/newsroom/press-releases/2015/symantec_1027_01>

Be secure and confident with Microsoft Teams

As part of Microsoft 365, Microsoft Teams provides organizations with advanced security. It is a complete, intelligent solution that empowers staff and volunteers to be creative and work together, securely from anywhere on their preferred device.

Microsoft Teams delivered on Microsoft 365 includes built-in holistic, identity-driven protection for users, devices, apps, and data. It provides sophisticated machine-learning models to reveal suspicious behavior in on-premises systems or in the cloud. And it applies advanced analytics to deliver richer insights that can help you detect and respond to attacks quickly. This level of security is woven into all layers of Microsoft 365. Here are four ways you can use Microsoft 365 tools to help protect your people, data, and devices while maintaining a high level of productivity.

Microsoft security management solutions

To gain more visibility and control, Microsoft Teams built on Microsoft 365 provides a holistic approach to security where protection starts at the front door of your system and continues to protect your data anywhere while detecting and remediating attacks. This helps you consolidate tools while ensuring that your security specialist teams have the flexibility and freedom to address their specific workloads.you can use Microsoft 365 tools to help protect your people, data, and devices while maintaining a high level of productivity.

> ‘Microsoft Teams delivered on Microsoft 365 includes **built-in holistic, identity-driven protection for users, devices, apps, and data.’**

How Microsoft defends its platform: The Cyber Defense Operations Center

In 2015, Microsoft opened the Cyber Defense Operations Center to bring together their cybersecurity specialists and data scientists in one facility to help protect, detect, and respond to security threats against Microsoft infrastructure and services in real time. Since that time, Microsoft has advanced policies and practices that accelerate the detection, identification and resolution of cybersecurity threats, and have shared key learnings with customers.

Simplified and intelligent security management provides more visibility and control

The key to any organization’s security is not having a single console for everything, but integration where it makes the most sense. Businesses don’t need all the point solutions to manage data points to help secure end-user devices and expanding networks required for better teamwork and collaboration. Microsoft Teams delivered by Microsoft 365 provides intelligent security management with specialized controls based on an organization’s needs, visibility where needed, and guidance on how to harden security posture based on unmatched intelligence.

Increasing security through identity and access controls

Microsoft Teams leverages Microsoft identity and access management solutions help protect user identities and control access to valuable resources based on user risk level. Microsoft 365 Enterprise offers protection across identity (Windows Hello, Touch ID, Credential Guard, Conditional Access, Azure Active Directory), apps and data (Office DLP, Azure Information Protection, Cloud App Security), and devices (Device Guard, Intune).

About Microsoft Teams

Microsoft Teams is the fastest growing business app in company history:

- **500,000+ Organizations**
- **91 Fortune 100 companies use Teams**
- **44 languages are supported in Teams**
- **150 customers have 10,000 or more active users**

Video Calling

Email is great for communicating information about projects that your group will need to reference later--sending a quick note about an upcoming meeting or PTO, for example--but for customer requirements sessions, challenging customer service conversations, or any time you wish to be a bit more persuasive; nothing beats a face-to-face meeting, which is where video calling comes in. After all, video calling makes it possible for people to see each other, get a feel for personality and mood, and pick up on nuances and intonations, which makes it easier to share ideas, have tough conversations, and make your case.

Chat/Instant Message

When you're leading virtual field service teams, it's impossible to experience the same level of spontaneity that you would in a traditional work setting. However, with a chat client you can still have those quick conversations. Best of all, if you want to run an idea by more than one person at a time, most chat clients give you that option – making it easier to work through ideas and issues on the fly.

Shared Workspaces

Whether you're managing global field service teams or working with a smaller group, odds are good that at some point you're going to need to collaborate on a presentation, client deliverable, or your own internal documents and processes. You can, of course, do everything over email, but version control can quickly become a nightmare, which is where shared workspaces come in. By having one central location where everyone in your group can work on the same files in real time--and see what the others have done–you can maintain version control and simplify the creation process.

Shared Virtual Task Lists

When you're working with virtual field service teams across multiple time zones, keeping everyone up to date on shared projects is more than a little challenging. But with virtual task lists, your team (or selected members of it) can see lists of all your tasks and their status, which makes sharing work and/or keeping everyone "in the know" simple. And to streamline things even more, some of the apps featuring virtual task lists also give you the option to attach files to tasks, work together on those files, and even share notes and have conversations about them without having to use a separate app – which makes it easy to work together even when your schedules don't sync up.

Contact us


NTT