Moving From Reactive To Proactive: A New Approach To Threat Protection
Moving From Reactive To Proactive: A New Approach To Threat Protection

Gaining a competitive advantage in the modern marketplace requires an infrastructure that allows for the secure execution of data and analytics, cloud, social, and mobile technologies. In line with this evolving technological environment, we see increased security breaches that consistently make headlines and lead to significant business disruption.

So how are the industry-leading enterprises adapting?

Perhaps one of the most significant trends among technologically visionary companies is the drive to unite infrastructure and security teams. With functional alignment across these teams, organizations unlock performance and reliability through a proactive threat detection and mitigation approach.

With this alignment in mind, it can be valuable to determine how your current network stacks up.
Modern Network Teams

As a starting point, let’s establish a basic overview of each department in the context of today’s network environment.

<table>
<thead>
<tr>
<th>RESPONSIBILITIES</th>
<th>INFRASTRUCTURE TEAM</th>
<th>SECURITY TEAM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>An IT infrastructure team is responsible for laying the increasingly crucial technological foundation upon which a business can scale, adapt, and meet challenging business goals.</strong></td>
<td><strong>A company’s security team is responsible for assessing network vulnerabilities and implementing policies and tools to protect a company’s valuable assets.</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PRACTICE AREAS</th>
<th>INFRASTRUCTURE TEAM</th>
<th>SECURITY TEAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IT team establishes and maintains the hardware, software, resources, and services that enable a company to deliver fast and reliable services.</td>
<td>With a comprehensive view of critical services, products, devices, and more, the security team maintains a macro view of an organization’s network to identify and mitigate security violations.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BIG PICTURE</th>
<th>INFRASTRUCTURE TEAM</th>
<th>SECURITY TEAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>From delivering valuable information to corporate stakeholders and prospective partners to facilitating operations for employees and customers, the infrastructure team is a necessity for driving business operations and growth.</td>
<td>The clearly defined and well-tested security strategy set forth by a security team allows a company to move forward in the face of a constantly evolving threat environment, minimizing business interruptions, damage to reputation, and critical data loss.</td>
<td></td>
</tr>
</tbody>
</table>

The overarching goal of these two network teams is clear: to reinforce and optimize an organization’s operations. Where the infrastructure team is focused on establishing and maintaining operational capabilities, the security team ensures critical network oversight and management. As these teams become more aligned, the network that they share will become more robust, flexible, and prepared.
Breaking Down The Barriers

We’ve established how the alignment of these key teams can benefit a network’s performance, let’s take a look at how you can start to encourage this type of collaboration within your own organization.

Initiate The Conversation

- Understand the value and location of your data assets
- Understand your applications’ security and the data they control and access
- Plan Architecture Audits

Ask The Right Questions

- What functional alignment already exists?
- Who are key members for bridging the gap?
- Where does communication break down?

Establish A Plan

- Set network Key Performance Indicators
- Outline alignment milestones
- Conduct internal reviews to validate alignment

Detailed Collaboration

As your teams move toward full alignment, your organization will have the opportunity to leverage insights into the network. From inbound traffic that has yet to enter your network to potentially malicious activity on an employee’s device, the combined perspectives of your network teams will contribute to an actionable view of your network.
The prominence of sophisticated attack techniques requires dynamic approaches to network security. And as threats multiply and evolve, it’s becoming increasingly important to have visibility into your network as well as the flexibility to make security maneuvers in real time.

**A proactive security approach can make the difference between debilitating downtime and operational stability.**

**Why?** Because in the face of proactive security policies, cyber criminals lack the advantage of concealing their activity beneath network noise and inefficient communication. With the ability to analyze traffic behavior before it engages with your network, you’ll be prepared to identify and mitigate attacks before they can impact your bottom line.
Coordinated Business Protection

The practice of aligning infrastructure and security teams is finding its place at the core of today’s most successful enterprise networks, and for good reason. An increasingly sophisticated threat landscape means that the ability to proactively anticipate future situations is critical to successful business operations.

And it’s not just about survival and recovery. To remain competitive in today’s digital marketplace, you need to adapt to threats before they ever breach your security perimeter.

Proactive security is a group effort, and it requires organizations to push their limits and initiate strategic conversations to encourage collaboration. At Level 3, we help to get these conversations started every day. Our global network offers insights and resources that can play a powerful role in bringing your organization to the next level of proactive security and business performance.

Contact Level 3 with questions about network security and protecting your organization against modern threats.